



CHAPTER 2

Alarm Troubleshooting



Note

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

This chapter gives a description, severity, and troubleshooting procedure for each commonly encountered Cisco ONS 15454 alarm and condition. Tables 2-1 through 2-5 provide lists of ONS 15454 alarms organized by severity. Table 2-6 on page 2-11 provides a list of alarms organized alphabetically. Table 2-7 gives definitions of all ONS 15454 alarm logical objects, which are the basis of the alarm profile list in Table 2-8 on page 2-24. For a comprehensive list of all conditions and instructions for using TL1 commands, refer to the *Cisco ONS SONET TL1 Command Guide*.

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

Alarms can occur even in those cards that are not explicitly mentioned in the Alarm sections. When an alarm is raised, refer to its clearing procedure.

For more information about alarm profiles, refer to the "Manage Alarms" chapter in the *Cisco ONS 15454 Procedure Guide*.

2.1 Alarm Indexes by Default Severity

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



Note

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

**Note**

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

2.1.1 Critical Alarms (CR)

Table 2-1 alphabetically lists ONS 15454 Critical (CR) alarms.

Table 2-1 ONS 15454 Critical Alarm List

—	LOF (DS3)	OPWR-HFAIL (AOTS)
—	LOF (EC1)	OPWR-HFAIL (OCH)
AUTOLSTROFF (OCN)	LOF (OCN)	OPWR-HFAIL (OMS)
AWG-FAIL (OTS)	LOF (STSTRM)	OPWR-HFAIL (OTS)
AWG-OVERTEMP (OTS)	LOF (TRUNK)	OPWR-LFAIL (AOTS)
BKUPMEMP (EQPT)	LOM (STSMON)	OPWR-LFAIL (OCH-TERM)
COMIOXC (EQPT)	LOM (STSTRM)	OPWR-LFAIL (OCH)
CONTBUS-DISABLED (EQPT)	LOM (TRUNK)	OPWR-LFAIL (OMS)
CTNEQPT-PBPROT (EQPT)	LOP-P (STSMON)	OPWR-LFAIL (OTS)
CTNEQPT-PBWORK (EQPT)	LOP-P (STSTRM)	OTUK-LOF (TRUNK)
ENCAP-MISMATCH-P (STSTRM)	LOS (2R)	OTUK-TIM (TRUNK)
EQPT (AICI-AEP)	LOS (DS3)	PLM-P (STSMON)
EQPT (AICI-AIE)	LOS (EC1)	PLM-P (STSTRM)
EQPT (EQPT)	LOS (ESCON)	PORT-FAIL (OCH)
EQPT (PPM)	LOS (ISC)	SQM (STSTRM)
EQPT-DIAG (EQPT)	LOS (OCN)	SWMTXMOD-PROT (EQPT)
EQPT-MISS (FAN)	LOS (OTS)	SWMTXMOD-WORK (EQPT)
FAN (FAN)	LOS (TRUNK)	TIM (OCN)
GAIN-HFAIL (AOTS)	LOS-P (OCH)	TIM (TRUNK)
GAIN-LFAIL (AOTS)	LOS-P (OMS)	TIM-P (STSTRM)
GE-OOSYNC (FC)	LOS-P (OTS)	TIM-S (EC1)
GE-OOSYNC (GE)	LOS-P (TRUNK)	TIM-S (OCN)
GE-OOSYNC (ISC)	LOS-RAMAN (OTS)	UNEQ-P (STSMON)
GE-OOSYNC (TRUNK)	MEA (AIP)	UNEQ-P (STSTRM)
HITEMP (NE)	MEA (BIC)	VOA-DISABLED (EQPT)
I-HITEMP (NE)	MEA (EQPT)	VOA-HFAIL (AOTS)
ILK-FAIL (TRUNK)	MEA (FAN)	VOA-HFAIL (OCH)
IMPROPRMVL (EQPT)	MEA (PPM)	VOA-HFAIL (OMS)

Table 2-1 ONS 15454 Critical Alarm List (continued)

IMPROPRMVL (PPM)	MFGMEM (AICI-AEP)	VOA-HFAIL (OTS)
LINK-KEEPALIVE (ML1000)	MFGMEM (AICI-AIE)	VOA-LFAIL (AOTS)
LINK-KEEPALIVE (ML100T)	MFGMEM (AIP)	VOA-LFAIL (OCH)
LINK-KEEPALIVE (MLFX)	MFGMEM (BPLANE)	VOA-LFAIL (OMS)
LINK-KEEPALIVE (MLMR)	MFGMEM (FAN)	VOA-LFAIL (OTS)
LOA (VCG)	MFGMEM (PPM)	—

2.1.2 Major Alarms (MJ)

Table 2-2 alphabetically lists ONS 15454 Major (MJ) alarms.

Table 2-2 ONS 15454 Major Alarm List

APSCNMIS (OCN)	GFP-DE-MISMATCH (FCMR)	TPTFAIL (FCMR)
AUTONEG-RFI (ML1000)	GFP-DE-MISMATCH (GFP-FAC)	TPTFAIL (G1000)
BAT-FAIL (PWR)	GFP-EX-MISMATCH (CE1000)	TPTFAIL (ML1000)
BLSROSYNC (OCN)	GFP-EX-MISMATCH (FCMR)	RCVR-MISS (DS1)
BLSR-SW-VER-MISM (OCN)	GFP-EX-MISMATCH (GFP-FAC)	RCVR-MISS (E1)
CARLOSS (CE1000)	GFP-LFD (CE1000)	RSV-RT-EXCD-RINGLET0 (RPRIF)
CARLOSS (CE100T)	GFP-LFD (CE100T)	RSV-RT-EXCD-RINGLET1 (RPRIF)
CARLOSS (CEMR)	GFP-LFD (CEMR)	RING-ID-MIS (OCN)
CARLOSS (E1000F)	GFP-LFD (FCMR)	RING-ID-MIS (OSC-RING)
CARLOSS (E100T)	GFP-LFD (GFP-FAC)	RING-MISMATCH (OCN)
CARLOSS (EQPT)	GFP-LFD (ML1000)	RPR-PEER-MISS (RPRIF)
CARLOSS (FC)	GFP-LFD (ML100T)	RPR-PROT-CONFIG-MISM (RPRIF)
CARLOSS (G1000)	GFP-LFD (MLFX)	RPR-RI-FAIL (RPRIF)
CARLOSS (GE)	GFP-LFD (MLMR)	RPR-SPAN-MISMATCH (ML1000)
CARLOSS (ISC)	GFP-NO-BUFFERS (FCMR)	RPR-SPAN-MISMATCH (ML100T)
CARLOSS (ML1000)	GFP-NO-BUFFERS (GFP-FAC)	RPR-SPAN-MISMATCH (MLFX)
CARLOSS (ML100T)	GFP-UP-MISMATCH (CE1000)	RPR-SPAN-MISMATCH (MLMR)
CARLOSS (MLFX)	GFP-UP-MISMATCH (CE100T)	SHELF-COMM-FAIL (SHELF)
CARLOSS (MLMR)	GFP-UP-MISMATCH (CEMR)	SIGLOSS (ESCON)
CARLOSS (TRUNK)	GFP-UP-MISMATCH (FCMR)	SIGLOSS (FC)
DATA-CRC (CE100T)	GFP-UP-MISMATCH (GFP-FAC)	SIGLOSS (FCMR)
DATA-CRC (ML1000)	GFP-UP-MISMATCH (ML1000)	SIGLOSS (GE)
DATA-CRC (ML100T)	GFP-UP-MISMATCH (ML100T)	SIGLOSS (ISC)
DATA-CRC (MLFX)	GFP-UP-MISMATCH (MLFX)	SIGLOSS (TRUNK)
DBOSYNC (NE)	GFP-UP-MISMATCH (MLMR)	SQM (VT-TERM)

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

DSP-COMM-FAIL (TRUNK)	HIBATVG (PWR)	SYNCLOSS (FC)
DSP-FAIL (TRUNK)	INVMACADR (AIP)	SYNCLOSS (FCMR)
DUP-SHELF-ID (SHELF)	LASERBIAS-FAIL (AOTS)	SYNCLOSS (GE)
EFM-RFI-CE (MLMR)	LOF (DS1)	SYNCLOSS (ISC)
EFM-RFI-DG (MLMR)	LOF (E1)	SYNCLOSS (TRUNK)
EFM-RFI-LF (MLMR)	LOM (VT-TERM)	SYNCPRI (NE-SREF)
EHIBATVG (PWR)	LOP-V (VT-MON)	SYSBOOT (NE)
ELWBATVG (PWR)	LOP-V (VT-TERM)	TIM-V (VT-MON)
E-W-MISMATCH (OCN)	LOS (DS1)	TIM-V (VT-TERM)
EXTRA-TRAF-PREEMPT (OCN)	LOS (E1)	TPTFAIL (CE1000)
FC-DE-NES (FC)	LWBATVG (PWR)	TPTFAIL (CE100T)
FC-DE-NES (FCMR)	MAX-STATIONS (RPRIF)	TPTFAIL (CEMR)
FC-DE-NES (TRUNK)	MEA (SHELF)	TPTFAIL (ML100T)
FC-NO-CREDITS (FC)	MEM-GONE (EQPT)	TPTFAIL (MLFX)
FC-NO-CREDITS (FCMR)	ODUK-TIM-PM (TRUNK)	TPTFAIL (MLMR)
FC-NO-CREDITS (TRUNK)	OUT-OF-SYNC (FC)	TRMT (DS1)
FEC-MISM (TRUNK)	OUT-OF-SYNC (GE)	TRMT (E1)
GFP-CSF (CE1000)	OUT-OF-SYNC (TRUNK)	TRMT-MISS (DS1)
GFP-CSF (CE100T)	PLM-V (VT-MON)	TRMT-MISS (E1)
GFP-CSF (CEMR)	PLM-V (VT-TERM)	UNEQ-V (VT-MON)
GFP-CSF (FCMR)	PORT-MISMATCH (CEMR)	UNEQ-V (VT-TERM)
GFP-CSF (GFP-FAC)	PORT-MISMATCH (MLMR)	UT-COMM-FAIL (TRUNK)
GFP-CSF (ML1000)	PRC-DUPID (OCN)	UT-FAIL (TRUNK)
GFP-CSF (ML100T)	PROV-MISMATCH (TRUNK)	WVL-MISMATCH (TRUNK)
GFP-CSF (MLFX)	PTIM (TRUNK)	—
GFP-CSF (MLMR)	PWR-PROT-ON (OTS)	—

2.1.3 Minor Alarms (MN)

Table 2-3 alphabetically lists ONS 15454 Minor (MN) alarms.

Table 2-3 ONS 15454 Minor Alarm List

—	HI-LASERBIAS (PPM)	LOS-O (OTS)
—	HI-LASERBIAS (TRUNK)	LO-TXPOWER (2R)
APC-CORR-SKIPPED (AOTS)	HI-LASERTEMP (EQPT)	LO-TXPOWER (EQPT)
APC-CORR-SKIPPED (OCH)	HI-LASERTEMP (OCN)	LO-TXPOWER (ESCON)
APC-CORR-SKIPPED (OMS)	HI-LASERTEMP (PPM)	LO-TXPOWER (FC)

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

APC-CORR-SKIPPED (OTS)	HI-RXPOWER (2R)	LO-TXPOWER (GE)
APC-OUT-OF-RANGE (AOTS)	HI-RXPOWER (ESCON)	LO-TXPOWER (ISC)
APC-OUT-OF-RANGE (OCH)	HI-RXPOWER (FC)	LO-TXPOWER (OCN)
APC-OUT-OF-RANGE (OMS)	HI-RXPOWER (GE)	LO-TXPOWER (PPM)
APC-OUT-OF-RANGE (OTS)	HI-RXPOWER (ISC)	LO-TXPOWER (TRUNK)
APSB (OCN)	HI-RXPOWER (OCN)	MEM-LOW (EQPT)
APSCDFTK (OCN)	HI-RXPOWER (TRUNK)	OPWR-HDEG (AOTS)
APSC-IMP (OCN)	HITEMP (EQPT)	OPWR-HDEG (OCH-TERM)
APSCINCON (OCN)	HI-TXPOWER (2R)	OPWR-HDEG (OCH)
APSCM (OCN)	HI-TXPOWER (EQPT)	OPWR-HDEG (OMS)
APSIMP (OCN)	HI-TXPOWER (ESCON)	OPWR-HDEG (OTS)
APS-INV-PRIM (OCN)	HI-TXPOWER (FC)	OPWR-LDEG (AOTS)
APSM (OCN)	HI-TXPOWER (GE)	OPWR-LDEG (OCH-TERM)
AUTORESET (EQPT)	HI-TXPOWER (ISC)	OPWR-LDEG (OCH)
AWG-DEG (OTS)	HI-TXPOWER (OCN)	OPWR-LDEG (OMS)
BPV (BITS)	HI-TXPOWER (PPM)	OPWR-LDEG (OTS)
CASETEMP-DEG (AOTS)	HI-TXPOWER (TRUNK)	OTUK-IAE (TRUNK)
COMM-FAIL (EQPT)	ISIS-ADJ-FAIL (OCN)	PEER-NORESPONSE (MLMR)
CONTBUS-A-18 (EQPT)	ISIS-ADJ-FAIL (TRUNK)	PROTNA (EQPT)
CONTBUS-B-18 (EQPT)	KBYTE-APS-CHAN-FAIL (OCN)	PROV-MISMATCH (PPM)
CONTBUS-IO-A (EQPT)	LASERBIAS-DEG (AOTS)	PWR-FAIL-A (EQPT)
CONTBUS-IO-B (EQPT)	LASERBIAS-DEG (OTS)	PWR-FAIL-B (EQPT)
CPP-PEER-NO-RESP (MLMR)	LASEREOL (OCN)	PWR-FAIL-RET-A (EQPT)
DATAFLT (NE)	LASERTEMP-DEG (AOTS)	PWR-FAIL-RET-B (EQPT)
DCU-LOSS-FAIL (OTS)	LMP-FAIL (CTRL)	ROUTE-OVERFLOW (NE)
DUP-IPADDR (NE)	LMP-FAIL (GE)	SFTWDOWN (EQPT)
DUP-NODENAME (NE)	LMP-FAIL (OCN)	SH-IL-VAR-DEG-HIGH (OTS)
EOC (OCN)	LMP-FAIL (TLINK)	SH-IL-VAR-DEG-LOW (OTS)
EOC (TRUNK)	LMP-SD (GE)	SNTP-HOST (NE)
EOC-L (OCN)	LMP-SD (OCN)	SPANLEN-OUT-OF-RANGE (OTS)
EOC-L (TRUNK)	LMP-SF (GE)	SSM-FAIL (BITS)
ERROR-CONFIG (EQPT)	LMP-SF (OCN)	SSM-FAIL (DS1)
EXCCOL (EQPT)	LOF (BITS)	SSM-FAIL (E1)
EXT (ENVALRM)	LO-LASERBIAS (EQPT)	SSM-FAIL (OCN)
FAPS-CONFIG-MISMATCH (EQPT)	LO-LASERBIAS (OCN)	SSM-FAIL (TRUNK)
FEPRLF (OCN)	LO-LASERBIAS (PPM)	SYNCPRI (EXT-SREF)
FIBERTEMP-DEG (AOTS)	LO-LASERTEMP (EQPT)	SYNCSEC (EXT-SREF)

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

FP-LINK-LOSS (EQPT)	LO-LASERTEMP (OCN)	SYNCSEC (NE-SREF)
GAIN-HDEG (AOTS)	LO-LASERTEMP (PPM)	SYNCTHIRD (EXT-SREF)
GAIN-LDEG (AOTS)	LO-RXPOWER (2R)	SYNCTHIRD (NE-SREF)
GCC-EOC (TRUNK)	LO-RXPOWER (ESCON)	TIM-MON (OCN)
HELLO (OCN)	LO-RXPOWER (FC)	TIM-MON (TRUNK)
HELLO (TRUNK)	LO-RXPOWER (GE)	TIM-P (STSMON)
HI-LASERBIAS (2R)	LO-RXPOWER (ISC)	VOA-HDEG (AOTS)
HI-LASERBIAS (EQPT)	LO-RXPOWER (OCN)	VOA-HDEG (OCH)
HI-LASERBIAS (ESCON)	LO-RXPOWER (TRUNK)	VOA-HDEG (OMS)
HI-LASERBIAS (FC)	LOS (BITS)	VOA-HDEG (OTS)
HI-LASERBIAS (GE)	LOS (FUDC)	VOA-LDEG (AOTS)
HI-LASERBIAS (ISC)	LOS (MSUDC)	VOA-LDEG (OCH)
HI-LASERBIAS (OCN)	LOS-O (OCH)	VOA-LDEG (OMS)
APS-PRIM-SEC-MISM (OCN)	LOS-O (OMS)	VOA-LDEG (OTS)

2.1.4 NA Conditions

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

Table 2-4 ONS 15454 NA Conditions List

ALS (2R)	FRCDSWTOSEC (NE-SREF)	SD (DS1)
ALS (AOTS)	FRCDSWTOTHIRD (EXT-SREF)	SD (DS3)
ALS (ESCON)	FRNGSYNC (NE-SREF)	SD (TRUNK)
ALS (FC)	FSTSYNC (NE-SREF)	SD-L (EC1)
ALS (GE)	FTA-MISMATCH (EQPT)	SD-L (TRUNK)
ALS (ISC)	FULLPASSTHR-BI (OCN)	SD-P (STSMON)
ALS (OCN)	HI-CCVOLT (BITS)	SD-P (STSTRM)
ALS (TRUNK)	HLDOVRSYNC (NE-SREF)	SD-V (VT-MON)
ALS-DISABLED (EQPT)	IDLE (DS1)	SD-V (VT-TERM)
AMPLI-INIT (AOTS)	INC-ISD (DS3)	SF (DS1)
APC-DISABLED (AOTS)	INHSWPR (EQPT)	SF (DS3)
APC-DISABLED (EQPT)	INHSWWKG (EQPT)	SF (TRUNK)
APC-DISABLED (NE)	INTRUSION-PSWD (NE)	SF-L (EC1)
APC-DISABLED (OCH)	IOSCFGCOPY (EQPT)	SF-L (OCN)
APC-DISABLED (OMS)	KB-PASSTHR (OCN)	SF-L (TRUNK)
APC-DISABLED (OTS)	LAN-POL-REV (NE)	SF-P (STSMON)
APC-DISABLED (SHELF)	LASER-APR (AOTS)	SF-P (STSTRM)

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

APC-END (NE)	LASER-APR (OTS)	SF-V (VT-MON)
APC-WRONG-GAIN (AOTS)	LCAS-CRC (STSTRM)	SF-V (VT-TERM)
APS-PRIM-FAC (OCN)	LCAS-CRC (VT-TERM)	SHUTTER-OPEN (OTS)
AS-CMD (2R)	LCAS-RX-DNU (STSTRM)	SPAN-NOT-MEASURED (OTS)
AS-CMD (AOTS)	LCAS-RX-DNU (VT-TERM)	SPAN-SW-EAST (OCN)
AS-CMD (BPLANE)	LCAS-RX-FAIL (STSTRM)	SPAN-SW-WEST (OCN)
AS-CMD (CE1000)	LCAS-RX-FAIL (VT-TERM)	SQUELCH (OCN)
AS-CMD (CE100T)	LCAS-RX-GRP-ERR (STSTRM)	SQUELCHED (2R)
AS-CMD (CEMR)	LCAS-RX-GRP-ERR (VT-TERM)	SQUELCHED (ESCON)
AS-CMD (DS1)	LCAS-TX-ADD (STSTRM)	SQUELCHED (FC)
AS-CMD (DS3)	LCAS-TX-ADD (VT-TERM)	SQUELCHED (GE)
AS-CMD (E1000F)	LCAS-TX-DNU (STSTRM)	SQUELCHED (ISC)
AS-CMD (E100T)	LCAS-TX-DNU (VT-TERM)	SQUELCHED (OCN)
AS-CMD (E1)	LKOUTPR-S (OCN)	SQUELCHED (TRUNK)
AS-CMD (EC1)	LMP-UNALLOC (GE)	SSM-DUS (BITS)
AS-CMD (EQPT)	LMP-UNALLOC (OCN)	SSM-DUS (DS1)
AS-CMD (ESCON)	LOCKOUT-REQ (2R)	SSM-DUS (E1)
AS-CMD (FC)	LOCKOUT-REQ (EQPT)	SSM-DUS (OCN)
AS-CMD (FCMR)	LOCKOUT-REQ (ESCON)	SSM-DUS (TRUNK)
AS-CMD (G1000)	LOCKOUT-REQ (FC)	SSM-LNC (BITS)
AS-CMD (GE)	LOCKOUT-REQ (GE)	SSM-LNC (NE-SREF)
AS-CMD (GFP-FAC)	LOCKOUT-REQ (ISC)	SSM-LNC (OCN)
AS-CMD (ISC)	LOCKOUT-REQ (OCN)	SSM-LNC (TRUNK)
AS-CMD (ML1000)	LOCKOUT-REQ (OTS)	SSM-OFF (BITS)
AS-CMD (ML100T)	LOCKOUT-REQ (STSMON)	SSM-OFF (DS1)
AS-CMD (MLFX)	LOCKOUT-REQ (TRUNK)	SSM-OFF (E1)
AS-CMD (MLMR)	LOCKOUT-REQ (VT-MON)	SSM-OFF (OCN)
AS-CMD (NE)	LPBKCRS (STSMON)	SSM-OFF (TRUNK)
AS-CMD (OCH)	LPBKCRS (STSTRM)	SSM-PRC (BITS)
AS-CMD (OCN)	LPBKDS1FE-CMD (DS1)	SSM-PRC (NE-SREF)
AS-CMD (OMS)	LPBKDS3FEAC (DS3)	SSM-PRC (OCN)
AS-CMD (OTS)	LPBKDS3FEAC-CMD (DS3)	SSM-PRC (TRUNK)
AS-CMD (PPM)	LPBKFACILITY (CE1000)	SSM-PRS (BITS)
AS-CMD (PWR)	LPBKFACILITY (CE100T)	SSM-PRS (DS1)
AS-CMD (SHELF)	LPBKFACILITY (CEMR)	SSM-PRS (E1)
AS-CMD (TRUNK)	LPBKFACILITY (DS1)	SSM-PRS (NE-SREF)
AS-MT (2R)	LPBKFACILITY (DS3)	SSM-PRS (OCN)

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

AS-MT (AOTS)	LPBKFACILITY (E1)	SSM-PRS (TRUNK)
AS-MT (CE1000)	LPBKFACILITY (EC1)	SSM-RES (BITS)
AS-MT (CE100T)	LPBKFACILITY (ESCON)	SSM-RES (DS1)
AS-MT (CEMR)	LPBKFACILITY (FC)	SSM-RES (E1)
AS-MT (DS1)	LPBKFACILITY (FCMR)	SSM-RES (NE-SREF)
AS-MT (DS3)	LPBKFACILITY (G1000)	SSM-RES (OCN)
AS-MT (E1)	LPBKFACILITY (GE)	SSM-RES (TRUNK)
AS-MT (EC1)	LPBKFACILITY (ISC)	SSM-SDH-TN (BITS)
AS-MT (EQPT)	LPBKFACILITY (MLMR)	SSM-SDH-TN (NE-SREF)
AS-MT (ESCON)	LPBKFACILITY (OCN)	SSM-SDH-TN (OCN)
AS-MT (FC)	LPBKFACILITY (TRUNK)	SSM-SDH-TN (TRUNK)
AS-MT (FCMR)	LPBKTERMINAL (CE1000)	SSM-SETS (BITS)
AS-MT (G1000)	LPBKTERMINAL (CE100T)	SSM-SETS (NE-SREF)
AS-MT (GE)	LPBKTERMINAL (CEMR)	SSM-SETS (OCN)
AS-MT (GFP-FAC)	LPBKTERMINAL (DS1)	SSM-SETS (TRUNK)
AS-MT (ISC)	LPBKTERMINAL (DS3)	SSM-SMC (BITS)
AS-MT (ML1000)	LPBKTERMINAL (E1)	SSM-SMC (DS1)
AS-MT (ML100T)	LPBKTERMINAL (EC1)	SSM-SMC (E1)
AS-MT (MLFX)	LPBKTERMINAL (ESCON)	SSM-SMC (NE-SREF)
AS-MT (MLMR)	LPBKTERMINAL (FC)	SSM-SMC (OCN)
AS-MT (OCH)	LPBKTERMINAL (FCMR)	SSM-SMC (TRUNK)
AS-MT (OCN)	FRCDSWTOTHIRD (NE-SREF)	SSM-ST2 (BITS)
AS-MT (OMS)	LPBKTERMINAL (G1000)	SSM-ST2 (DS1)
AS-MT (OTS)	LPBKTERMINAL (GE)	SSM-ST2 (E1)
AS-MT (PPM)	LPBKTERMINAL (ISC)	SSM-ST2 (NE-SREF)
AS-MT (SHELF)	LPBKTERMINAL (MLMR)	SSM-ST2 (OCN)
AS-MT (TRUNK)	LPBKTERMINAL (OCN)	SSM-ST2 (TRUNK)
AS-MT-OOG (STSTRM)	LPBKTERMINAL (TRUNK)	SSM-ST3 (BITS)
AS-MT-OOG (VT-TERM)	MAN-REQ (EQPT)	SSM-ST3 (DS1)
AUD-LOG-LOSS (NE)	MAN-REQ (ML1000)	SSM-ST3 (E1)
AUD-LOG-LOW (NE)	MAN-REQ (ML100T)	SSM-ST3 (NE-SREF)
AUTOSW-LOP (STSMON)	MAN-REQ (MLFX)	SSM-ST3 (OCN)
AUTOSW-LOP (VT-MON)	MAN-REQ (MLMR)	SSM-ST3 (TRUNK)
AUTOSW-PDI (STSMON)	MAN-REQ (STSMON)	SSM-ST3E (BITS)
AUTOSW-PDI (VT-MON)	MAN-REQ (VT-MON)	SSM-ST3E (DS1)
AUTOSW-SDBER (STSMON)	MANRESET (EQPT)	SSM-ST3E (E1)
AUTOSW-SDBER (VT-MON)	MANSWTOINT (NE-SREF)	SSM-ST3E (NE-SREF)

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

AUTOSW-SFBER (STSMON)	MANSWTOPRI (EXT-SREF)	SSM-ST3E (OCN)
AUTOSW-SFBER (VT-MON)	MANSWTOPRI (NE-SREF)	SSM-ST3E (TRUNK)
AUTOSW-UNEQ (STSMON)	MANSWTOSEC (EXT-SREF)	SSM-ST4 (BITS)
AUTOSW-UNEQ (VT-MON)	MANSWTOSEC (NE-SREF)	SSM-ST4 (DS1)
AWG-WARM-UP (OTS)	MANSWTOTHIRD (EXT-SREF)	SSM-ST4 (E1)
CLDRESTART (EQPT)	MANSWTOTHIRD (NE-SREF)	SSM-ST4 (NE-SREF)
CPP-INCAPABLE (EQPT)	MANUAL-REQ-RING (OCN)	SSM-ST4 (OCN)
CPP-INCAPABLE (MLMR)	MANUAL-REQ-SPAN (2R)	SSM-ST4 (TRUNK)
CPP-INCAPABLE (RPR)	MANUAL-REQ-SPAN (EC1)	SSM-STU (BITS)
CTNEQPT-MISMATCH (EQPT)	MANUAL-REQ-SPAN (ESCON)	SSM-STU (DS1)
DS3-MISM (DS3)	MANUAL-REQ-SPAN (FC)	SSM-STU (E1)
ETH-LINKLOSS (NE)	MANUAL-REQ-SPAN (GE)	SSM-STU (NE-SREF)
EXERCISE-RING-FAIL (OCN)	MANUAL-REQ-SPAN (ISC)	SSM-STU (OCN)
EXERCISE-SPAN-FAIL (OCN)	MANUAL-REQ-SPAN (OCN)	SSM-STU (TRUNK)
FAILTOSW (2R)	MANUAL-REQ-SPAN (OTS)	SSM-TNC (BITS)
FAILTOSW (EQPT)	MANUAL-REQ-SPAN (TRUNK)	SSM-TNC (NE-SREF)
FAILTOSW (ESCON)	MCAST-MAC-TABLE-FULL (EQPT)	SSM-TNC (OCN)
FAILTOSW (FC)	MS-DEG (E1)	SSM-TNC (TRUNK)
FAILTOSW (GE)	MS-EXC (E1)	STS-SQUELCH-L (OCN)
FAILTOSW (ISC)	MT-OCHNC (OTS)	SW-MISMATCH (EQPT)
FAILTOSW (OCN)	NO-CONFIG (EQPT)	SWTOPRI (EXT-SREF)
FAILTOSW (OTS)	OCHNC-INC (OCHNC-CONN)	SWTOPRI (NE-SREF)
FAILTOSW (TRUNK)	OCHTERM-INC (OCH-TERM)	SWTOSEC (EXT-SREF)
FAILTOSW-PATH (STSMON)	ODUK-SD-PM (TRUNK)	SWTOSEC (NE-SREF)
FAILTOSW-PATH (VT-MON)	ODUK-SF-PM (TRUNK)	SWTOTHIRD (EXT-SREF)
FAILTOSWR (OCN)	OOU-TPT (STSTRM)	SWTOTHIRD (NE-SREF)
FAILTOSWS (OCN)	OOU-TPT (VT-TERM)	SYNC-FREQ (BITS)
FAPS (FCMR)	OPEN-SLOT (EQPT)	SYNC-FREQ (DS1)
FAPS (TRUNK)	OSRION (AOTS)	SYNC-FREQ (E1)
FDI (OCH-TERM)	OSRION (OTS)	SYNC-FREQ (OCN)
FDI (OCH)	OTUK-SD (TRUNK)	SYNC-FREQ (TRUNK)
FE-AIS (DS3)	OTUK-SF (TRUNK)	TEMP-MISM (NE)
FE-DS1-MULTLOS (DS3)	OUT-OF-SYNC (ISC)	TRAIL-SIGNAL-FAIL (OCH)
FE-DS1-NSA (DS3)	PARAM-MISM (AOTS)	TRAIL-SIGNAL-FAIL (TRUNK)
FE-DS1-SA (DS3)	PARAM-MISM (OCH-TERM)	TX-IDLE (DS1)
FE-DS1-SNGLLOS (DS3)	PARAM-MISM (OCH)	TX-RAI (DS1)
FE-DS3-NSA (DS3)	PARAM-MISM (OMS)	TX-RAI (DS3)

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

FE-DS3-SA (DS3)	PARAM-MISM (OTS)	TX-RAI (E1)
FE-EQPT-NSA (DS3)	PDI-P (STSMON)	UNC-WORD (TRUNK)
FE-FRCDWKS WBK-SPAN (OCN)	PDI-P (STSTRM)	VCG-DEG (VCG)
FE-FRCDWKS WPR-RING (EC1)	PMI (OMS)	VCG-DOWN (VCG)
FE-FRCDWKS WPR-RING (OCN)	PMI (OTS)	VOLT-MISM (PWR)
FE-FRCDWKS WPR-SPAN (OCN)	PORT-MISMATCH (FCMR)	VT-SQUELCH-L (OCN)
FE-IDLE (DS3)	RAI (DS1)	WIZARD-IS-RUNNING (OTS)
FE-LOCKOUTOFPR-SPAN (OCN)	RAI (DS3)	WKS WPR (2R)
FE-LOF (DS3)	RAI (E1)	WKS WPR (EQPT)
FE-LOS (DS3)	RAMAN-SPAN-NOT-TUNED (OTS)	WKS WPR (ESCON)
FE-MANWKS WBK-SPAN (OCN)	RING-SW-EAST (OCN)	WKS WPR (FC)
FE-MANWKS WPR-RING (EC1)	RING-SW-WEST (OCN)	WKS WPR (GE)
FE-MANWKS WPR-RING (OCN)	RLS (OTS)	WKS WPR (ISC)
FE-MANWKS WPR-SPAN (OCN)	ROLL (STSMON)	WKS WPR (OCN)
FORCED-REQ (EQPT)	ROLL (STSTRM)	WKS WPR (OTS)
FORCED-REQ (ML1000)	ROLL (VT-MON)	WKS WPR (STSMON)
FORCED-REQ (ML100T)	ROLL (VT-TERM)	WKS WPR (VT-MON)
FORCED-REQ (MLFX)	ROLL-PEND (STSMON)	WORK-QUEUE-FULL (EQPT)
FORCED-REQ (MLMR)	ROLL-PEND (VT-MON)	WTR (2R)
FORCED-REQ (STSMON)	ROLL-PEND (VT-TERM)	WTR (EC1)
FORCED-REQ (VT-MON)	RPR-PASSTHR (RPRIF)	WTR (EQPT)
FORCED-REQ-RING (OCN)	RPR-PROT-ACTIVE (RPRIF)	WTR (ESCON)
FORCED-REQ-SPAN (2R)	RPR-SD (ML1000)	WTR (FC)
FORCED-REQ-SPAN (EC1)	RPR-SD (ML100T)	WTR (GE)
FORCED-REQ-SPAN (ESCON)	RPR-SD (MLFX)	WTR (ISC)
FORCED-REQ-SPAN (FC)	SD-L (OCN)	WTR (ML1000)
FORCED-REQ-SPAN (GE)	RPR-SD (MLMR)	WTR (ML100T)
FORCED-REQ-SPAN (ISC)	RPR-SF (ML1000)	WTR (MLFX)
FORCED-REQ-SPAN (OCN)	RPR-SF (ML100T)	WTR (MLMR)
FORCED-REQ-SPAN (OTS)	RPR-SF (MLFX)	WTR (OCN)
FORCED-REQ-SPAN (TRUNK)	RPR-SF (MLMR)	WTR (STSMON)
FRCDSWTOINT (NE-SREF)	RPRW (ML1000)	WTR (TRUNK)
FRCDSWTOPRI (EXT-SREF)	RPRW (ML100T)	WTR (VT-MON)
FRCDSWTOPRI (NE-SREF)	RPRW (MLFX)	—
FRCDSWTOSEC (EXT-SREF)	RUNCFG-SAVENEED (EQPT)	—

2.1.5 NR Conditions

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

Table 2-5 ONS 15454 NR Conditions List

AIS (BITS)	BERT-SYNC-FAIL (DS1, DS3)	OTUK-BDI (TRUNK)
AIS (DS1)	ERFI-P-CONN (STSMON)	RFI (TRUNK)
AIS (DS3)	ERFI-P-CONN (STSTRM)	RFI-L (EC1)
AIS (E1)	ERFI-P-PAYLD (STSMON)	RFI-L (OCN)
AIS (FUDC)	ERFI-P-PAYLD (STSTRM)	RFI-L (TRUNK)
AIS (MSUDC)	ERFI-P-SRVR (STSMON)	RFI-P (STSMON)
AIS (TRUNK)	ERFI-P-SRVR (STSTRM)	RFI-P (STSTRM)
AIS-L (EC1)	NON-CISCO-PPM (PPM)	RFI-V (VT-MON)
AIS-L (OCN)	ODUK-1-AIS-PM (TRUNK)	RFI-V (VT-TERM)
AIS-L (TRUNK)	ODUK-2-AIS-PM (TRUNK)	ROLL-PEND (STSTRM)
AIS-P (STSMON)	ODUK-3-AIS-PM (TRUNK)	TX-AIS (DS1)
AIS-P (STSTRM)	ODUK-4-AIS-PM (TRUNK)	TX-AIS (DS3)
AIS-V (VT-MON)	ODUK-AIS-PM (TRUNK)	TX-AIS (E1)
AIS-V (VT-TERM)	ODUK-BDI-PM (TRUNK)	TX-LOF (DS1)
AUTOSW-AIS (STSMON)	ODUK-LCK-PM (TRUNK)	TX-LOF (E1)
AUTOSW-AIS (VT-MON)	ODUK-OCI-PM (TRUNK)	UNQUAL-PPM (PPM)
BERT-ENBL (DS1, DS3)	OTUK-AIS (TRUNK)	VLAN-AIS (ETH)

2.2 Alarms and Conditions Listed By Alphabetical Entry

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

Table 2-6 ONS 15454 Alarm and Condition Alphabetical List

—	GFP-EX-MISMATCH (GFP-FAC)	PLM-V (VT-MON)
—	GFP-LFD (CE1000)	PLM-V (VT-TERM)
—	GFP-LFD (CE100T)	PMI (OMS)
—	GFP-LFD (CEMR)	PMI (OTS)
AIS (BITS)	GFP-LFD (FCMR)	PORT-FAIL (OCH)
AIS (DS1)	GFP-LFD (ML1000)	PORT-MISMATCH (CEMR)
AIS (DS3)	GFP-LFD (ML100T)	PORT-MISMATCH (FCMR)
AIS (E1)	GFP-LFD (MLFX)	PORT-MISMATCH (MLMR)
AIS (FUDC)	GFP-LFD (MLMR)	PRC-DUPID (OCN)
AIS (MSUDC)	GFP-NO-BUFFERS (FCMR)	PROTNA (EQPT)
AIS (TRUNK)	GFP-NO-BUFFERS (GFP-FAC)	PROV-MISMATCH (PPM)

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

AIS-L (EC1)	GFP-UP-MISMATCH (CE1000)	PROV-MISMATCH (TRUNK)
AIS-L (OCN)	GFP-UP-MISMATCH (CE100T)	PTIM (TRUNK)
AIS-L (TRUNK)	GFP-UP-MISMATCH (CEMR)	PWR-FAIL-A (EQPT)
AIS-P (STSMON)	GFP-UP-MISMATCH (FCMR)	PWR-FAIL-B (EQPT)
AIS-P (STSTRM)	GFP-UP-MISMATCH (GFP-FAC)	PWR-FAIL-RET-A (EQPT)
AIS-V (VT-MON)	GFP-UP-MISMATCH (ML1000)	PWR-FAIL-RET-B (EQPT)
AIS-V (VT-TERM)	GFP-UP-MISMATCH (ML100T)	PWR-PROT-ON (OTS)
ALS (2R)	GFP-UP-MISMATCH (MLFX)	RAI (DS1)
ALS (AOTS)	GFP-UP-MISMATCH (MLMR)	RAI (DS3)
ALS (ESCON)	HELLO (OCN)	RAI (E1)
ALS (FC)	HELLO (TRUNK)	RAMAN-SPAN-NOT-TUNED (OTS)
ALS (GE)	HIBATVG (PWR)	RCVR-MISS (DS1)
ALS (ISC)	HI-CCVOLT (BITS)	RCVR-MISS (E1)
ALS (OCN)	HI-LASERBIAS (2R)	RSV-RT-EXCD-RINGLET0 (RPRIF)
ALS (TRUNK)	HI-LASERBIAS (EQPT)	RSV-RT-EXCD-RINGLET1 (RPRIF)
ALS-DISABLED (EQPT)	HI-LASERBIAS (ESCON)	RFI (TRUNK)
AMPLI-INIT (AOTS)	HI-LASERBIAS (FC)	RFI-L (EC1)
APC-CORR-SKIPPED (AOTS)	HI-LASERBIAS (GE)	RFI-L (OCN)
APC-CORR-SKIPPED (OCH)	HI-LASERBIAS (ISC)	RFI-L (TRUNK)
APC-CORR-SKIPPED (OMS)	HI-LASERBIAS (OCN)	RFI-P (STSMON)
APC-CORR-SKIPPED (OTS)	HI-LASERBIAS (PPM)	RFI-P (STSTRM)
APC-DISABLED (AOTS)	HI-LASERBIAS (TRUNK)	RFI-V (VT-MON)
APC-DISABLED (EQPT)	HI-LASERTEMP (EQPT)	RFI-V (VT-TERM)
APC-DISABLED (NE)	HI-LASERTEMP (OCN)	RING-ID-MIS (OCN)
APC-DISABLED (OCH)	HI-LASERTEMP (PPM)	RING-ID-MIS (OSC-RING)
APC-DISABLED (OMS)	HI-RXPOWER (2R)	RING-MISMATCH (OCN)
APC-DISABLED (OTS)	HI-RXPOWER (ESCON)	RING-SW-EAST (OCN)
APC-DISABLED (SHELF)	HI-RXPOWER (FC)	RING-SW-WEST (OCN)
APC-END (NE)	HI-RXPOWER (GE)	RLS (OTS)
APC-OUT-OF-RANGE (AOTS)	HI-RXPOWER (ISC)	ROLL (STSMON)
APC-OUT-OF-RANGE (OCH)	HI-RXPOWER (OCN)	ROLL (STSTRM)
APC-OUT-OF-RANGE (OMS)	HI-RXPOWER (TRUNK)	ROLL (VT-MON)
APC-OUT-OF-RANGE (OTS)	HITEMP (EQPT)	ROLL (VT-TERM)
APC-WRONG-GAIN (AOTS)	HITEMP (NE)	ROLL-PEND (STSMON)
APSB (OCN)	HI-TXPOWER (2R)	ROLL-PEND (STSTRM)
APSCDFLTK (OCN)	HI-TXPOWER (EQPT)	ROLL-PEND (VT-MON)
APSC-IMP (OCN)	HI-TXPOWER (ESCON)	ROLL-PEND (VT-TERM)

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

APSCINCON (OCN)	HI-TXPOWER (FC)	RPR-PASSTHR (RPRIF)
APSCM (OCN)	HI-TXPOWER (GE)	RPR-PEER-MISS (RPRIF)
APSCNMIS (OCN)	HI-TXPOWER (ISC)	RPR-PROT-ACTIVE (RPRIF)
APSIMP (OCN)	HI-TXPOWER (OCN)	RPR-PROT-CONFIG-MISM (RPRIF)
APS-INV-PRIM (OCN)	HI-TXPOWER (PPM)	RPR-RI-FAIL (RPRIF)
APSM (OCN)	HI-TXPOWER (TRUNK)	RPR-SD (ML1000)
APS-PRIM-FAC (OCN)	HLDOVRSYNC (NE-SREF)	RPR-SD (ML100T)
APS-PRIM-SEC-MISM (OCN)	IDLE (DS1)	RPR-SD (MLFX)
AS-CMD (2R)	I-HITEMP (NE)	RPR-SD (MLMR)
AS-CMD (AOTS)	ILK-FAIL (TRUNK)	RPR-SF (ML1000)
AS-CMD (BPLANE)	IMPROPRMVL (EQPT)	RPR-SF (ML100T)
AS-CMD (CE1000)	IMPROPRMVL (PPM)	RPR-SF (MLFX)
AS-CMD (CE100T)	INC-ISD (DS3)	RPR-SF (MLMR)
AS-CMD (CEMR)	INHSWPR (EQPT)	RPR-SPAN-MISMATCH (ML1000)
AS-CMD (DS1)	INHSWWKG (EQPT)	RPR-SPAN-MISMATCH (ML100T)
AS-CMD (DS3)	INTRUSION-PSWD (NE)	RPR-SPAN-MISMATCH (MLFX)
AS-CMD (E1)	INVMACADR (AIP)	RPR-SPAN-MISMATCH (MLMR)
AS-CMD (E1000F)	IOSCFGCOPY (EQPT)	RPRW (ML1000)
AS-CMD (E100T)	ISIS-ADJ-FAIL (OCN)	RPRW (ML100T)
AS-CMD (EC1)	ISIS-ADJ-FAIL (TRUNK)	RPRW (MLFX)
AS-CMD (EQPT)	KB-PASSTHR (OCN)	RUNCFG-SAVENEED (EQPT)
AS-CMD (ESCON)	KBYTE-APS-CHAN-FAIL (OCN)	SD (DS1)
AS-CMD (FC)	LAN-POL-REV (NE)	SD (DS3)
AS-CMD (FCMR)	LASER-APR (AOTS)	SD (TRUNK)
AS-CMD (G1000)	LASER-APR (OTS)	SD-L (EC1)
AS-CMD (GE)	LASERBIAS-DEG (AOTS)	SD-L (OCN)
AS-CMD (GFP-FAC)	LASERBIAS-DEG (OTS)	SD-L (TRUNK)
AS-CMD (ISC)	LASERBIAS-FAIL (AOTS)	SD-P (STSMON)
AS-CMD (ML1000)	LASEREOL (OCN)	SD-P (STSTRM)
AS-CMD (ML100T)	LASERTEMP-DEG (AOTS)	SD-V (VT-MON)
AS-CMD (MLFX)	LCAS-CRC (STSTRM)	SD-V (VT-TERM)
AS-CMD (MLMR)	LCAS-CRC (VT-TERM)	SF (DS1)
AS-CMD (NE)	LCAS-RX-DNU (STSTRM)	SF (DS3)
AS-CMD (OCH)	LCAS-RX-DNU (VT-TERM)	SF (TRUNK)
AS-CMD (OCN)	LCAS-RX-FAIL (STSTRM)	SF-L (EC1)
AS-CMD (OMS)	LCAS-RX-FAIL (VT-TERM)	SF-L (OCN)
AS-CMD (OTS)	LCAS-RX-GRP-ERR (STSTRM)	SF-L (TRUNK)

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

AS-CMD (PPM)	LCAS-RX-GRP-ERR (VT-TERM)	SF-P (STSMON)
AS-CMD (PWR)	LCAS-TX-ADD (STSTRM)	SF-P (STSTRM)
AS-CMD (SHELF)	LCAS-TX-ADD (VT-TERM)	SFTWDOWN (EQPT)
AS-CMD (TRUNK)	LCAS-TX-DNU (STSTRM)	SF-V (VT-MON)
AS-MT (2R)	LCAS-TX-DNU (VT-TERM)	SF-V (VT-TERM)
AS-MT (AOTS)	LINK-KEEPALIVE (ML1000)	SHELF-COMM-FAIL (SHELF)
AS-MT (CE1000)	LINK-KEEPALIVE (ML100T)	SH-IL-VAR-DEG-HIGH (OTS)
AS-MT (CE100T)	LINK-KEEPALIVE (MLFX)	SH-IL-VAR-DEG-LOW (OTS)
AS-MT (CEMR)	LINK-KEEPALIVE (MLMR)	SHUTTER-OPEN (OTS)
AS-MT (DS1)	LKOUTPR-S (OCN)	SIGLOSS (ESCON)
AS-MT (DS3)	LMP-FAIL (CTRL)	SIGLOSS (FC)
AS-MT (E1)	LMP-FAIL (GE)	SIGLOSS (FCMR)
AS-MT (EC1)	LMP-FAIL (OCN)	SIGLOSS (GE)
AS-MT (EQPT)	LMP-FAIL (TLINK)	SIGLOSS (ISC)
AS-MT (ESCON)	LMP-SD (GE)	SIGLOSS (TRUNK)
AS-MT (FC)	LMP-SD (OCN)	SNTP-HOST (NE)
AS-MT (FCMR)	LMP-SF (GE)	SPANLEN-OUT-OF-RANGE (OTS)
AS-MT (G1000)	LMP-SF (OCN)	SPAN-NOT-MEASURED (OTS)
AS-MT (GE)	LMP-UNALLOC (GE)	SPAN-SW-EAST (OCN)
AS-MT (GFP-FAC)	LMP-UNALLOC (OCN)	SPAN-SW-WEST (OCN)
AS-MT (ISC)	LOA (VCG)	SQM (STSTRM)
AS-MT (ML1000)	LOCKOUT-REQ (2R)	SQM (VT-TERM)
AS-MT (ML100T)	LOCKOUT-REQ (EQPT)	SQUELCH (OCN)
AS-MT (MLFX)	LOCKOUT-REQ (ESCON)	SQUELCHED (2R)
AS-MT (MLMR)	LOCKOUT-REQ (FC)	SQUELCHED (ESCON)
AS-MT (OCH)	LOCKOUT-REQ (GE)	SQUELCHED (FC)
AS-MT (OCN)	LOCKOUT-REQ (ISC)	SQUELCHED (GE)
AS-MT (OMS)	LOCKOUT-REQ (OCN)	SQUELCHED (ISC)
AS-MT (OTS)	LOCKOUT-REQ (OTS)	SQUELCHED (OCN)
AS-MT (PPM)	LOCKOUT-REQ (STSMON)	SQUELCHED (TRUNK)
AS-MT (SHELF)	LOCKOUT-REQ (TRUNK)	SSM-DUS (BITS)
AS-MT (TRUNK)	LOCKOUT-REQ (VT-MON)	SSM-DUS (DS1)
AS-MT-OOG (STSTRM)	LOF (BITS)	SSM-DUS (E1)
AS-MT-OOG (VT-TERM)	LOF (DS1)	SSM-DUS (OCN)
AUD-LOG-LOSS (NE)	LOF (DS3)	SSM-DUS (TRUNK)
AUD-LOG-LOW (NE)	LOF (E1)	SSM-FAIL (BITS)
AUTOLSROFF (OCN)	LOF (EC1)	SSM-FAIL (DS1)

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

AUTONEG-RFI (ML1000)	LOF (OCN)	SSM-FAIL (E1)
AUTORESET (EQPT)	LOF (STSTRM)	SSM-FAIL (OCN)
AUTOSW-AIS (STSMON)	LOF (TRUNK)	SSM-FAIL (TRUNK)
AUTOSW-AIS (VT-MON)	LO-LASERBIAS (EQPT)	SSM-LNC (BITS)
AUTOSW-LOP (STSMON)	LO-LASERBIAS (OCN)	SSM-LNC (NE-SREF)
AUTOSW-LOP (VT-MON)	LO-LASERBIAS (PPM)	SSM-LNC (OCN)
AUTOSW-PDI (STSMON)	LO-LASERTEMP (EQPT)	SSM-LNC (TRUNK)
AUTOSW-PDI (VT-MON)	LO-LASERTEMP (OCN)	SSM-OFF (BITS)
AUTOSW-SDBER (STSMON)	LO-LASERTEMP (PPM)	SSM-OFF (DS1)
AUTOSW-SDBER (VT-MON)	LOM (STSMON)	SSM-OFF (E1)
AUTOSW-SFBER (STSMON)	LOM (STSTRM)	SSM-OFF (OCN)
AUTOSW-SFBER (VT-MON)	LOM (TRUNK)	SSM-OFF (TRUNK)
AUTOSW-UNEQ (STSMON)	LOM (VT-TERM)	SSM-PRC (BITS)
AUTOSW-UNEQ (VT-MON)	LOP-P (STSMON)	SSM-PRC (NE-SREF)
AWG-DEG (OTS)	LOP-P (STSTRM)	SSM-PRC (OCN)
AWG-FAIL (OTS)	LOP-V (VT-MON)	SSM-PRC (TRUNK)
AWG-OVERTEMP (OTS)	LOP-V (VT-TERM)	SSM-PRS (BITS)
AWG-WARM-UP (OTS)	LO-RXPOWER (2R)	SSM-PRS (DS1)
BAT-FAIL (PWR)	LO-RXPOWER (ESCON)	SSM-PRS (E1)
BERT-ENBL (DS1, DS3)	LO-RXPOWER (FC)	SSM-PRS (NE-SREF)
BERT-SYNC-FAIL (DS1, DS3)	LO-RXPOWER (GE)	SSM-PRS (OCN)
BKUPMEMP (EQPT)	LO-RXPOWER (ISC)	SSM-PRS (TRUNK)
BLSROSYNC (OCN)	LO-RXPOWER (OCN)	SSM-RES (BITS)
BLSR-SW-VER-MISM (OCN)	LO-RXPOWER (TRUNK)	SSM-RES (DS1)
BPV (BITS)	LOS (2R)	SSM-RES (E1)
CARLOSS (CE1000)	LOS (BITS)	SSM-RES (NE-SREF)
CARLOSS (CE100T)	LOS (DS1)	SSM-RES (OCN)
CARLOSS (CEMR)	LOS (DS3)	SSM-RES (TRUNK)
CARLOSS (E1000F)	LOS (E1)	SSM-SDH-TN (BITS)
CARLOSS (E100T)	LOS (EC1)	SSM-SDH-TN (NE-SREF)
CARLOSS (EQPT)	LOS (ESCON)	SSM-SDH-TN (OCN)
CARLOSS (FC)	LOS (FUDC)	SSM-SDH-TN (TRUNK)
CARLOSS (G1000)	LOS (ISC)	SSM-SETS (BITS)
CARLOSS (GE)	LOS (MSUDC)	SSM-SETS (NE-SREF)
CARLOSS (ISC)	LOS (OCN)	SSM-SETS (OCN)
CARLOSS (ML1000)	LOS (OTS)	SSM-SETS (TRUNK)
CARLOSS (ML100T)	LOS (TRUNK)	SSM-SMC (BITS)

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

CARLOSS (MLFX)	LOS-O (OCH)	SSM-SMC (DS1)
CARLOSS (MLMR)	LOS-O (OMS)	SSM-SMC (E1)
CARLOSS (TRUNK)	LOS-O (OTS)	SSM-SMC (NE-SREF)
CASETEMP-DEG (AOTS)	LOS-P (OCH)	SSM-SMC (OCN)
CLDRESTART (EQPT)	LOS-P (OMS)	SSM-SMC (TRUNK)
COMIOXC (EQPT)	LOS-P (OTS)	SSM-ST2 (BITS)
COMM-FAIL (EQPT)	LOS-P (TRUNK)	SSM-ST2 (DS1)
CONTBUS-A-18 (EQPT)	LOS-RAMAN (OTS)	SSM-ST2 (E1)
CONTBUS-B-18 (EQPT)	LO-TXPOWER (2R)	SSM-ST2 (NE-SREF)
CONTBUS-DISABLED (EQPT)	LO-TXPOWER (EQPT)	SSM-ST2 (OCN)
CONTBUS-IO-A (EQPT)	LO-TXPOWER (ESCON)	SSM-ST2 (TRUNK)
CONTBUS-IO-B (EQPT)	LO-TXPOWER (FC)	SSM-ST3 (BITS)
CPP-INCAPABLE (MLMR)	LO-TXPOWER (GE)	SSM-ST3 (DS1)
CPP-PEER-NO-RESP (MLMR)	LO-TXPOWER (ISC)	SSM-ST3 (E1)
CTNEQPT-MISMATCH (EQPT)	LO-TXPOWER (OCN)	SSM-ST3 (NE-SREF)
CTNEQPT-PBPROT (EQPT)	LO-TXPOWER (PPM)	SSM-ST3 (OCN)
CTNEQPT-PBWORK (EQPT)	LO-TXPOWER (TRUNK)	SSM-ST3 (TRUNK)
DATA-CRC (CE100T)	LPBKCRS (STSMON)	SSM-ST3E (BITS)
DATA-CRC (ML1000)	LPBKCRS (STSTRM)	SSM-ST3E (DS1)
DATA-CRC (ML100T)	LPBKDS1FE-CMD (DS1)	SSM-ST3E (E1)
DATA-CRC (MLFX)	LPBKDS3FEAC (DS3)	SSM-ST3E (NE-SREF)
DATAFLT (NE)	LPBKDS3FEAC-CMD (DS3)	SSM-ST3E (OCN)
DBOSYNC (NE)	LPBKFACILITY (CE1000)	SSM-ST3E (TRUNK)
DCU-LOSS-FAIL (OTS)	LPBKFACILITY (CE100T)	SSM-ST4 (BITS)
DS3-MISM (DS3)	LPBKFACILITY (CEMR)	SSM-ST4 (DS1)
DSP-COMM-FAIL (TRUNK)	LPBKFACILITY (DS1)	SSM-ST4 (E1)
DSP-FAIL (TRUNK)	LPBKFACILITY (DS3)	SSM-ST4 (NE-SREF)
DUP-IPADDR (NE)	LPBKFACILITY (E1)	SSM-ST4 (OCN)
DUP-NODENAME (NE)	LPBKFACILITY (EC1)	SSM-ST4 (TRUNK)
DUP-SHELF-ID (SHELF)	LPBKFACILITY (ESCON)	SSM-STU (BITS)
EFM-RFI-CE (MLMR)	LPBKFACILITY (FC)	SSM-STU (DS1)
EFM-RFI-DG (MLMR)	LPBKFACILITY (FCMR)	SSM-STU (E1)
EFM-RFI-LF (MLMR)	LPBKFACILITY (G1000)	SSM-STU (NE-SREF)
EHIBATVG (PWR)	LPBKFACILITY (GE)	SSM-STU (OCN)
ELWBATVG (PWR)	LPBKFACILITY (ISC)	SSM-STU (TRUNK)
ENCAP-MISMATCH-P (STSTRM)	LPBKFACILITY (MLMR)	SSM-TNC (BITS)
EOC (OCN)	LPBKFACILITY (OCN)	SSM-TNC (NE-SREF)

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

EOC (TRUNK)	LPBKFACILITY (TRUNK)	SSM-TNC (OCN)
EOC-L (OCN)	LPBKTERMINAL (CE1000)	SSM-TNC (TRUNK)
EOC-L (TRUNK)	LPBKTERMINAL (CE100T)	STS-SQUELCH-L (OCN)
EQPT (AICI-AEP)	LPBKTERMINAL (CEMR)	SW-MISMATCH (EQPT)
EQPT (AICI-AIE)	LPBKTERMINAL (DS1)	SWMTXMOD-PROT (EQPT)
EQPT (EQPT)	LPBKTERMINAL (DS3)	SWMTXMOD-WORK (EQPT)
EQPT (PPM)	LPBKTERMINAL (E1)	SWTOPRI (EXT-SREF)
EQPT-DIAG (EQPT)	LPBKTERMINAL (EC1)	SWTOPRI (NE-SREF)
EQPT-MISS (FAN)	LPBKTERMINAL (ESCON)	SWTOSEC (EXT-SREF)
ERFI-P-CONN (STSMON)	LPBKTERMINAL (FC)	SWTOSEC (NE-SREF)
ERFI-P-CONN (STSTRM)	LPBKTERMINAL (FCMR)	SWTOTHIRD (EXT-SREF)
ERFI-P-PAYLD (STSMON)	LPBKTERMINAL (G1000)	SWTOTHIRD (NE-SREF)
ERFI-P-PAYLD (STSTRM)	LPBKTERMINAL (GE)	SYNC-FREQ (BITS)
ERFI-P-SRVR (STSMON)	LPBKTERMINAL (ISC)	SYNC-FREQ (DS1)
ERFI-P-SRVR (STSTRM)	LPBKTERMINAL (MLMR)	SYNC-FREQ (E1)
ERROR-CONFIG (EQPT)	LPBKTERMINAL (OCN)	SYNC-FREQ (OCN)
ETH-LINKLOSS (NE)	LPBKTERMINAL (TRUNK)	SYNC-FREQ (TRUNK)
E-W-MISMATCH (OCN)	LWBATVG (PWR)	SYNCLOSS (FC)
EXCCOL (EQPT)	MAN-REQ (EQPT)	SYNCLOSS (FCMR)
EXERCISE-RING-FAIL (OCN)	MAN-REQ (ML1000)	SYNCLOSS (GE)
EXERCISE-SPAN-FAIL (OCN)	MAN-REQ (ML100T)	SYNCLOSS (ISC)
EXT (ENVALRM)	MAN-REQ (MLFX)	SYNCLOSS (TRUNK)
EXTRA-TRAF-PREEMPT (OCN)	MAN-REQ (MLMR)	SYNCPRI (EXT-SREF)
FAILTOSW (2R)	MAN-REQ (STSMON)	SYNCPRI (NE-SREF)
FAILTOSW (EQPT)	MAN-REQ (VT-MON)	SYNCSEC (EXT-SREF)
FAILTOSW (ESCON)	MANRESET (EQPT)	SYNCSEC (NE-SREF)
FAILTOSW (FC)	MANSWTOINT (NE-SREF)	SYNCTHIRD (EXT-SREF)
FAILTOSW (GE)	MANSWTOPRI (EXT-SREF)	SYNCTHIRD (NE-SREF)
FAILTOSW (ISC)	MANSWTOPRI (NE-SREF)	SYSBOOT (NE)
FAILTOSW (OCN)	MANSWTOSEC (EXT-SREF)	TEMP-MISM (NE)
FAILTOSW (OTS)	MANSWTOSEC (NE-SREF)	TIM (OCN)
FAILTOSW (TRUNK)	MANSWTOTHIRD (EXT-SREF)	TIM (TRUNK)
FAILTOSW-PATH (STSMON)	MANSWTOTHIRD (NE-SREF)	TIM-MON (OCN)
FAILTOSW-PATH (VT-MON)	MANUAL-REQ-RING (OCN)	TIM-MON (TRUNK)
FAILTOSWR (OCN)	MANUAL-REQ-SPAN (2R)	TIM-P (STSMON)
FAILTOSWS (OCN)	MANUAL-REQ-SPAN (EC1)	TIM-P (STSTRM)
FAN (FAN)	MANUAL-REQ-SPAN (ESCON)	TIM-S (EC1)

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

FAPS (FCMR)	MANUAL-REQ-SPAN (FC)	TIM-S (OCN)
FAPS (TRUNK)	MANUAL-REQ-SPAN (GE)	TIM-V (VT-MON)
FAPS-CONFIG-MISMATCH (EQPT)	MANUAL-REQ-SPAN (ISC)	TIM-V (VT-TERM)
FC-DE-NES (FC)	MANUAL-REQ-SPAN (OCN)	TPTFAIL (CE1000)
FC-DE-NES (FCMR)	MANUAL-REQ-SPAN (OTS)	TPTFAIL (CE100T)
FC-DE-NES (TRUNK)	MANUAL-REQ-SPAN (TRUNK)	TPTFAIL (CEMR)
FC-NO-CREDITS (FC)	MAX-STATIONS (RPRIF)	TPTFAIL (FCMR)
FC-NO-CREDITS (FCMR)	MCAST-MAC-TABLE-FULL (EQPT)	TPTFAIL (G1000)
FC-NO-CREDITS (TRUNK)	MEA (AIP)	TPTFAIL (ML1000)
FDI (OCH)	MEA (BIC)	TPTFAIL (ML100T)
FDI (OCH-TERM)	MEA (EQPT)	TPTFAIL (MLFX)
FE-AIS (DS3)	MEA (FAN)	TPTFAIL (MLMR)
FEC-MISM (TRUNK)	MEA (PPM)	TRAIL-SIGNAL-FAIL (OCH)
FE-DS1-MULTLOS (DS3)	MEA (SHELF)	TRAIL-SIGNAL-FAIL (TRUNK)
FE-DS1-NSA (DS3)	MEM-GONE (EQPT)	TRMT (DS1)
FE-DS1-SA (DS3)	MEM-LOW (EQPT)	TRMT (E1)
FE-DS1-SNGLLOS (DS3)	MFGMEM (AICI-AEP)	TRMT-MISS (DS1)
FE-DS3-NSA (DS3)	MFGMEM (AICI-AIE)	TRMT-MISS (E1)
FE-DS3-SA (DS3)	MFGMEM (AIP)	TX-AIS (DS1)
FE-EQPT-NSA (DS3)	MFGMEM (BPLANE)	TX-AIS (DS3)
FE-FRCDWKS WBK-SPAN (OCN)	MFGMEM (FAN)	TX-AIS (E1)
FE-FRCDWKS WPR-RING (EC1)	MFGMEM (PPM)	TX-IDLE (DS1)
FE-FRCDWKS WPR-RING (OCN)	MS-DEG (E1)	TX-LOF (DS1)
FE-FRCDWKS WPR-SPAN (OCN)	MS-EXC (E1)	TX-LOF (E1)
FE-IDLE (DS3)	MT-OCHNC (OTS)	TX-RAI (DS1)
FE-LOCKOUTOFPR-SPAN (OCN)	NO-CONFIG (EQPT)	TX-RAI (DS3)
FE-LOF (DS3)	NON-CISCO-PPM (PPM)	TX-RAI (E1)
FE-LOS (DS3)	OCHNC-INC (OCHNC-CONN)	UNC-WORD (TRUNK)
FE-MANWKS WBK-SPAN (OCN)	OCHTERM-INC (OCH-TERM)	UNEQ-P (STSMON)
FE-MANWKS WPR-RING (EC1)	ODUK-1-AIS-PM (TRUNK)	UNEQ-P (STSTRM)
FE-MANWKS WPR-RING (OCN)	ODUK-2-AIS-PM (TRUNK)	UNEQ-V (VT-MON)
FE-MANWKS WPR-SPAN (OCN)	ODUK-3-AIS-PM (TRUNK)	UNEQ-V (VT-TERM)
FEPRLF (OCN)	ODUK-4-AIS-PM (TRUNK)	UNQUAL-PPM (PPM)
FIBERTEMP-DEG (AOTS)	ODUK-AIS-PM (TRUNK)	UT-COMM-FAIL (TRUNK)
FORCED-REQ (EQPT)	ODUK-BDI-PM (TRUNK)	UT-FAIL (TRUNK)
FORCED-REQ (ML1000)	ODUK-LCK-PM (TRUNK)	VCG-DEG (VCG)
FORCED-REQ (ML100T)	ODUK-OCI-PM (TRUNK)	VCG-DOWN (VCG)

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

FORCED-REQ (MLFX)	ODUK-SD-PM (TRUNK)	VLAN-AIS (ETH)
FORCED-REQ (MLMR)	ODUK-SF-PM (TRUNK)	VOA-DISABLED (EQPT)
FORCED-REQ (STSMON)	ODUK-TIM-PM (TRUNK)	VOA-HDEG (AOTS)
FORCED-REQ (VT-MON)	OOU-TPT (STSTRM)	VOA-HDEG (OCH)
FORCED-REQ-RING (OCN)	OOU-TPT (VT-TERM)	VOA-HDEG (OMS)
FORCED-REQ-SPAN (2R)	OPEN-SLOT (EQPT)	VOA-HDEG (OTS)
FORCED-REQ-SPAN (EC1)	OPWR-HDEG (AOTS)	VOA-HFAIL (AOTS)
FORCED-REQ-SPAN (ESCON)	OPWR-HDEG (OCH)	VOA-HFAIL (OCH)
FORCED-REQ-SPAN (FC)	OPWR-HDEG (OCH-TERM)	VOA-HFAIL (OMS)
FORCED-REQ-SPAN (GE)	OPWR-HDEG (OMS)	VOA-HFAIL (OTS)
FORCED-REQ-SPAN (ISC)	OPWR-HDEG (OTS)	VOA-LDEG (AOTS)
FORCED-REQ-SPAN (OCN)	OPWR-HFAIL (AOTS)	VOA-LDEG (OCH)
FORCED-REQ-SPAN (OTS)	OPWR-HFAIL (OCH)	VOA-LDEG (OMS)
FORCED-REQ-SPAN (TRUNK)	OPWR-HFAIL (OMS)	VOA-LDEG (OTS)
FP-LINK-LOSS (EQPT)	OPWR-HFAIL (OTS)	VOA-LFAIL (AOTS)
FRCDSWTOINT (NE-SREF)	OPWR-LDEG (AOTS)	VOA-LFAIL (OCH)
FRCDSWTOPRI (EXT-SREF)	OPWR-LDEG (OCH)	VOA-LFAIL (OMS)
FRCDSWTOPRI (NE-SREF)	OPWR-LDEG (OCH-TERM)	VOA-LFAIL (OTS)
FRCDSWTOSEC (EXT-SREF)	OPWR-LDEG (OMS)	VOLT-MISM (PWR)
FRCDSWTOSEC (NE-SREF)	OPWR-LDEG (OTS)	VT-SQUELCH-L (OCN)
FRCDSWTOTHIRD (EXT-SREF)	OPWR-LFAIL (AOTS)	WIZARD-IS-RUNNING (OTS)
FRCDSWTOTHIRD (NE-SREF)	OPWR-LFAIL (OCH)	WKS WPR (2R)
FRNGSYNC (NE-SREF)	OPWR-LFAIL (OCH-TERM)	WKS WPR (EQPT)
FSTSYNC (NE-SREF)	OPWR-LFAIL (OMS)	WKS WPR (ESCON)
FTA-MISMATCH (EQPT)	OPWR-LFAIL (OTS)	WKS WPR (FC)
FULLPASSTHR-BI (OCN)	OSRION (AOTS)	WKS WPR (GE)
GAIN-HDEG (AOTS)	OSRION (OTS)	WKS WPR (ISC)
GAIN-HFAIL (AOTS)	OTUK-AIS (TRUNK)	WKS WPR (OCN)
GAIN-LDEG (AOTS)	OTUK-BDI (TRUNK)	WKS WPR (OTS)
GAIN-LFAIL (AOTS)	OTUK-IAE (TRUNK)	WKS WPR (STSMON)
GCC-EOC (TRUNK)	OTUK-LOF (TRUNK)	WKS WPR (VT-MON)
GE-OOSYNC (FC)	OTUK-SD (TRUNK)	WORK-QUEUE-FULL (EQPT)
GE-OOSYNC (GE)	OTUK-SF (TRUNK)	WTR (2R)
GE-OOSYNC (ISC)	OTUK-TIM (TRUNK)	WTR (EC1)
GE-OOSYNC (TRUNK)	OUT-OF-SYNC (FC)	WTR (EQPT)
GFP-CSF (CE1000)	OUT-OF-SYNC (GE)	WTR (ESCON)
GFP-CSF (CE100T)	OUT-OF-SYNC (ISC)	WTR (FC)

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

GFP-CSF (CEMR)	OUT-OF-SYNC (TRUNK)	WTR (GE)
GFP-CSF (FCMR)	PARAM-MISM (AOTS)	WTR (ISC)
GFP-CSF (GFP-FAC)	PARAM-MISM (OCH)	WTR (ML1000)
GFP-CSF (ML1000)	PARAM-MISM (OCH-TERM)	WTR (ML100T)
GFP-CSF (ML100T)	PARAM-MISM (OMS)	WTR (MLFX)
GFP-CSF (MLFX)	PARAM-MISM (OTS)	WTR (MLMR)
GFP-CSF (MLMR)	PDI-P (STSMON)	WTR (OCN)
GFP-DE-MISMATCH (FCMR)	PDI-P (STSTRM)	WTR (STSMON)
GFP-DE-MISMATCH (GFP-FAC)	PEER-NORESPONSE (MLMR)	WTR (TRUNK)
GFP-EX-MISMATCH (CE1000)	PLM-P (STSMON)	WTR (VT-MON)
GFP-EX-MISMATCH (FCMR)	PLM-P (STSTRM)	WVL-MISMATCH (TRUNK)

2.3 Alarm Logical Objects

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

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



Note

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

Table 2-7 Alarm Logical Object Type Definitions

Logical Object	Definition
2R	Reshape and retransmit (used for transponder [TXP] cards).
AICI-AEP	Alarm Interface Controller–International/alarm expansion panel. A combination term that refers to this platform’s AIC-I card.
AICI-AIE	Alarm Interface Controller-International/Alarm Interface Extension. A combination term that refers to this platform's AIC-I card.
AIP	Alarm Interface Panel.
AOTS	Amplified optical transport section. For information about AOTS alarms, refer to the “Alarm Troubleshooting” chapter in the <i>Cisco ONS 15454 DWDM Troubleshooting Guide</i> .
BIC	Backplane interface connector.
BITS	Building integrated timing supply incoming references (BITS-1, BITS-2).

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

Logical Object	Definition
BPLANE	The backplane.
CE1000	CE-1000-4 card.
CE100T	CE-100T-8 card.
CEMR	CE-MR-10 card.
CTRL	Control channel.
DS1	A DS-1 line on a DS-1 or DS-3 electrical card (DS1-14, DS3N-12E, DS3XM-6, DS3XM-12).
DS3	A DS-3 line on a DS3-12, DS3N-12, DS3-12E, DS3XM-6, DS3XM-12, DS3/EC1-48 card.
E1	An E1 line on a DS1/E1-56 card.
E1000F	An E1000 Ethernet card (E1000-2, E1000-2G).
E100T	An E100 Ethernet card (E100T-12, E100T-G).
EC1	Any EC-1 port (including EC1-12 card ports).
ENVALRM	An environmental alarm port.
EQPT	A card, its physical objects, and its logical objects as they are located in any of the eight noncommon card slots. The EQPT object is used for alarms that refer to the card itself and all other objects on the card including ports, lines, synchronous transport signals (STS), and virtual tributaries (VT).
ESCON	Enterprise System Connection fiber optic technology, referring to the following TXP cards: TXP_MR_2.5G, TXPP_MR_2.5G. For more information about ESCON alarms, refer to the “Alarm Troubleshooting” chapter in the <i>Cisco ONS 15454 DWDM Troubleshooting Guide</i> .
EXT-SREF	BITS outgoing references (SYNC-BITS1, SYNC-BITS2).
FAN	Fan-tray assembly.
FC	Fibre channel data transfer architecture, referring to the following muxponder (MXP) or TXP cards: MXP_MR_2.5G, MXPP_MR_2.5G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E. For more information about FC alarms, refer to the “Alarm Troubleshooting” chapter in the <i>Cisco ONS 15454 DWDM Troubleshooting Guide</i> .
FCMR	An FC_MR-4 Fibre Channel card.
FUDC	SONET F1 byte user data channel for ONS 15454 ML-Series Ethernet cards.
G1000	A G-Series Ethernet card.
GE	Gigabit Ethernet, referring to the following MXP or TXP cards: MXP_MR_2.5G, MXPP_MR_2.5G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, TXP_MR_10G.
GFP-FAC	Generic framing procedure facility port, referring to all MXP and TXP cards.
ISC	Inter-service channel, referring to TXPP_MR_2.5G or TXP_MR_2.5G cards. For more information about ISC alarms, refer to the “Alarm Troubleshooting” chapter in the <i>Cisco ONS 15454 DWDM Troubleshooting Guide</i> .
ML1000	An ML1000 Ethernet card (ML1000-2).

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

Logical Object	Definition
ML100T	An ML100 Ethernet card (ML100T-12).
MLFX	An ML100X-8 Ethernet card.
MLMR	An ML-MR-10 Ethernet card.
MSUDC	Multiplex section user data channel.
NE	The entire network element.
NE-SREF	The timing status of the NE.
OCH	The optical channel, referring to dense wavelength division multiplexing (DWDM) cards. For more information about OCH alarms, refer to the “Alarm Troubleshooting” chapter in the <i>Cisco ONS 15454 DWDM Troubleshooting Guide</i> .
OCHNC-CONN	The optical channel network connection, referring to DWDM cards. For more information about OCHNC-CONN alarms, refer to the “Alarm Troubleshooting” chapter in the <i>Cisco ONS 15454 DWDM Troubleshooting Guide</i> .
OCH-TERM	The optical channel termination node, referring to DWDM cards. For more information about most of the alarms on this object, refer to the “Alarm Troubleshooting” chapter of the <i>Cisco ONS 15454 DWDM Troubleshooting Guide</i>. Note The network element reports alarms or conditions on ingress ports of the card. Alarms detected at the internal ports (TERM side) will be ingress mapped to the MON side. The alarm profile entities of OCH-TERM, if available, should be changed to the same severity as the customized severity for a specific OCH-TERM alarm.
OCN	An OC-N line on any OC-N card.
OMS	Optical multiplex section.
OSC-RING	Optical service channel ring. For more information about OSC-RING alarms, refer to the “Alarm Troubleshooting” chapter in the <i>Cisco ONS 15454 DWDM Troubleshooting Guide</i> .
OTS	Optical transport section. For more information about OTS alarms, refer to the “Alarm Troubleshooting” chapter in the <i>Cisco ONS 15454 DWDM Troubleshooting Guide</i> .
PPM	Pluggable port module (PPM), referring to OC192-XFP, MXP, TXP, and MRC cards. For more information about PPM alarms, refer to the “Alarm Troubleshooting” chapter in the <i>Cisco ONS 15454 DWDM Troubleshooting Guide</i> .
PWR	Power equipment.
RPRIF	Interface for Resilient Packet Ring technology as defined in IEEE 802.17b. Also called RPR-IEEE.
SHELF	The shelf assembly. For more information about most of the alarms on this object, refer to the “Alarm Troubleshooting” chapter of the <i>Cisco ONS 15454 DWDM Troubleshooting Guide</i> .

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

Logical Object	Definition
STSMON	STS alarm detection at the monitor point (upstream from the cross-connect). Note The network element reports alarms or conditions on ingress ports of the card. Alarms detected at the internal ports (TERM side) will be ingress mapped to the MON side. The alarm profile entities of STSMON, if available, should be changed to the same severity as the customized severity for a specific STS alarm.
STSTRM	STS alarm detection at termination (downstream from the cross-connect). Note The network element reports alarms or conditions on ingress ports of the card. Alarms detected at the internal ports (TERM side) will be ingress mapped to the MON side. The alarm profile entities of STSTRM, if available, should be changed to the same severity as the customized severity for a specific STS alarm.
TLINK	Traffic engineering (TE) link correlation.
TRUNK	The optical or DWDM card carrying the high-speed signal; referring to MXP or TXP cards. For more information about TRUNK alarms, refer to the “Alarm Troubleshooting” chapter in the <i>Cisco ONS 15454 DWDM Troubleshooting Guide</i> .
VCG	A virtual concatenation group of VTs.
VT-MON	VT1 alarm detection at the monitor point (upstream from the cross-connect). Note The network element reports alarms or conditions on ingress ports of the card. Alarms detected at the internal ports (TERM side) will be ingress mapped to the MON side. The alarm profile entities of VT-MON, if available, should be changed to the same severity as the customized severity for a specific VT alarm.
VT-TERM	VT1 alarm detection at termination (downstream from the cross-connect). Note The network element reports alarms or conditions on ingress ports of the card. Alarms detected at the internal ports (TERM side) will be ingress mapped to the MON side. The alarm profile entities of VT-TERM, if available, should be changed to the same severity as the customized severity for a specific VT alarm.

2.4 Alarm List by Logical Object Type

Table 2-8 lists all ONS 15454 alarms and logical objects as they are given in the system alarm profile. The list entries are organized by logical object name and then by alarm or condition name. Where appropriate, the alarm entries also contain troubleshooting procedures.



Note

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

**Note**

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

Table 2-8 Alarm List by Logical Object in Alarm Profile

2R: ALS (NA)	FC: CARLOSS (MJ)	OCN: RING-ID-MIS (MJ)
2R: AS-CMD (NA)	FC: FAILTOSW (NA)	OCN: RING-MISMATCH (MJ)
2R: AS-MT (NA)	FC: FC-DE-NES (MJ)	OCN: RING-SW-EAST (NA)
2R: FAILTOSW (NA)	FC: FC-NO-CREDITS (MJ)	OCN: RING-SW-WEST (NA)
2R: FORCED-REQ-SPAN (NA)	FC: FORCED-REQ-SPAN (NA)	OCN: SD-L (NA)
2R: HI-LASERBIAS (MN)	FC: GE-OOSYNC (CR)	OCN: SF-L (NA)
2R: HI-RXPOWER (MN)	FC: HI-LASERBIAS (MN)	OCN: SPAN-SW-EAST (NA)
2R: HI-TXPOWER (MN)	FC: HI-RXPOWER (MN)	OCN: SPAN-SW-WEST (NA)
2R: LO-RXPOWER (MN)	FC: HI-TXPOWER (MN)	OCN: SQUELCH (NA)
2R: LO-TXPOWER (MN)	FC: LO-RXPOWER (MN)	OCN: SQUELCHED (NA)
2R: LOCKOUT-REQ (NA)	FC: LO-TXPOWER (MN)	OCN: SSM-DUS (NA)
2R: LOS (CR)	FC: LOCKOUT-REQ (NA)	OCN: SSM-FAIL (MN)
2R: MANUAL-REQ-SPAN (NA)	FC: LPBKFACILITY (NA)	OCN: SSM-LNC (NA)
2R: SQUELCHED (NA)	FC: LPBKTERMINAL (NA)	OCN: SSM-OFF (NA)
2R: WKSWPR (NA)	FC: MANUAL-REQ-SPAN (NA)	OCN: SSM-PRC (NA)
2R: WTR (NA)	FC: OUT-OF-SYNC (MJ)	OCN: SSM-PRS (NA)
AICI-AEP: EQPT (CR)	FC: SIGLOSS (MJ)	OCN: SSM-RES (NA)
AICI-AEP: MFGMEM (CR)	FC: SQUELCHED (NA)	OCN: SSM-SDH-TN (NA)
AICI-AIE: EQPT (CR)	FC: SYNCLOSS (MJ)	OCN: SSM-SETS (NA)
AICI-AIE: MFGMEM (CR)	FC: WKSWPR (NA)	OCN: SSM-SMC (NA)
AIP: INVMACADR (MJ)	FC: WTR (NA)	OCN: SSM-ST2 (NA)
AIP: MEA (CR)	FCMR: AS-CMD (NA)	OCN: SSM-ST3 (NA)
AIP: MFGMEM (CR)	FCMR: AS-MT (NA)	OCN: SSM-ST3E (NA)
AOTS: ALS (NA)	FCMR: FAPS (NA)	OCN: SSM-ST4 (NA)
AOTS: AMPLI-INIT (NA)	FCMR: FC-DE-NES (MJ)	OCN: SSM-STU (NA)
AOTS: APC-CORR-SKIPPED (MN)	FCMR: FC-NO-CREDITS (MJ)	OCN: SSM-TNC (NA)
AOTS: APC-DISABLED (NA)	FCMR: GFP-CSF (MJ)	OCN: STS-SQUELCH-L (NA)
AOTS: APC-OUT-OF-RANGE (MN)	FCMR: GFP-DE-MISMATCH (MJ)	OCN: SYNC-FREQ (NA)
AOTS: APC-WRONG-GAIN (NA)	FCMR: GFP-EX-MISMATCH (MJ)	OCN: TIM (CR)
AOTS: AS-CMD (NA)	FCMR: GFP-LFD (MJ)	OCN: TIM-MON (MN)
AOTS: AS-MT (NA)	FCMR: GFP-NO-BUFFERS (MJ)	OCN: TIM-S (CR)
AOTS: CASETEMP-DEG (MN)	FCMR: GFP-UP-MISMATCH (MJ)	OCN: VT-SQUELCH-L (NA)
AOTS: FIBERTEMP-DEG (MN)	FCMR: LPBKFACILITY (NA)	OCN: WKSWPR (NA)
AOTS: GAIN-HDEG (MN)	FCMR: LPBKTERMINAL (NA)	OCN: WTR (NA)

Table 2-8 Alarm List by Logical Object in Alarm Profile (continued)

AOTS: GAIN-HFAIL (CR)	FCMR: PORT-MISMATCH (NA)	OMS: APC-CORR-SKIPPED (MN)
AOTS: GAIN-LDEG (MN)	FCMR: SIGLOSS (MJ)	OMS: APC-DISABLED (NA)
AOTS: GAIN-LFAIL (CR)	FCMR: SYNCLOSS (MJ)	OMS: APC-OUT-OF-RANGE (MN)
AOTS: LASER-APR (NA)	FCMR: TPTFAIL (MJ)	OMS: AS-CMD (NA)
AOTS: LASERBIAS-DEG (MN)	FUDC: AIS (NR)	OMS: AS-MT (NA)
AOTS: LASERBIAS-FAIL (MJ)	FUDC: LOS (MN)	OMS: LOS-O (MN)
AOTS: LASERTEMP-DEG (MN)	G1000: AS-CMD (NA)	OMS: LOS-P (CR)
AOTS: OPWR-HDEG (MN)	G1000: AS-MT (NA)	OMS: OPWR-HDEG (MN)
AOTS: OPWR-HFAIL (CR)	G1000: CARLOSS (MJ)	OMS: OPWR-HFAIL (CR)
AOTS: OPWR-LDEG (MN)	G1000: LPBKFACILITY (NA)	OMS: OPWR-LDEG (MN)
AOTS: OPWR-LFAIL (CR)	G1000: LPBKTERMINAL (NA)	OMS: OPWR-LFAIL (CR)
AOTS: OSRION (NA)	G1000: TPTFAIL (MJ)	OMS: PARAM-MISM (NA)
AOTS: PARAM-MISM (NA)	GE: ALS (NA)	OMS: PMI (NA)
AOTS: VOA-HDEG (MN)	GE: AS-CMD (NA)	OMS: VOA-HDEG (MN)
AOTS: VOA-HFAIL (CR)	GE: AS-MT (NA)	OMS: VOA-HFAIL (CR)
AOTS: VOA-LDEG (MN)	GE: CARLOSS (MJ)	OMS: VOA-LDEG (MN)
AOTS: VOA-LFAIL (CR)	GE: FAILTOSW (NA)	OMS: VOA-LFAIL (CR)
BIC: MEA (CR)	GE: FORCED-REQ-SPAN (NA)	OSC-RING: RING-ID-MIS (MJ)
BITS: AIS (NR)	GE: GE-OOSYNC (CR)	OTS: APC-CORR-SKIPPED (MN)
BITS: BPV (MN)	GE: HI-LASERBIAS (MN)	OTS: APC-DISABLED (NA)
BITS: HI-CCVOLT (NA)	GE: HI-RXPOWER (MN)	OTS: APC-OUT-OF-RANGE (MN)
BITS: LOF (MN)	GE: HI-TXPOWER (MN)	OTS: AS-CMD (NA)
BITS: LOS (MN)	GE: LMP-FAIL (MN)	OTS: AS-MT (NA)
BITS: SSM-DUS (NA)	GE: LMP-SD (MN)	OTS: AWG-DEG (MN)
BITS: SSM-FAIL (MN)	GE: LMP-SF (MN)	OTS: AWG-FAIL (CR)
BITS: SSM-LNC (NA)	GE: LMP-UNALLOC (NA)	OTS: AWG-OVERTEMP (CR)
BITS: SSM-OFF (NA)	GE: LO-RXPOWER (MN)	OTS: AWG-WARM-UP (NA)
BITS: SSM-PRC (NA)	GE: LO-TXPOWER (MN)	OTS: DCU-LOSS-FAIL (MN)
BITS: SSM-PRS (NA)	GE: LOCKOUT-REQ (NA)	OTS: FAILTOSW (NA)
BITS: SSM-RES (NA)	GE: LPBKFACILITY (NA)	OTS: FORCED-REQ-SPAN (NA)
BITS: SSM-SDH-TN (NA)	GE: LPBKTERMINAL (NA)	OTS: LASER-APR (NA)
BITS: SSM-SETS (NA)	GE: MANUAL-REQ-SPAN (NA)	OTS: LASERBIAS-DEG (MN)
BITS: SSM-SMC (NA)	GE: OUT-OF-SYNC (MJ)	OTS: LOCKOUT-REQ (NA)
BITS: SSM-ST2 (NA)	GE: SIGLOSS (MJ)	OTS: LOS (CR)
BITS: SSM-ST3 (NA)	GE: SQUELCHED (NA)	OTS: LOS-O (MN)
BITS: SSM-ST3E (NA)	GE: SYNCLOSS (MJ)	OTS: LOS-P (CR)
BITS: SSM-ST4 (NA)	GE: WKSWPR (NA)	OTS: LOS-RAMAN (CR)

Table 2-8 Alarm List by Logical Object in Alarm Profile (continued)

BITS: SSM-STU (NA)	GE: WTR (NA)	OTS: MANUAL-REQ-SPAN (NA)
BITS: SSM-TNC (NA)	GFP-FAC: AS-CMD (NA)	OTS: MT-OCHNC (NA)
BITS: SYNC-FREQ (NA)	GFP-FAC: AS-MT (NA)	OTS: OPWR-HDEG (MN)
BPLANE: AS-CMD (NA)	GFP-FAC: GFP-CSF (MJ)	OTS: OPWR-HFAIL (CR)
BPLANE: MFGMEM (CR)	GFP-FAC: GFP-DE-MISMATCH (MJ)	OTS: OPWR-LDEG (MN)
CE1000: AS-CMD (NA)	GFP-FAC: GFP-EX-MISMATCH (MJ)	OTS: OPWR-LFAIL (CR)
CE1000: AS-MT (NA)	GFP-FAC: GFP-LFD (MJ)	OTS: OSRION (NA)
CE1000: CARLOSS (MJ)	GFP-FAC: GFP-NO-BUFFERS (MJ)	OTS: PARAM-MISM (NA)
CE1000: GFP-CSF (MJ)	GFP-FAC: GFP-UP-MISMATCH (MJ)	OTS: PMI (NA)
CE1000: GFP-EX-MISMATCH (MJ)	ISC: ALS (NA)	OTS: PWR-PROT-ON (MJ)
CE1000: GFP-LFD (MJ)	ISC: AS-CMD (NA)	OTS: RAMAN-SPAN-NOT-TUNED (NA)
CE1000: GFP-UP-MISMATCH (MJ)	ISC: AS-MT (NA)	OTS: RLS (NA)
CE1000: LPBKFACILITY (NA)	ISC: CARLOSS (MJ)	OTS: SH-IL-VAR-DEG-HIGH (MN)
CE1000: LPBKTERMINAL (NA)	ISC: FAILTOSW (NA)	OTS: SH-IL-VAR-DEG-LOW (MN)
CE1000: TPTFAIL (MJ)	ISC: FORCED-REQ-SPAN (NA)	OTS: SHUTTER-OPEN (NA)
CE100T: AS-CMD (NA)	ISC: GE-OOSYNC (CR)	OTS: SPAN-NOT-MEASURED (NA)
CE100T: AS-MT (NA)	ISC: HI-LASERBIAS (MN)	OTS: SPANLEN-OUT-OF-RANGE (MN)
CE100T: CARLOSS (MJ)	ISC: HI-RXPOWER (MN)	OTS: VOA-HDEG (MN)
CE100T: DATA-CRC (MJ)	ISC: HI-TXPOWER (MN)	OTS: VOA-HFAIL (CR)
CE100T: GFP-CSF (MJ)	ISC: LO-RXPOWER (MN)	OTS: VOA-LDEG (MN)
CE100T: GFP-LFD (MJ)	ISC: LO-TXPOWER (MN)	OTS: VOA-LFAIL (CR)
CE100T: GFP-UP-MISMATCH (MJ)	ISC: LOCKOUT-REQ (NA)	OTS: WIZARD-IS-RUNNING (NA)
CE100T: LPBKFACILITY (NA)	ISC: LOS (CR)	OTS: WKSWPR (NA)
CE100T: LPBKTERMINAL (NA)	ISC: LPBKFACILITY (NA)	PPM: AS-CMD (NA)
CE100T: TPTFAIL (MJ)	ISC: LPBKTERMINAL (NA)	PPM: AS-MT (NA)
CEMR: AS-CMD (NA)	ISC: MANUAL-REQ-SPAN (NA)	PPM: EQPT (CR)
CEMR: AS-MT (NA)	ISC: OUT-OF-SYNC (NA)	PPM: HI-LASERBIAS (MN)
CEMR: CARLOSS (MJ)	ISC: SIGLOSS (MJ)	PPM: HI-LASERTEMP (MN)
CEMR: GFP-CSF (MJ)	ISC: SQUELCHED (NA)	PPM: HI-TXPOWER (MN)
CEMR: GFP-LFD (MJ)	ISC: SYNCLOSS (MJ)	PPM: IMPROPRMVL (CR)
CEMR: GFP-UP-MISMATCH (MJ)	ISC: WKSWPR (NA)	PPM: LO-LASERBIAS (MN)
CEMR: LPBKFACILITY (NA)	ISC: WTR (NA)	PPM: LO-LASERTEMP (MN)
CEMR: LPBKTERMINAL (NA)	ML1000: AS-CMD (NA)	PPM: LO-TXPOWER (MN)
CEMR: PORT-MISMATCH (MJ)	ML1000: AS-MT (NA)	PPM: MEA (CR)
CEMR: TPTFAIL (MJ)	ML1000: AUTONEG-RFI (MJ)	PPM: MFGMEM (CR)
CTRL: LMP-FAIL (MN)	ML1000: CARLOSS (MJ)	PPM: NON-CISCO-PPM (NR)

Table 2-8 Alarm List by Logical Object in Alarm Profile (continued)

DS1: AIS (NR)	ML1000: DATA-CRC (MJ)	PPM: PROV-MISMATCH (MN)
DS1: AS-CMD (NA)	ML1000: FORCED-REQ (NA)	PPM: UNQUAL-PPM (NR)
DS1: AS-MT (NA)	ML1000: GFP-CSF (MJ)	PWR: AS-CMD (NA)
DS1: BERT-ENBL (NR)	ML1000: GFP-LFD (MJ)	PWR: BAT-FAIL (MJ)
DS1: BERT-SYNC-FAIL (NR)	ML1000: GFP-UP-MISMATCH (MJ)	PWR: EHIBATVG (MJ)
DS1: IDLE (NA)	ML1000: LINK-KEEPALIVE (CR)	PWR: ELWBATVG (MJ)
DS1: LOF (MJ)	ML1000: MAN-REQ (NA)	PWR: HIBATVG (MJ)
DS1: LOS (MJ)	ML1000: RPR-SD (NA)	PWR: LWBATVG (MJ)
DS1: LPBKDS1FE-CMD (NA)	ML1000: RPR-SF (NA)	PWR: VOLT-MISM (NA)
DS1: LPBKFACILITY (NA)	ML1000: RPR-SPAN-MISMATCH (MJ)	RPR: CPP-INCAPABLE (NA)
DS1: LPBKTERMINAL (NA)	ML1000: RPRW (NA)	RPRIF: MAX-STATIONS (MJ)
DS1: RAI (NA)	ML1000: TPTFAIL (MJ)	RPRIF: RSV-RT-EXCD-RINGLETO (MJ)
DS1: RCVR-MISS (MJ)	ML1000: WTR (NA)	RPRIF: RSV-RT-EXCD-RINGLETO1 (MJ)
DS1: SD (NA)	ML100T: AS-CMD (NA)	RPRIF: RPR-PASSTHR (NA)
DS1: SF (NA)	ML100T: AS-MT (NA)	RPRIF: RPR-PEER-MISS (MJ)
DS1: SSM-DUS (NA)	ML100T: CARLOSS (MJ)	RPRIF: RPR-PROT-ACTIVE (NA)
DS1: SSM-FAIL (MN)	ML100T: DATA-CRC (MJ)	RPRIF: RPR-PROT-CONFIG-MISM (MJ)
DS1: SSM-OFF (NA)	ML100T: FORCED-REQ (NA)	RPRIF: RPR-RI-FAIL (MJ)
DS1: SSM-PRS (NA)	ML100T: GFP-CSF (MJ)	SHELF: APC-DISABLED (NA)
DS1: SSM-RES (NA)	ML100T: GFP-LFD (MJ)	SHELF: AS-CMD (NA)
DS1: SSM-SMC (NA)	ML100T: GFP-UP-MISMATCH (MJ)	SHELF: AS-MT (NA)
DS1: SSM-ST2 (NA)	ML100T: LINK-KEEPALIVE (CR)	SHELF: DUP-SHELF-ID (MJ)
DS1: SSM-ST3 (NA)	ML100T: MAN-REQ (NA)	SHELF: MEA (MJ)
DS1: SSM-ST3E (NA)	ML100T: RPR-SD (NA)	SHELF: SHELF-COMM-FAIL (MJ)
DS1: SSM-ST4 (NA)	ML100T: RPR-SF (NA)	STSMON: AIS-P (NR)
DS1: SSM-STU (NA)	ML100T: RPR-SPAN-MISMATCH (MJ)	STSMON: AUTOSW-AIS (NR)
DS1: SYNC-FREQ (NA)	ML100T: RPRW (NA)	STSMON: AUTOSW-LOP (NA)
DS1: TRMT (MJ)	ML100T: TPTFAIL (MJ)	STSMON: AUTOSW-PDI (NA)
DS1: TRMT-MISS (MJ)	ML100T: WTR (NA)	STSMON: AUTOSW-SDBER (NA)
DS1: TX-AIS (NR)	MLFX: AS-CMD (NA)	STSMON: AUTOSW-SFBER (NA)
DS1: TX-IDLE (NA)	MLFX: AS-MT (NA)	STSMON: AUTOSW-UNEQ (NA)
DS1: TX-LOF (NR)	MLFX: CARLOSS (MJ)	STSMON: ERFI-P-CONN (NR)
DS1: TX-RAI (NA)	MLFX: DATA-CRC (MJ)	STSMON: ERFI-P-PAYLD (NR)

Table 2-8 Alarm List by Logical Object in Alarm Profile (continued)

DS3: AIS (NR)	MLFX: FORCED-REQ (NA)	STSMON: ERFI-P-SRVR (NR)
DS3: AS-CMD (NA)	MLFX: GFP-CSF (MJ)	STSMON: FAILTOSW-PATH (NA)
DS3: AS-MT (NA)	MLFX: GFP-LFD (MJ)	STSMON: FORCED-REQ (NA)
DS3: BERT-ENBL (NR)	MLFX: GFP-UP-MISMATCH (MJ)	STSMON: LOCKOUT-REQ (NA)
DS3: BERT-SYNC-FAIL (NR)	MLFX: LINK-KEEPALIVE (CR)	STSMON: LOM (CR)
DS3: DS3-MISM (NA)	MLFX: MAN-REQ (NA)	STSMON: LOP-P (CR)
DS3: FE-AIS (NA)	MLFX: RPR-SD (NA)	STSMON: LPBKCRS (NA)
DS3: FE-DS1-MULTLOS (NA)	MLFX: RPR-SF (NA)	STSMON: MAN-REQ (NA)
DS3: FE-DS1-NSA (NA)	MLFX: RPR-SPAN-MISMATCH (MJ)	STSMON: PDI-P (NA)
DS3: FE-DS1-SA (NA)	MLFX: RPRW (NA)	STSMON: PLM-P (CR)
DS3: FE-DS1-SNGLLOS (NA)	MLFX: TPTFAIL (MJ)	STSMON: RFI-P (NR)
DS3: FE-DS3-NSA (NA)	MLFX: WTR (NA)	STSMON: ROLL (NA)
DS3: FE-DS3-SA (NA)	MLMR: AS-CMD (NA)	STSMON: ROLL-PEND (NA)
DS3: FE-EQPT-NSA (NA)	MLMR: AS-MT (NA)	STSMON: SD-P (NA)
DS3: FE-IDLE (NA)	MLMR: CARLOSS (MJ)	STSMON: SF-P (NA)
DS3: FE-LOF (NA)	MLMR: CPP-INCAPABLE (NA)	STSMON: TIM-P (MN)
DS3: FE-LOS (NA)	MLMR: CPP-PEER-NO-RESP (MN)	STSMON: UNEQ-P (CR)
DS3: INC-ISD (NA)	MLMR: EFM-RFI-CE (MJ)	STSMON: WKSUPR (NA)
DS3: LOF (CR)	MLMR: EFM-RFI-DG (MJ)	STSMON: WTR (NA)
DS3: LOS (CR)	MLMR: EFM-RFI-LF (MJ)	STSTRM: AIS-P (NR)
DS3: LPBKDS3FEAC (NA)	MLMR: FORCED-REQ (NA)	STSTRM: AS-MT-OOG (NA)
DS3: LPBKDS3FEAC-CMD (NA)	MLMR: GFP-CSF (MJ)	STSTRM: ENCAP-MISMATCH-P (CR)
DS3: LPBKFACILITY (NA)	MLMR: GFP-LFD (MJ)	STSTRM: ERFI-P-CONN (NR)
DS3: LPBKTERMINAL (NA)	MLMR: GFP-UP-MISMATCH (MJ)	STSTRM: ERFI-P-PAYLD (NR)
DS3: RAI (NA)	MLMR: LINK-KEEPALIVE (CR)	STSTRM: ERFI-P-SRVR (NR)
DS3: SD (NA)	MLMR: LPBKFACILITY (NA)	STSTRM: LCAS-CRC (NA)
DS3: SF (NA)	MLMR: LPBKTERMINAL (NA)	STSTRM: LCAS-RX-DNU (NA)
DS3: TX-AIS (NR)	MLMR: MAN-REQ (NA)	STSTRM: LCAS-RX-FAIL (NA)
DS3: TX-RAI (NA)	MLMR: PEER-NORESPONSE (MN)	STSTRM: LCAS-RX-GRP-ERR (NA)
E1000F: AS-CMD (NA)	MLMR: PORT-MISMATCH (MJ)	STSTRM: LCAS-TX-ADD (NA)
E1000F: CARLOSS (MJ)	MLMR: RPR-SD (NA)	STSTRM: LCAS-TX-DNU (NA)
E100T: AS-CMD (NA)	MLMR: RPR-SF (NA)	STSTRM: LOF (CR)
E100T: CARLOSS (MJ)	MLMR: RPR-SPAN-MISMATCH (MJ)	STSTRM: LOM (CR)
E1: AIS (NR)	MLMR: TPTFAIL (MJ)	STSTRM: LOP-P (CR)
E1: AS-CMD (NA)	MLMR: WTR (NA)	STSTRM: LPBKCRS (NA)
E1: AS-MT (NA)	MSUDC: AIS (NR)	STSTRM: OOU-TPT (NA)

Table 2-8 Alarm List by Logical Object in Alarm Profile (continued)

E1: LOF (MJ)	MSUDC: LOS (MN)	STSTRM: PDI-P (NA)
E1: LOS (MJ)	NE-SREF: FRCDSWTOINT (NA)	STSTRM: PLM-P (CR)
E1: LPBKFACILITY (NA)	NE-SREF: FRCDSWTOPRI (NA)	STSTRM: RFI-P (NR)
E1: LPBKTERMINAL (NA)	NE-SREF: FRCDSWTOSEC (NA)	STSTRM: ROLL (NA)
E1: MS-DEG (NA)	NE-SREF: FRCDSWTOTHIRD (NA)	STSTRM: ROLL-PEND (NR)
E1: MS-EXC (NA)	NE-SREF: FRNGSYNC (NA)	STSTRM: SD-P (NA)
E1: RAI (NA)	NE-SREF: FSTSYNC (NA)	STSTRM: SF-P (NA)
E1: RCVR-MISS (MJ)	NE-SREF: HLDVRSYNC (NA)	STSTRM: SQM (CR)
E1: SSM-DUS (NA)	NE-SREF: MANSWTOINT (NA)	STSTRM: TIM-P (CR)
E1: SSM-FAIL (MN)	NE-SREF: MANSWTOPRI (NA)	STSTRM: UNEQ-P
E1: SSM-OFF (NA)	NE-SREF: MANSWTOSEC (NA)	TRUNK: ALS (NA)
E1: SSM-PRS (NA)	NE-SREF: MANSWTOTHIRD (NA)	TRUNK: AS-CMD (NA)
E1: SSM-RES (NA)	NE-SREF: SSM-LNC (NA)	TRUNK: AS-MT (NA)
E1: SSM-SMC (NA)	NE-SREF: SSM-PRC (NA)	TRUNK: CARLOSS (MJ)
E1: SSM-ST2 (NA)	NE-SREF: SSM-PRS (NA)	TRUNK: DSP-COMM-FAIL (MJ)
E1: SSM-ST3 (NA)	NE-SREF: SSM-RES (NA)	TRUNK: DSP-FAIL (MJ)
E1: SSM-ST3E (NA)	NE-SREF: SSM-SDH-TN (NA)	TRUNK: EOC (MN)
E1: SSM-ST4 (NA)	NE-SREF: SSM-SETS (NA)	TRUNK: EOC-L (MN)
E1: SSM-STU (NA)	NE-SREF: SSM-SMC (NA)	TRUNK: FAILTOSW (NA)
E1: SYNC-FREQ (NA)	NE-SREF: SSM-ST2 (NA)	TRUNK: FAPS (NA)
E1: TRMT (MJ)	NE-SREF: SSM-ST3 (NA)	TRUNK: FC-DE-NES (MJ)
E1: TRMT-MISS (MJ)	NE-SREF: SSM-ST3E (NA)	TRUNK: FC-NO-CREDITS (MJ)
E1: TX-AIS (NR)	NE-SREF: SSM-ST4 (NA)	TRUNK: FEC-MISM (MJ)
E1: TX-LOF (NR)	NE-SREF: SSM-STU (NA)	TRUNK: FORCED-REQ-SPAN (NA)
E1: TX-RAI (NA)	NE-SREF: SSM-TNC (NA)	TRUNK: GCC-EOC (MN)
EC1: AIS-L (NR)	NE-SREF: SWTOPRI (NA)	TRUNK: GE-OOSYNC (CR)
EC1: AS-CMD (NA)	NE-SREF: SWTOSEC (NA)	TRUNK: HELLO (MN)
EC1: AS-MT (NA)	NE-SREF: SWTOTHIRD (NA)	TRUNK: HI-LASERBIAS (MN)
EC1: FE-FRCDWKSWPR-RING (NA)	NE-SREF: SYNCPRI (MJ)	TRUNK: HI-RXPOWER (MN)
EC1: FE-MANWKSWPR-RING (NA)	NE-SREF: SYNCSEC (MN)	TRUNK: HI-TXPOWER (MN)
EC1: FORCED-REQ-SPAN (NA)	NE-SREF: SYNCTHIRD (MN)	TRUNK: ILK-FAIL (CR)
EC1: LOF (CR)	NE: APC-DISABLED (NA)	TRUNK: ISIS-ADJ-FAIL (MN)
EC1: LOS (CR)	NE: APC-END (NA)	TRUNK: LO-RXPOWER (MN)
EC1: LPBKFACILITY (NA)	NE: AS-CMD (NA)	TRUNK: LO-TXPOWER (MN)
EC1: LPBKTERMINAL (NA)	NE: AUD-LOG-LOSS (NA)	TRUNK: LOCKOUT-REQ (NA)
EC1: MANUAL-REQ-SPAN (NA)	NE: AUD-LOG-LOW (NA)	TRUNK: LOF (CR)
EC1: RFI-L (NR)	NE: DATAFLT (MN)	TRUNK: LOM (CR)

Table 2-8 Alarm List by Logical Object in Alarm Profile (continued)

EC1: SD-L (NA)	NE: DBOSYNC (MJ)	TRUNK: LOS (CR)
EC1: SF-L (NA)	NE: DUP-IPADDR (MN)	TRUNK: LOS-P (CR)
EC1: TIM-S (CR)	NE: DUP-NODENAME (MN)	TRUNK: LPBKFACILITY (NA)
EC1: WTR (NA)	NE: ETH-LINKLOSS (NA)	TRUNK: LPBKTERMINAL (NA)
ENVALRM: EXT (MN)	NE: HITEMP (CR)	TRUNK: MANUAL-REQ-SPAN (NA)
EQPT: ALS-DISABLED (NA)	NE: I-HITEMP (CR)	TRUNK: ODUK-1-AIS-PM (NR)
EQPT: APC-DISABLED (NA)	NE: INTRUSION-PSWD (NA)	TRUNK: ODUK-2-AIS-PM (NR)
EQPT: AS-CMD (NA)	NE: LAN-POL-REV (NA)	TRUNK: ODUK-3-AIS-PM (NR)
EQPT: AS-MT (NA)	NE: SNTP-HOST (MN)	TRUNK: ODUK-4-AIS-PM (NR)
EQPT: AUTORESET (MN)	NE: SYSBOOT (MJ)	TRUNK: ODUK-AIS-PM (NR)
EQPT: BKUPMEMP (CR)	NE: TEMP-MISM (NA)	TRUNK: ODUK-BDI-PM (NR)
EQPT: CARLOSS (MJ)	OCH: APC-DISABLED (NA)	TRUNK: ODUK-LCK-PM (NR)
EQPT: CLDRESTART (NA)	OCH-TERM: FDI (NA)	TRUNK: ODUK-OCI-PM (NR)
EQPT: COMIOXC (CR)	OCH-TERM: OCHTERM-INC (NA)	TRUNK: ODUK-SD-PM (NA)
EQPT: COMM-FAIL (MN)	OCH-TERM: OPWR-HDEG (MN)	TRUNK: ODUK-SF-PM (NA)
EQPT: CONTBUS-A-18 (MN)	OCH-TERM: OPWR-LDEG (MN)	TRUNK: ODUK-TIM-PM (MJ)
EQPT: CONTBUS-B-18 (MN)	OCH-TERM: OPWR-LFAIL (CR)	TRUNK: OTUK-AIS (NR)
EQPT: CONTBUS-DISABLED (CR)	OCH-TERM: PARAM-MISM (NA)	TRUNK: OTUK-BDI (NR)
EQPT: CONTBUS-IO-A (MN)	—	TRUNK: OTUK-IAE (MN)
EQPT: CONTBUS-IO-B (MN)	—	TRUNK: OTUK-LOF (CR)
EQPT: CPP-INCAPABLE (NA)	—	TRUNK: OTUK-SD (NA)
EQPT: CTNEQPT-MISMATCH (NA)	—	TRUNK: OTUK-SF (NA)
EQPT: CTNEQPT-PBPROT (CR)	OCH: APC-CORR-SKIPPED (MN)	TRUNK: OTUK-TIM (CR)
EQPT: CTNEQPT-PBWORK (CR)	OCH: APC-OUT-OF-RANGE (MN)	TRUNK: OUT-OF-SYNC (MJ)
EQPT: EQPT (CR)	OCH: AS-CMD (NA)	TRUNK: PROV-MISMATCH (MJ)
EQPT: EQPT-DIAG (CR)	OCH: AS-MT (NA)	TRUNK: PTIM (MJ)
EQPT: ERROR-CONFIG (MN)	OCH: FDI (NA)	TRUNK: RFI (NR)
EQPT: EXCCOL (MN)	OCH: LOS-O (MN)	TRUNK: RFI-L (NR)
EQPT: FAILTOSW (NA)	OCH: LOS-P (CR)	TRUNK: SD (NA)
EQPT: FAPS-CONFIG-MISMATCH (MN)	OCH: OPWR-HDEG (MN)	TRUNK: SD-L (NA)
EQPT: FORCED-REQ (NA)	OCH: OPWR-HFAIL (CR)	TRUNK: SF (NA)
EQPT: FP-LINK-LOSS (MN)	OCH: OPWR-LDEG (MN)	TRUNK: SF-L (NA)
EQPT: FTA-MISMATCH (NA)	OCH: OPWR-LFAIL (CR)	TRUNK: SIGLOSS (MJ)
EQPT: HI-LASERBIAS (MN)	OCH: PARAM-MISM (NA)	TRUNK: SQUELCHED (NA)
EQPT: HI-LASERTEMP (MN)	OCH: PORT-FAIL (CR)	TRUNK: SSM-DUS (NA)
EQPT: HI-TXPOWER (MN)	OCH: TRAIL-SIGNAL-FAIL (NA)	TRUNK: SSM-FAIL (MN)

Table 2-8 Alarm List by Logical Object in Alarm Profile (continued)

EQPT: HITEMP (MN)	OCH: VOA-HDEG (MN)	TRUNK: SSM-LNC (NA)
EQPT: IMPROPRMVL (CR)	OCH: VOA-HFAIL (CR)	TRUNK: SSM-OFF (NA)
EQPT: INHSWPR (NA)	OCH: VOA-LDEG (MN)	TRUNK: SSM-PRC (NA)
EQPT: INHSWWKG (NA)	OCH: VOA-LFAIL (CR)	TRUNK: SSM-PRS (NA)
EQPT: IOSCFGCOPY (NA)	OCHNC-CONN: OCHNC-INC (NA)	TRUNK: SSM-RES (NA)
EQPT: LO-LASERBIAS (MN)	OCN: AIS-L (NR)	TRUNK: SSM-SDH-TN (NA)
EQPT: LO-LASERTEMP (MN)	OCN: ALS (NA)	TRUNK: SSM-SETS (NA)
EQPT: LO-TXPOWER (MN)	OCN: APS-INV-PRIM (MN)	TRUNK: SSM-SMC (NA)
EQPT: LOCKOUT-REQ (NA)	OCN: APS-PRIM-FAC (NA)	TRUNK: SSM-ST2 (NA)
EQPT: MAN-REQ (NA)	OCN: APS-PRIM-SEC-MISM (MN)	TRUNK: SSM-ST3 (NA)
EQPT: MANRESET (NA)	OCN: APSB (MN)	TRUNK: SSM-ST3E (NA)
EQPT: MCAST-MAC-TABLE-FULL (NA)	OCN: APSC-IMP (MN)	TRUNK: SSM-ST4 (NA)
EQPT: MEA (CR)	OCN: APSCDFLTK (MN)	TRUNK: SSM-STU (NA)
EQPT: MEM-GONE (MJ)	OCN: APSCINCON (MN)	TRUNK: SSM-TNC (NA)
EQPT: MEM-LOW (MN)	OCN: APSCM (MN)	TRUNK: SYNC-FREQ (NA)
EQPT: NO-CONFIG (NA)	OCN: APSCNMIS (MJ)	TRUNK: SYNCLOSS (MJ)
EQPT: OPEN-SLOT (NA)	OCN: APSIMP (MN)	TRUNK: TIM (CR)
EQPT: PROTNA (MN)	OCN: APSMM (MN)	TRUNK: TIM-MON (MN)
EQPT: PWR-FAIL-A (MN)	OCN: AS-CMD (NA)	TRUNK: TRAIL-SIGNAL-FAIL (NA)
EQPT: PWR-FAIL-B (MN)	OCN: AS-MT (NA)	TRUNK: UNC-WORD (NA)
EQPT: PWR-FAIL-RET-A (MN)	OCN: AUTOLSROFF (CR)	TRUNK: UT-COMM-FAIL (MJ)
EQPT: PWR-FAIL-RET-B (MN)	OCN: BLSR-SW-VER-MISM (MJ)	TRUNK: UT-FAIL (MJ)
EQPT: RUNCFG-SAVENEED (NA)	OCN: BLSROSYNC (MJ)	TRUNK: WTR (NA)
EQPT: SFTWDOWN (MN)	OCN: E-W-MISMATCH (MJ)	TRUNK: WVL-MISMATCH (MJ)
EQPT: SW-MISMATCH (NA)	OCN: EOC (MN)	VCG: LOA (CR)
EQPT: SWMTXMOD-PROT (CR)	OCN: EOC-L (MN)	VCG: VCG-DEG (NA)
EQPT: SWMTXMOD-WORK (CR)	OCN: EXERCISE-RING-FAIL (NA)	VCG: VCG-DOWN (NA)
EQPT: VOA-DISABLED (CR)	OCN: EXERCISE-SPAN-FAIL (NA)	VT-MON: AIS-V (NR)
EQPT: WKSWPR (NA)	OCN: EXTRA-TRAF-PREEMPT (MJ)	VT-MON: AUTOSW-AIS (NR)
EQPT: WORK-QUEUE-FULL (NA)	OCN: FAILTOSW (NA)	VT-MON: AUTOSW-LOP (NA)
EQPT: WTR (NA)	OCN: FAILTOSWR (NA)	VT-MON: AUTOSW-PDI (NA)
ESCON: ALS (NA)	OCN: FAILTOSWS (NA)	VT-MON: AUTOSW-SDBER (NA)
ESCON: AS-CMD (NA)	OCN: FE-FRCDWKSWBK-SPAN (NA)	VT-MON: AUTOSW-SFBER (NA)
ESCON: AS-MT (NA)	OCN: FE-FRCDWKSWPR-RING (NA)	VT-MON: AUTOSW-UNEQ (NA)
ESCON: FAILTOSW (NA)	OCN: FE-FRCDWKSWPR-SPAN (NA)	VT-MON: FAILTOSW-PATH (NA)

Table 2-8 Alarm List by Logical Object in Alarm Profile (continued)

ESCON: FORCED-REQ-SPAN (NA)	OCN: FE-LOCKOUTOFPR-SPAN (NA)	VT-MON: FORCED-REQ (NA)
ESCON: HI-LASERBIAS (MN)	OCN: FE-MANWKSWBK-SPAN (NA)	VT-MON: LOCKOUT-REQ (NA)
ESCON: HI-RXPOWER (MN)	OCN: FE-MANWKSWPR-RING (NA)	VT-MON: LOP-V (MJ)
ESCON: HI-TXPOWER (MN)	OCN: FE-MANWKSWPR-SPAN (NA)	VT-MON: MAN-REQ (NA)
ESCON: LO-RXPOWER (MN)	OCN: FEPRLF (MN)	VT-MON: PLM-V (MJ)
ESCON: LO-TXPOWER (MN)	OCN: FORCED-REQ-RING (NA)	VT-MON: RFI-V (NR)
ESCON: LOCKOUT-REQ (NA)	OCN: FORCED-REQ-SPAN (NA)	VT-MON: ROLL (NA)
ESCON: LOS (CR)	OCN: FULLPASSTHR-BI (NA)	VT-MON: ROLL-PEND (NA)
ESCON: LPBKFACILITY (NA)	OCN: HELLO (MN)	VT-MON: SD-V (NA)
ESCON: LPBKTERMINAL (NA)	OCN: HI-LASERBIAS (MN)	VT-MON: SF-V (NA)
ESCON: MANUAL-REQ-SPAN (NA)	OCN: HI-LASERTEMP (MN)	VT-MON: TIM-V (MJ)
ESCON: SIGLOSS (MJ)	OCN: HI-RXPOWER (MN)	VT-MON: UNEQ-V (MJ)
ESCON: SQUELCHED (NA)	OCN: HI-TXPOWER (MN)	VT-MON: WKSWPR (NA)
ESCON: WKSWPR (NA)	OCN: ISIS-ADJ-FAIL (MN)	VT-MON: WTR (NA)
ESCON: WTR (NA)	OCN: KB-PASSTHR (NA)	VT-TERM: AIS-V (NR)
ETH: VLAN-AIS (NR)	OCN: KBYTE-APS-CHAN-FAIL (MN)	VT-TERM: AS-MT-OOG (NA)
EXT-SREF: FRCDSWTOPRI (NA)	OCN: LASEREOL (MN)	VT-TERM: LCAS-CRC (NA)
EXT-SREF: FRCDSWTOSEC (NA)	OCN: LKOUTPR-S (NA)	VT-TERM: LCAS-RX-DNU (NA)
EXT-SREF: FRCDSWTOTHIRD (NA)	OCN: LMP-FAIL (MN)	VT-TERM: LCAS-RX-FAIL (NA)
EXT-SREF: MANSWTOPRI (NA)	OCN: LMP-SD (MN)	VT-TERM: LCAS-RX-GRP-ERR (NA)
EXT-SREF: MANSWTOSEC (NA)	OCN: LMP-SF (MN)	VT-TERM: LCAS-TX-ADD (NA)
EXT-SREF: MANSWTOTHIRD (NA)	OCN: LMP-UNALLOC (NA)	VT-TERM: LCAS-TX-DNU (NA)
EXT-SREF: SWTOPRI (NA)	OCN: LO-LASERBIAS (MN)	VT-TERM: LOM (MJ)
EXT-SREF: SWTOSEC (NA)	OCN: LO-LASERTEMP (MN)	VT-TERM: LOP-V (MJ)
EXT-SREF: SWTOTHIRD (NA)	OCN: LO-RXPOWER (MN)	VT-TERM: OOU-TPT (NA)
EXT-SREF: SYNCPRI (MN)	OCN: LO-TXPOWER (MN)	VT-TERM: PLM-V (MJ)
EXT-SREF: SYNCSEC (MN)	OCN: LOCKOUT-REQ (NA)	VT-TERM: RFI-V (NR)
EXT-SREF: SYNCTHIRD (MN)	OCN: LOF (CR)	VT-TERM: ROLL (NA)
FAN: EQPT-MISS (CR)	OCN: LOS (CR)	VT-TERM: ROLL-PEND (NA)
FAN: FAN (CR)	OCN: LPBKFACILITY (NA)	VT-TERM: SD-V (NA)
FAN: MEA (CR)	OCN: LPBKTERMINAL (NA)	VT-TERM: SF-V (NA)
FAN: MFGMEM (CR)	OCN: MANUAL-REQ-RING (NA)	VT-TERM: SQM (MJ)
FC: ALS (NA)	OCN: MANUAL-REQ-SPAN (NA)	VT-TERM: TIM-V (MJ)
FC: AS-CMD (NA)	OCN: PRC-DUPID (MJ)	VT-TERM: UNEQ-V (MJ)
FC: AS-MT (NA)	OCN: RFI-L (NR)	—

2.5 Trouble Notifications

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

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

2.5.1 Alarm Characteristics

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

2.5.2 Condition Characteristics

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

For a comprehensive list of all conditions, refer to the *Cisco ONS SONET TL1 Command Guide*. For more information about transient conditions, see [Chapter 3, “Transient Conditions.”](#)

**Note**

When an entity is put in the OOS, MT administrative state, the ONS 15454 suppresses all standing alarms on that entity and alarms and events appear on the Conditions tab. You can change this behavior for the LPBKFACILITY and LPBKTERMINAL alarms. To display these alarms on the Alarms tab, set the NODE.general.ReportLoopbackConditionsOnOOS-MTPorts value to TRUE on the NE Defaults tab. For more information about changing NE defaults, refer to the “Maintain the Node” chapter in the *Cisco ONS 15454 Procedure Guide*.

2.5.3 Severities

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

- A Critical (CR) alarm generally indicates severe, Service-Affecting (SA) trouble that needs immediate correction. Loss of traffic on an STS-1, which can hold 28 DS-1 circuits, would be a Critical (CR), Service-Affecting (SA) alarm.
- A Major (MJ) alarm is a serious alarm, but the trouble has less impact on the network. For example, loss of traffic on more than five DS-1 circuits is Critical (CR), but loss of traffic on one to four DS-1 circuits is Major (MJ).

- Minor (MN) alarms generally are those that do not affect service. For example, the automatic protection switching (APS) byte failure (APSB) alarm indicates that line terminating equipment (LTE) detects a byte failure on the signal that could prevent traffic from properly executing a traffic switch.
- Not Alarmed (NA) conditions are information indicators, such as for free-run synchronization state (FRNGSYNC) or a forced-switch to primary (FRCSWTOPRI) timing event. They could or could not require troubleshooting, as indicated in the entries.
- Not Reported (NR) conditions occur as a secondary result of another event. For example, the alarm indication signal (AIS), with severity NR, is inserted by a downstream node when an LOS (CR or MJ) alarm occurs upstream. These conditions do not in themselves require troubleshooting, but are to be expected in the presence of primary alarms.

Severities can be customized for an entire network or for single nodes, from the network level down to the port level by changing or downloading customized alarm profiles. These custom severities are subject to the standard severity-demoting rules given in Telcordia GR-474-CORE and shown in the [“2.5.4 Alarm Hierarchy” section on page 2-34](#). Procedures for customizing alarm severities are located in the “Manage Alarms” chapter in the *Cisco ONS 15454 Procedure Guide*.

2.5.4 Alarm Hierarchy

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

A path alarm can be demoted if a higher-ranking alarm is raised for the same object. For example, If a path trace identifier mismatch (TIM-P) is raised on a circuit path and then a loss of pointer on the path (LOP-P) is raised on the path, the LOP-P alarm stands and the TIM-P closes. The path alarm hierarchy used in the ONS 15454 system is shown in [Table 2-9](#).

Table 2-9 Path Alarm Hierarchy

Priority	Condition Type
Highest	AIS-P
—	LOP-P
—	UNEQ-P
Lowest	TIM-P

Facility (port) alarms also follow a hierarchy, which means that lower-ranking alarms are closed by higher-ranking alarms. The facility alarm hierarchy used in the ONS 15454 is shown in [Table 2-10](#).

Table 2-10 Facility Alarm Hierarchy

Priority	Condition Type
Highest	LOS
—	LOF
—	AIS-L
—	SF-L

Table 2-10 Facility Alarm Hierarchy (continued)

Priority	Condition Type
—	SD-L
—	RFI-L
—	TIM-S
—	AIS-P
—	LOP-P
—	SF-P
—	SD-P
—	UNEQ-P
—	TIM-P
Lowest	PLM-P

Near-end failures and far-end failures follow different hierarchies. Near-end failures stand according to whether they are for the entire signal (LOS, LOF), facility (AIS-L), path (AIS-P, etc.) or VT (AIS-V, etc.). The full hierarchy for near-end failures is shown in [Table 2-11](#). This table is taken from Telcordia GR-253-CORE.

Table 2-11 Near-End Alarm Hierarchy

Priority	Condition Type
Highest	LOS
—	LOF
—	AIS-L
—	AIS-P ¹
—	LOP-P ²
—	UNEQ-P
—	TIM-P
—	PLM-P
—	AIS-V ¹
—	LOP-V ²
—	UNEQ-V
—	PLM-V
Lowest	DS-N AIS (if reported for outgoing DS-N signals)

1. Although it is not defined as a defect or failure, all-ones STS pointer relay is also higher priority than LOP-P. Similarly, all-ones VT pointer relay is higher priority than LOP-V.
2. LOP-P is also higher priority than the far-end failure RFI-P, which does not affect the detection of any near-end failures. Similarly, LOP-V is higher priority than RFI-V.

The far-end failure alarm hierarchy is shown in [Table 2-12](#), as given in Telcordia GR-253-CORE.

Table 2-12 *Far-End Alarm Hierarchy*

Priority	Condition Type
Highest	RFI-L
—	RFI-P
Lowest	RFI-V

2.5.5 Service Effect

Service-Affecting (SA) alarms—those that interrupt service—could be Critical (CR), Major (MJ), or Minor (MN) severity alarms. Service-Affecting (SA) alarms indicate service is affected. Non-Service-Affecting (NSA) alarms always have a Minor (MN) default severity.

2.5.6 States

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

- A raised (R) event is one that is active.
- A cleared (C) event is one that is no longer active.
- A transient (T) event is one that is automatically raised and cleared in CTC during system changes such as user login, logout, loss of connection to node view, etc. Transient events do not require user action. These are listed in [Chapter 3, “Transient Conditions.”](#)

2.6 Safety Summary

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



Caution

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

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



Warning

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

**Warning**

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

**Warning**

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

**Warning**

Class 1 laser product. Statement 1008

**Warning**

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

**Warning**

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

2.7 Alarm Procedures

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

**Note**

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

**Note**

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

**Note**

When an entity is put in the OOS,MT administrative state, the ONS 15454 suppresses all standing alarms on that entity and alarms and events appear on the Conditions tab. You can change this behavior for the LPBKFACILITY and LPBKTERMINAL alarms. To display these alarms on the Alarms tab, set the

NODE.general.ReportLoopbackConditionsOnPortsInOOS-MT value to TRUE on the NE Defaults tab. For more information about changing NE defaults, refer to the “Maintain the Node” chapter in the *Cisco ONS 15454 Procedure Guide*.

2.7.1 AIS

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

SONET Logical Objects: BITS, DS1, DS3, E1, FUDC, MSUDC

DWDM Logical Object: TRUNK

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

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



Note

ONS 15454 DS-3 terminal (inward) loopbacks do not transmit an AIS in the direction away from the loopback. Instead of AIS, a continuance of the signal transmitted into the loopback is provided. A DS3/EC1-48 card can be provisioned to transmit AIS for a terminal loopback.

Clear the AIS Condition

- Step 1** Determine whether there are alarms on the upstream nodes and equipment, especially the “[LOS \(OCN\)](#)” alarm on [page 2-168](#), or if there are out-of-service (OOS,MT or OOS,DSBLD) ports.
- Step 2** Clear the upstream alarms using the applicable procedures in this chapter.
- Step 3** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

2.7.2 AIS-L

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

SONET Logical Objects: EC1, OCN

DWDM Logical Object: TRUNK

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

This condition can also be raised in conjunction with the “[TIM-S](#)” alarm on [page 2-252](#) if AIS-L is enabled.

**Note**

ONS 15454 DS-3 terminal (inward) loopbacks do not transmit an AIS in the direction away from the loopback. Instead of AIS, a continuance of the signal transmitted into the loopback is provided. A DS3/EC1-48 card can be provisioned to transmit AIS for a terminal loopback.

Clear the AIS-L Condition

-
- Step 1** Complete the “[Clear the AIS Condition](#)” procedure on page 2-38.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.3 AIS-P

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

SONET Logical Objects: STSMON, STSTRM

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

Clear the AIS-P Condition

-
- Step 1** Complete the “[Clear the AIS Condition](#)” procedure on page 2-38.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.4 AIS-V

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

SONET Logical Objects: VT-MON, VT-TERM

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

See the “[1.11.2 AIS-V on DS3XM-6 or DS3XM-12 Unused VT Circuits](#)” section on page 1-137 for more information.

Clear the AIS-V Condition

-
- Step 1** Complete the “[Clear the AIS Condition](#)” procedure on page 2-38.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.5 ALS

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.6 AMPLI-INIT

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.7 APC-CORR-SKIPPED

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.8 APC-DISABLED

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.9 APC-END

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.10 APC-OUT-OF-RANGE

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.11 APC-WRONG-GAIN

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.12 APSB

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

SONET Logical Object: OCN

The APS Channel Byte Failure alarm occurs when LTE detects protection switching byte failure or an invalid switching code in the incoming APS signal. Some older SONET not manufactured by Cisco send invalid APS codes if they are configured in a 1+1 protection group with newer SONET nodes, such as the ONS 15454. These invalid codes cause an APSB alarm on an ONS 15454.

-
- Step 1** Use an optical test set to examine the incoming SONET overhead to confirm inconsistent or invalid K bytes. For specific procedures to use the test set equipment, consult the manufacturer. If corrupted K bytes are confirmed and the upstream equipment is functioning properly, the upstream equipment might not interoperate effectively with the ONS 15454.
- Step 2** If the alarm does not clear and the overhead shows inconsistent or invalid K bytes, you could need to replace the upstream cards for protection switching to operate properly. Complete the [“Physically Replace a Traffic Card” procedure on page 2-281](#).
- Step 3** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.13 APSCDFLTk

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

SONET Logical Object: OCN

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

Troubleshooting for APSCDFLTk is often similar to troubleshooting for the [“BLSROSYNC” alarm on page 2-59](#).

Clear the APSCDFLTk Alarm

-
- Step 1** Complete the [“Identify a BLSR Ring Name or Node ID Number” procedure on page 2-268](#) to verify that each node has a unique node ID number.
- Step 2** Repeat [Step 1](#) for all nodes in the ring.
- Step 3** If two nodes have the same node ID number, complete the [“Change a BLSR Node ID Number” procedure on page 2-269](#) to change one node ID number so that each node ID is unique.
- Step 4** If the alarm does not clear, verify correct configuration of east port and west port optical fibers. (See the [“E-W-MISMATCH” alarm on page 2-94](#).) West port fibers must connect to east port fibers and east port fibers must connect to west port fibers. The “Install Cards and Fiber-Optic Cable” chapter in the *Cisco ONS 15454 Procedure Guide* provides procedures for fiber BLSRs.
- Step 5** If the alarm does not clear and the network is a four-fiber BLSR, ensure that each protect fiber is connected to another protect fiber and each working fiber is connected to another working fiber. The software does not report any alarm if a working fiber is incorrectly attached to a protect fiber.
- Step 6** If the alarm does not clear, complete the [“Verify Node Visibility for Other Nodes” procedure on page 2-269](#).
- Step 7** If nodes are not visible, complete the [“Verify or Create Node Section DCC Terminations” procedure on page 2-283](#) to ensure that section data communications channel (SDCC) terminations exist on each node.

- Step 8** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

2.7.14 APSC-IMP

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

SONET Logical Object: OCN

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

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



Note

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



Note

The APSC-IMP alarm may be raised on a BLSR or MS-SPRing when a drop connection is part of a cross-connect loopback.



Note

The APSC-IMP alarm may be momentarily raised on BLSR spans during PCA circuit creation or deletion across multiple nodes using CTC.



Warning

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



Warning

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

Clear the APSC-IMP Alarm

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

**Caution**

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

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

- Step 2** If the K byte is valid, verify that each node has a ring name that matches the other node ring names. Complete the [“Identify a BLSR Ring Name or Node ID Number” procedure on page 2-268](#).
- Step 3** Repeat [Step 2](#) for all nodes in the ring.
- Step 4** If a node has a ring name that does not match the other nodes, make that node’s ring name identical to the other nodes. Complete the [“Change a BLSR Ring Name” procedure on page 2-268](#).
- Step 5** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

2.7.15 APSCINCON

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

SONET Logical Object: OCN

An APS Inconsistent alarm means that an inconsistent APS byte is present. The SONET overhead contains K1/K2 APS bytes that notify receiving equipment, such as the ONS 15454, to switch the SONET signal from a working to a protect path when necessary. An inconsistent APS code occurs when three consecutive frames contain nonidentical APS bytes, which in turn give the receiving equipment conflicting commands about switching.

Clear the APSCINCON Alarm

- Step 1** Look for other alarms, especially the [“LOS \(OCN\)” alarm on page 2-168](#), the [“LOF \(OCN\)” alarm on page 2-155](#), or the [“AIS” condition on page 2-38](#). Clearing these alarms clears the APSCINCON alarm.
- Step 2** If an APSINCON alarm occurs with no other alarms, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

2.7.16 APSCM

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

SONET Logical Object: OCN

The APS Channel Mismatch alarm occurs when the ONS 15454 expects a working channel but receives a protect channel. In many cases, the working and protect channels are crossed and the protect channel is active. If the fibers are crossed and the working line is active, the alarm does not occur. The APSCM

alarm occurs only on the ONS 15454 when bidirectional protection is used on OC-N cards in a 1+1 protection group configuration. The APSCM alarm does not occur in an optimized 1+1 protection configuration.



Warning

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



Warning

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



Warning

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

Clear the APSCM Alarm



Caution

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

- 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 into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.

2.7.17 APSCNMIS

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

SONET Logical Object: OCN

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

Clear the APSCNMIS Alarm

- Step 1** Complete the [“Identify a BLSR Ring Name or Node ID Number” procedure on page 2-268](#) to verify that each node has a unique node ID number.
- Step 2** If the Node ID column contains any two nodes with the same node ID listed, record the repeated node ID.
- Step 3** Click **Close** in the Ring Map dialog box.
- Step 4** If two nodes have the same node ID number, complete the [“Change a BLSR Node ID Number” procedure on page 2-269](#) to change one node ID number so that each node ID is unique.


Note

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


Note

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

- Step 5** If the alarm does not clear, use the [“Initiate a Lockout on a BLSR Protect Span” procedure on page 2-276](#) to lock out the span.
- Step 6** Complete the [“Clear a BLSR External Switching Command” procedure on page 2-277](#) to clear the lockout.
- Step 7** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.

2.7.18 APSIMP

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

SONET Logical Object: OCN

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

The alarm is superseded by an APSCM or APSMM alarm, but not by an AIS condition. It clears when the port receives a valid code for 10 ms.

Clear the APSIMP Alarm

- Step 1** Check the configuration of the other node in the 1+1 protection group. If the far end is not configured for 1+1 protection, create the group. For procedures, refer to the [“Turn Up Node” chapter in the Cisco ONS 15454 Procedure Guide](#).

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

2.7.19 APS-INV-PRIM

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

SONET Logical Object: OCN

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



Note

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

2.7.20 APSMM

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

SONET Logical Object: OCN

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

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

Clear the APSMM Alarm

-
- Step 1** For the reporting ONS 15454, display node view and verify the protection scheme provisioning:
- Click the **Provisioning > Protection** tabs.
 - Click the 1+1 protection group configured for the OC-N cards.
The chosen protection group is the protection group optically connected (with data communications channel, or DCC, connectivity) to the far end.
 - Click **Edit**.
 - Record whether the Bidirectional Switching check box is checked.
- Step 2** Click **OK** in the Edit Protection Group dialog box.

- Step 3** Log into the far-end node and verify that the OC-N 1+1 protection group is provisioned.
- Step 4** Verify that the Bidirectional Switching check box matches the checked or unchecked condition of the box recorded in [Step 1](#). If not, change it to match.
- Step 5** Click **Apply**.
- Step 6** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.21 APS-PRIM-FAC

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

SONET Logical Object: OCN

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



Note

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

Clear the APS-PRIM-FAC Condition

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

2.7.22 APS-PRIM-SEC-MISM

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

SONET Logical Object: OCN

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

Clear the APS-PRIM-SEC-MISM Alarm

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

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

2.7.23 AS-CMD

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

SONET Logical Objects: BPLANE, CEMR, CE1000, CE100T, DS1, DS3, E1, E1000F, E100T, EC1, EQPT, FCMR, G1000, GFP-FAC, ML1000, ML100T, MLFX, NE, OCN, PWR

DWDM Logical Objects: 2R, AOTS, ESCON, FC, GE, ISC, OCH, OMS, OTS, PPM, SHELF, TRUNK

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



Note

For more information about suppressing alarms, refer to the “Manage Alarms” chapter in the *Cisco ONS 15454 Procedure Guide*.

Clear the AS-CMD Condition

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

- b. In the backplane row, uncheck the **Suppress Alarms** column check box.
 - c. Click **Apply**.
- Step 8** If the condition is reported for the shelf, cards and other equipment are affected. To clear the alarm, complete the following steps:
- a. In node view, click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs if you have not already done so.
 - b. Click the **Suppress Alarms** check box located at the bottom of the window to deselect the option.
 - c. Click **Apply**.
- Step 9** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.24 AS-MT

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

SONET Logical Objects: CEMR, CE1000, CE100T, DS1, DS3, E1, EC1, EQPT, FCMR, G1000, GFP-FAC, ML1000, ML100T, MLFX, OCN

DWDM Logical Objects: 2R, AOTS, ESCON, FC, GE, ISC, OCH, OMS, OTS, PPM, SHELF, TRUNK

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

Clear the AS-MT Condition

-
- Step 1** Complete the [“Clear an OC-N Card Facility or Terminal Loopback Circuit” procedure on page 2-283](#).
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.25 AS-MT-OOG

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

SONET Logical Objects: STSTRM, VT-TERM

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

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

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

2.7.26 AUD-LOG-LOSS

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

SONET Logical Object: NE

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

Clear the AUD-LOG-LOSS Condition

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

2.7.27 AUD-LOG-LOW

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

SONET Logical Object: NE

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



Note

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

2.7.28 AUTOLSROFF

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

SONET Logical Object: OCN

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



Warning

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



Warning

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



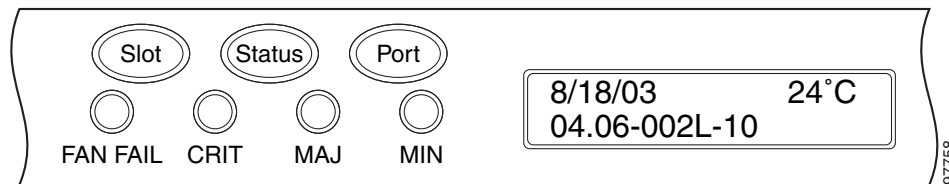
Warning

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

Clear the AUTOLSROFF Alarm

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

Figure 2-1 Shelf LCD Panel



- Step 2** If the temperature of the shelf exceeds 194 degrees F (90 degrees C), the alarm should clear if you solve the ONS 15454 temperature problem. Complete the [“Clear the HITEMP Alarm” procedure on page 2-128](#).
- Step 3** If the temperature of the shelf is under 194 degrees F (90 degrees C), the HITEMP alarm is not the cause of the AUTOLSROFF alarm. Complete the [“Physically Replace a Traffic Card” procedure on page 2-281](#) for the OC-192 card.
- Step 4** If card replacement does not clear the alarm, call Cisco TAC 1 800 553-2447 to discuss the case and if necessary open a returned materials authorization (RMA) on the original OC-192 card.

2.7.29 AUTONEG-RFI

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

SONET Logical Object: ML1000

The autonegotiation remote fault indication (RFI) indicates that an ML1000 Gigabit Ethernet port cannot detect its far-end link partner. This is typically caused by a far-end port shutdown or a unidirectional fiber cut. The partner node is likely raising a CARLOSS alarm.

AUTONEG-RFI may also be caused by misconfigured autonegotiation parameters. This causes more of a soft failure as opposed to the “[CARLOSS \(ML1000, ML100T, MLFX\)](#)” alarm on page 2-67, which is typically caused by a failure like a loss of light or optical fiber. The alarm clears when the partner node is detected.

**Note**

The far end of an Ethernet link is usually a switch or router that does not use an ONS management system.

Clear the AUTONEG-RFI Alarm

- Step 1** Check for the “[CARLOSS \(EQPT\)](#)” alarm on page 2-62 or the “[CARLOSS \(ML1000, ML100T, MLFX\)](#)” alarm on page 2-67 at the partner node. If the alarm exists there, follow the appropriate clearing procedure in this chapter.
- Step 2** If the alarm does not clear or if there is no far-end CARLOSS, check the near-end Gigabit Ethernet port autonegotiation settings:
 - a. Double-click the ML1000 card to display the card view.
 - b. Click the upper IOS tab, then click **Open IOS Connection**.
 - c. In Privileged Executive mode, enter the following command:

```
router# show interface gigabitethernet 0
```
 - d. View the command output and record the autonegotiation setting, such as the following example:

```
Full-duplex, 1000Mb/s, Gbic not connected, Auto-negotiation
output flow-control is off, input flow-control is on
```
- Step 3** View the autonegotiation configuration for the partner node. If it is ONS equipment, follow the previous step for this node. If the node is different vendor client equipment, follow that equipment documentation to obtain the information.
- Step 4** If the alarm does not clear, check for any fiber breaks such as on the transmit cable from the partner node to the near-end node.
- Step 5** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 to report a Service-Affecting (SA) problem.

2.7.30 AUTORESET

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

SONET Logical Object: EQPT

The Automatic System Reset alarm occurs when you change an IP address or perform any other operation that causes an automatic card-level reboot. AUTORESET typically clears after a card reboots (up to ten minutes).

Resets performed during a software upgrade also prompt the condition. This condition clears automatically when the card finishes resetting. If the alarm does not clear, complete the following procedure.

Clear the AUTORESET Alarm

-
- Step 1** Determine whether there are additional alarms that could have triggered an automatic reset. If there are, troubleshoot these alarms using the applicable section of this chapter.
- Step 2** If the card automatically resets more than once a month with no apparent cause, complete the “[Physically Replace a Traffic Card](#)” procedure on page 2-281.
- Step 3** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.31 AUTOSW-AIS

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

SONET Logical Objects: STSMON, VT-MON

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



Note

This condition is only reported if the path protection is set up for revertive switching.

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

Clear the AUTOSW-AIS Condition

-
- Step 1** Complete the “[Clear the AIS Condition](#)” procedure on page 2-38.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.32 AUTOSW-LOP (STSMON)

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

SONET Logical Object: STSMON

The Automatic Path Protection Switch Caused by LOP condition for the STS monitor (STSMON) indicates that automatic path protection switching occurred because of the “[LOP-P](#)” alarm on [page 2-158](#). If the path protection is configured for revertive switching, it reverts to the working path after the fault clears.

**Note**

This condition is only reported if the path protection is set up for revertive switching.

Clear the AUTOSW-LOP (STSMON) Condition

-
- Step 1** Complete the “[Clear the LOP-P Alarm](#)” procedure on [page 2-159](#).
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.33 AUTOSW-LOP (VT-MON)

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

SONET Logical Object: VT-MON

The AUTOSW-LOP alarm for the VT monitor (VT-MON) indicates that automatic path protection switching occurred because of the “[LOP-V](#)” alarm on [page 2-159](#). If the path protection is configured for revertive switching, it reverts to the working path after the fault clears.

**Note**

This condition is only reported if the path protection is set up for revertive switching.

Clear the AUTOSW-LOP (VT-MON) Condition

-
- Step 1** Complete the “[Clear the LOP-V Alarm](#)” procedure on [page 2-160](#).
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.
-

2.7.34 AUTOSW-PDI

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

SONET Logical Object: STSMON, VT-MON

The Automatic Path Protection Switch Caused by Payload Defect Indication (PDI) condition indicates that automatic path protection switching occurred because of a “[PDI-P](#)” alarm on [page 2-198](#). If the path protection is configured for revertive switching, it reverts to the working path after the fault clears.

**Note**

This condition is only reported if the path protection is set up for revertive switching.

Clear the AUTOSW-PDI Condition

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

2.7.35 AUTOSW-SDBER

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

Logical Object: STSMON, VT-MON

The Automatic Path Protection Switch Caused by Signal Degrade Bit Error Rate (SDBER) condition indicates that a [“SD-P” condition on page 2-226](#) caused automatic path protection switching to occur. If the path protection is configured for revertive switching, the path protection reverts to the working path when the SD-P is resolved.

**Note**

This condition is only reported if the path protection is set up for revertive switching.

Clear the AUTOSW-SDBER Condition

- Step 1** Complete the [“Clear the SD-P Condition” procedure on page 2-227](#).
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

2.7.36 AUTOSW-SFBER

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

Logical Object: STSMON, VT-MON

The Automatic USPR Switch Caused by Signal Fail Bit Error Rate (SFBER) condition indicates that a [“SF-P” condition on page 2-230](#) caused automatic path protection switching to occur. If the path protection is configured for revertive switching, the path protection reverts to the working path when the SF-P is resolved.

**Note**

This condition is only reported if the path protection is set up for revertive switching.

Clear the AUTOSW-SFBER Condition

-
- Step 1** Complete the “[Clear the SF-P Condition](#)” procedure on page 2-230.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.37 AUTOSW-UNEQ (STSMON)

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

SONET Logical Object: STSMON

The Automatic Path Protection Switch Caused by Unequipped condition indicates that an “[UNEQ-P](#)” alarm on page 2-258, caused automatic path protection switching to occur. If the path protection is configured for revertive switching, it reverts to the working path after the fault clears.



Note

This condition is only reported if the path protection is set up for revertive switching.

Clear the AUTOSW-UNEQ (STSMON) Condition

-
- Step 1** Complete the “[Clear the UNEQ-P Alarm](#)” procedure on page 2-259.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.38 AUTOSW-UNEQ (VT-MON)

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

SONET Logical Object: VT-MON

AUTOSW-UNEQ (VT-MON) indicates that the “[UNEQ-V](#)” alarm on page 2-260 caused automatic path protection switching to occur. If the path protection is configured for revertive switching, it reverts to the working path after the fault clears.



Note

This condition is only reported if the path protection is set up for revertive switching.

Clear the AUTOSW-UNEQ (VT-MON) Condition

-
- Step 1** Complete the “[Clear the UNEQ-V Alarm](#)” procedure on page 2-261.

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

2.7.39 AWG-DEG

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.40 AWG-FAIL

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.41 AWG-OVERTEMP

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.42 AWG-WARM-UP

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.43 BAT-FAIL

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

SONET Logical Object: PWR

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

Clear the BAT-FAIL Alarm

-
- Step 1** At the site, determine which battery is not present or operational.
- Step 2** Remove the power cable from the faulty supply. For procedures, refer to the “Install the Shelf and Backplane Cable” chapter in the *Cisco ONS 15454 Procedure Guide*. Reverse the power cable installation procedure.

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

2.7.44 BERT-ENBL

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

SONET Logical Object: DS1/DS3

The Bert Enabled alarm specifies that the bit error rate testing (BERT) feature is enabled.

2.7.45 BERT-SYNC-FAIL

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

SONET Logical Object: DS1/DS3

The Bert Synchronization Fail alarm occurs when the errors injected by the Test Pattern Generator (TPG) reaches the Test Pattern Monitor (TPM) and connectivity fails. This alarm clears when TPG and TPM synchronize.

2.7.46 BKUPMEMP

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

SONET Logical Object: EQPT

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

- Flash manager fails to format a flash partition.
- Flash manager fails to write a file to a flash partition.
- Problem at the driver level.
- Code volume fails cyclic redundancy checking (CRC, a method to verify for errors in data transmitted to the TCC2/TCC2P).

The BKUPMEMP alarm can also cause the “EQPT” alarm on [page 2-89](#). If the EQPT alarm is caused by BKUPMEMP, complete the following procedure to clear the BKUPMEMP and the EQPT alarm.



Caution

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

Clear the BKUPMEMP Alarm

- Step 1** Verify that both TCC2/TCC2Ps are powered and enabled by confirming lighted ACT/SBY LEDs on the TCC2/TCC2Ps.
- Step 2** Determine whether the active or standby TCC2/TCC2P has the alarm.

- Step 3** If both TCC2/TCC2Ps are powered and enabled, reset the TCC2/TCC2P where the alarm is raised. If the card is the active TCC2/TCC2P, complete the [“Reset an Active TCC2/TCC2P Card and Activate the Standby Card” procedure on page 2-278](#). If the card is the standby TCC2/TCC2P:
- Right-click the standby TCC2/TCC2P in CTC.
 - Choose **Reset Card** from the shortcut menu.
 - Click **Yes** in the Are You Sure dialog box. The card resets, the FAIL LED blinks on the physical card.
 - Wait ten minutes to verify that the card you reset completely reboots.
- Step 4** If the TCC2/TCC2P you reset does not reboot successfully, or the alarm has not cleared, call Cisco TAC 1 800 553-2447. If the Cisco TAC technician tells you to reseat the card, complete the [“Remove and Reinsert \(Reseat\) the Standby TCC2/TCC2P Card” procedure on page 2-280](#). If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the [“Physically Replace a Traffic Card” procedure on page 2-281](#).
-

2.7.47 BLSROSYNC

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

SONET Logical Object: OCN

The BLSR Out Of Synchronization alarm occurs is raised temporarily during a span upgrade, downgrade, or two-fiber to four-fiber mode upgrade and clears when the procedure is complete for all nodes on the ring. If the alarm does not clear, ensure that all maintenance procedures have completed for all nodes on the ring. If the alarm still does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.

2.7.48 BLSR-SW-VER-MISM

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

SONET Logical Object: OCN

The BLSR Software Version Mismatch alarm is raised by the TCC2/TCC2P when it checks all software versions for all nodes in a ring and discovers a mismatch in versions.

Clear the BLSR-SW-VER-MISM Alarm

- Step 1** Clear the alarm by loading the correct software version on the TCC2/TCC2P with the incorrect load. To download software, refer to the release-specific software download document.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 to report a Service-Affecting (SA) problem.
-

2.7.49 BPV

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

SONET Logical Object: BITS

The 64K Clock Bipolar Density Violation alarm is raised on the TCC2P card if there is a frequency variation in the 8K BITS clock.

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



Note

This alarm is not raised on the TCC2 card.

Clear the BPV Alarm

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

2.7.50 CARLOSS (CEMR, CE1000, CE100T)

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

SONET Logical Objects: CEMR, CE1000, CE100T

The Carrier Loss alarm is raised on CE-Series cards in Mapper mode when the port is In-Service (IS) state and if there is no carrier signal. Circuit need not be present to raise the alarm. In releases prior to 6.01 the Carrier Loss alarm is raised on CE-100T-8 cards in Mapper mode when there is a circuit failure due to link integrity. It does not get raised when a user simply puts the port in the In-Service and Normal (IS-NR) service state.



Note

The Carrier Loss alarm is raised as a minor alarm when there is no circuit present on the CE-Series card and major alarm, when a circuit is present on the port.



Note

For more information about Ethernet cards, refer to the Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.

Clear the CARLOSS (CEMR, CE1000, CE100T) Alarm

-
- Step 1** Complete the “[Clear the CARLOSS \(G1000\) Alarm](#)” procedure on page 2-65. However, rather than checking for a TPTFAIL (G1000) at the end of the procedure, check for a “[TPTFAIL \(CEMR, CE100T, CE1000\)](#)” alarm on page 2-253.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.
-

2.7.51 CARLOSS (E1000F, E100T)

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

SONET Logical Objects: E1000F, E100T

A Carrier Loss alarm on the LAN E-Series Ethernet card is the data equivalent of the “[LOS \(OCN\)](#)” alarm on page 2-168. The Ethernet card has lost its link and is not receiving a valid signal. The most common causes of the CARLOSS alarm are a disconnected cable, an Ethernet Gigabit Interface Converter (GBIC) fiber connected to an optical card rather than an Ethernet device, or an improperly installed Ethernet card. Ethernet card ports must be enabled for CARLOSS to occur. CARLOSS is declared after no signal is received for approximately 2.5 seconds.

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



Note

For more information about Ethernet cards, refer to the Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.

Clear the CARLOSS (E1000F, E100T) Alarm

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



Caution

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

- Step 2** If the fiber cable is properly connected and attached to the port, verify that the cable connects the card to another Ethernet device and is not misconnected to an OC-N card. For more information about fiber connections and terminations, refer to the “Install Cards and Fiber-Optic Cable” chapter in the *Cisco ONS 15454 Procedure Guide*.
- Step 3** If no misconnection to an OC-N card exists, verify that the transmitting device is operational. If not, troubleshoot the device.
- Step 4** If the alarm does not clear, use an Ethernet test set to determine whether a valid signal is coming into the Ethernet port. For specific procedures to use the test set equipment, consult the manufacturer.

- Step 5** If a valid Ethernet signal is not present and the transmitting device is operational, replace the fiber cable connecting the transmitting device to the Ethernet port. To do this, refer to the “Install Cards and Fiber-Optic Cable” chapter in the *Cisco ONS 15454 Procedure Guide*.
- Step 6** If a valid Ethernet signal is present, complete the “[Remove and Reinsert \(Reseat\) Any Card](#)” procedure on page 2-280 for the Ethernet card.
- Step 7** If the alarm does not clear, complete the “[Physically Replace a Traffic Card](#)” procedure on page 2-281 for the Ethernet card.
- Step 8** If a CARLOSS alarm repeatedly appears and clears, use the following steps to examine the layout of your network to determine whether the Ethernet circuit is part of an Ethernet manual cross-connect.
- An Ethernet manual cross-connect is used when another vendor’s equipment sits between ONS 15454 nodes, and the open systems interconnect/target identifier address resolution protocol (OSI/TARP)-based equipment does not allow tunneling of the ONS 15454 TCP/IP-based DCC. To circumvent a lack of continuous DCC, the Ethernet circuit is manually cross connected to an STS channel riding through the non-ONS network.
- If the reporting Ethernet circuit is part of an Ethernet manual cross-connect, complete the following steps. The reappearing alarm could be a result of mismatched STS circuit sizes in the set up of the manual cross-connect. If the Ethernet circuit is not part of a manual cross-connect, the following steps do not apply.
- Right-click anywhere in the row of the CARLOSS alarm.
 - Click **Select Affected Circuits** in the shortcut menu that appears.
 - Record the information in the type and size columns of the highlighted circuit.
 - From the examination of the layout of your network, determine which ONS 15454 and card and card are hosting the Ethernet circuit at the other end of the Ethernet manual cross-connect and complete the following substeps:
 - Log into the ONS 15454 at the other end of the Ethernet manual cross-connect.
 - Double-click the Ethernet card that is part of the Ethernet manual cross-connect.
 - Click the **Circuits** tab.
 - Record the information in the type and size columns of the circuit that is part of the Ethernet manual cross-connect. The Ethernet manual cross-connect circuit connects the Ethernet card to an OC-N card at the same node.
 - Use the information you recorded to determine whether the two Ethernet circuits on each side of the Ethernet manual cross-connect have the same circuit size.
- If one of the circuit sizes is incorrect, complete the “[Delete a Circuit](#)” procedure on page 2-283 and reconfigure the circuit with the correct circuit size. For more information, refer to the “Create Circuits and VT Tunnels” chapter in the *Cisco ONS 15454 Procedure Guide*.
- Step 9** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.

2.7.52 CARLOSS (EQPT)

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

SONET Logical Object: EQPT

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

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

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

**Warning**

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

**Warning**

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

**Note**

For more information about provisioning MXP or TXP PPMs, refer to the “Provision Transponders and Muxponders” chapter of the *Cisco ONS 15454 DWDM Procedure Guide*. For more information about the cards themselves, refer to the *Cisco ONS 15454 DWDM Reference Manual*. For more information about MRC-12, MRC-4, and OC192-XFP/STM64-XFP cards, refer to the “Optical Cards” chapter in the *Cisco ONS 15454 Reference Manual*. For more information about Ethernet cards, refer to the “Ethernet Cards” chapter in the *Cisco ONS 15454 Reference Manual*.

Clear the CARLOSS (EQPT) Alarm

- Step 1** If the reporting card is an MXP or TXP card in an ONS 15454 node, verify the data rate configured on the pluggable port module (PPM):
- Double-click the reporting MXP or TXP card.
 - Click the **Provisioning > Pluggable Port Modules** tabs.
 - View the Pluggable Port Modules area port listing in the **Actual Equipment Type** column and compare this with the contents of the Selected PPM area Rate column for the MXP or TXP multirate port.
 - If the rate does not match the actual equipment, you must delete and recreate the selected PPM. Select the PPM, click **Delete**, then click **Create** and choose the correct rate for the port rate.
- Step 2** If the reporting card is an OC-N card, verify connectivity by pinging the ONS 15454 that is reporting the alarm by completing the [“1.9.8 Verify PC Connection to the ONS 15454 \(ping\)” procedure on page 1-120](#).
- Step 3** If the ping is successful, it demonstrates that an active TCP/IP connection exists. Restart CTC:
- Exit from CTC.
 - Reopen the browser.
 - Log into CTC.

2.7.53 CARLOSS (FC)

- Step 4** Using optical test equipment, verify that proper receive levels are achieved. (For instructions to use optical test equipment, refer to the manufacturer documentation.)

**Caution**

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

- Step 5** Verify that the optical LAN cable is properly connected and attached to the correct port. For more information about fiber connections and terminations, refer to the “Install Cards and Fiber-Optic Cable” chapter in the *Cisco ONS 15454 Procedure Guide*.
- Step 6** If the fiber cable is properly connected and attached to the port, verify that the cable connects the card to another Ethernet device and is not misconnected to an OC-N card.
- Step 7** If you are unable to establish connectivity, replace the fiber cable with a new known-good cable. To do this, refer to the “Install Cards and Fiber-Optic Cable” chapter in the *Cisco ONS 15454 Procedure Guide*.
- Step 8** If you are unable to establish connectivity, perform standard network or LAN diagnostics. For example, trace the IP route, verify cable continuity, and troubleshoot any routers between the node and CTC. To verify cable continuity, follow site practices.
- Step 9** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.

2.7.53 CARLOSS (FC)

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.54 CARLOSS (G1000)

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

SONET Logical Object: G1000

A Carrier Loss alarm on the LAN G-Series Ethernet card is the data equivalent of the [“LOS \(OCN\)” alarm on page 2-168](#). The Ethernet card has lost its link and is not receiving a valid signal.

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

- The G1000-4 port reporting the alarm is not receiving a valid signal from the attached Ethernet device. The CARLOSS can be caused by an improperly connected Ethernet cable or a problem with the signal between the Ethernet device and the G1000-4 port.
- If a problem exists in the end-to-end path (including possibly the far-end G1000-4 card), it causes the reporting card to turn off the Gigabit Ethernet transmitter. Turning off the transmitter typically causes the attached device to turn off its link laser, which results in a CARLOSS on the reporting G1000-4 card. The root cause is the problem in the end-to-end path. When the root cause is cleared, the far-end G1000-4 port turns the transmitter laser back on and clears the CARLOSS on the reporting card. If a turned-off transmitter causes the CARLOSS alarm, other alarms such as the [“TPTFAIL \(G1000\)” alarm on page 2-254](#) or OC-N alarms or conditions on the end-to-end path normally accompany the CARLOSS (G1000) alarm.

Refer to the *Cisco ONS 15454 Reference Manual* for a description of the G1000-4 card's end-to-end Ethernet link integrity capability. Also see the [“TRMT” alarm on page 2-256](#) for more information about alarms that occur when a point-to-point circuit exists between two cards.

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

**Note**

For more information about Ethernet cards, refer to the Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.

Clear the CARLOSS (G1000) Alarm

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

**Caution**

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

- Step 2** If the fiber cable is correctly connected and attached, verify that the cable connects the card to another Ethernet device and is not misconnected to an OC-N card.
- Step 3** If no misconnection to the OC-N card exists, verify that the attached transmitting Ethernet device is operational. If not, troubleshoot the device.
- Step 4** Verify that optical receive levels are within the normal range. The correct specifications are listed in the [“1.12.3 OC-N Card Transmit and Receive Levels” section on page 1-147](#).
- Step 5** If the alarm does not clear, use an Ethernet test set to determine whether a valid signal is coming into the Ethernet port. For specific procedures to use the test set equipment, consult the manufacturer.
- Step 6** If a valid Ethernet signal is not present and the transmitting device is operational, replace the fiber cable connecting the transmitting device to the Ethernet port. To do this, refer to the “Install Cards and Fiber-Optic Cable” chapter in the *Cisco ONS 15454 Procedure Guide*.
- Step 7** If the alarm does not clear, and link autonegotiation is enabled on the port but the autonegotiation process fails, the card turns off its transmitter laser and reports a CARLOSS alarm. If link autonegotiation has been enabled for the port, determine whether there are conditions that could cause autonegotiation to fail:
- Confirm that the attached Ethernet device has autonegotiation enabled and is configured for compatibility with the asymmetric flow control on the card.
 - Confirm that the attached Ethernet device configuration allows reception of flow control frames.
- Step 8** If the alarm does not clear, disable and reenable the Ethernet port to attempt to remove the CARLOSS condition. (The autonegotiation process restarts.)
- Step 9** If the alarm does not clear and the [“TPTFAIL \(G1000\)” alarm on page 2-254](#) is also reported, complete the [“Clear the TPTFAIL \(G1000\) Alarm” procedure on page 2-255](#). If the TPTFAIL alarm is not raised, continue to the next step.

**Note**

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

- Step 10** If the TPTFAIL alarm was not raised, determine whether a terminal (inward) loopback has been provisioned on the port:
- In node view, click the card to go to card view.
 - Click the **Maintenance > Loopback** tabs.
 - If the service state is listed as OOS-MA,LPBK&MT, a loopback is provisioned. Go to [Step 11](#).
- Step 11** If a loopback was provisioned, complete the [“Clear Other Electrical Card or Ethernet Card Loopbacks” procedure on page 2-284](#).
- On the G1000-4, provisioning a terminal (inward) loopback causes the transmit laser to turn off. If an attached Ethernet device detects the loopback as a loss of carrier, the attached Ethernet device shuts off the transmit laser to the G1000-4 card. Terminating the transmit laser could raise the CARLOSS alarm because the loopbacked G1000-4 port detects the termination.
- If the does not have a loopback condition, continue to [Step 12](#).
- Step 12** If a CARLOSS alarm repeatedly appears and clears, the reappearing alarm could be a result of mismatched STS circuit sizes in the setup of the manual cross-connect. Perform the following steps if the Ethernet circuit is part of a manual cross-connect:

**Note**

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

- Right-click anywhere in the row of the CARLOSS alarm.
- Right-click or left-click **Select Affected Circuits** in the shortcut menu that appears.
- Record the information in the type and size columns of the highlighted circuit.
- Examine the layout of your network and determine which ONS 15454 and card are hosting the Ethernet circuit at the other end of the Ethernet manual cross-connect and complete the following substeps:
 - Log into the node at the other end of the Ethernet manual cross-connect.
 - Double-click the Ethernet card that is part of the Ethernet manual cross-connect.
 - Click the **Circuits** tab.
 - Record the information in the type and size columns of the circuit that is part of the Ethernet manual cross-connect. The cross-connect circuit connects the Ethernet card to an OC-N card at the same node.
- Determine whether the two Ethernet circuits on each side of the Ethernet manual cross-connect have the same circuit size from the circuit size information you recorded.
- If one of the circuit sizes is incorrect, complete the [“Delete a Circuit” procedure on page 2-283](#) and reconfigure the circuit with the correct circuit size. Refer to the “Create Circuits and VT Tunnels” chapter in the *Cisco ONS 15454 Procedure Guide* for detailed procedures to create circuits.

- Step 13** If a valid Ethernet signal is present, complete the [“Remove and Reinsert \(Reseat\) Any Card” procedure on page 2-280](#).
- Step 14** If the alarm does not clear, complete the [“Physically Replace a Traffic Card” procedure on page 2-281](#) for the Ethernet card.
- Step 15** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.
-

2.7.55 CARLOSS (GE)

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.56 CARLOSS (ISC)

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.57 CARLOSS (ML1000, ML100T, MLFX)

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

SONET Logical Objects: ML1000, ML100T, MLFX

A Carrier Loss alarm on an ML-Series Ethernet card is the data equivalent of the [“LOS \(OCN\)” alarm on page 2-168](#). The Ethernet port has lost its link and is not receiving a valid signal.

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

- The cable is not properly connected to the near or far port.
- Autonegotiation is failing (which raises the [“AUTONEG-RFI” alarm on page 2-51](#)).
- The speed (10/100 ports only) is set incorrectly.



Note

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

Clear the CARLOSS (ML1000, ML100T, MLFX) Alarm

- Step 1** Verify that the LAN cable is properly connected and attached to the correct port on the ML-Series card and on the peer Ethernet port. For more information about fiber connections and terminations, refer to the “Install Cards and Fiber-Optic Cable” chapter in the *Cisco ONS 15454 Procedure Guide*.
- Step 2** If the alarm does not clear, verify that autonegotiation is set properly on the ML-Series card port and the peer Ethernet port.

2.7.58 CARLOSS (TRUNK)

- Step 3** If the alarm does not clear, verify that the speed is set properly on the ML-Series card port and the peer Ethernet port if you are using 10/100 ports.
- Step 4** If the alarm does not clear, the Ethernet signal is not valid, but the transmitting device is operational, replace the LAN cable connecting the transmitting device to the Ethernet port.
- Step 5** If the alarm does not clear, disable and reenble the Ethernet port by performing a “shutdown” and then a “no shutdown” on the Cisco IOS CLI as in the following example:

```
router(config)# shut

router(config)# no shut
```

This action restarts autonegotiation.

- Step 6** If the alarm does not clear, complete the [“Create the Facility Loopback on the Source DS-1, DS-3, DS3N-12, DS3i-N-12, or EC1 Port” procedure on page 1-11](#) and test the loopback.
- Step 7** If the problem persists with the loopback installed, complete the [“Remove and Reinsert \(Reseat\) Any Card” procedure on page 2-280](#).
- Step 8** If the alarm does not clear, complete the [“Physically Replace a Traffic Card” procedure on page 2-281](#).
- Step 9** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.

2.7.58 CARLOSS (TRUNK)

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.59 CASETEMP-DEG

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.60 CLDRESTART

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

SONET Logical Object: EQPT

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

Clear the CLDRESTART Condition

- Step 1** Complete the [“Remove and Reinsert \(Reseat\) the Standby TCC2/TCC2P Card” procedure on page 2-280](#).
- Step 2** If the condition fails to clear after the card reboots, complete the [“Remove and Reinsert \(Reseat\) Any Card” procedure on page 2-280](#).

- Step 3** If the condition does not clear, complete the “[Physically Replace a Traffic Card](#)” procedure on [page 2-281](#) for the card.
- Step 4** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.61 COMIOXC

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

SONET Logical Object: EQPT

The Input/Output Slot To Cross-Connect Communication Failure alarm is caused by the XC10G or XC-VXC-10G cross-connect card when there is a communication failure for a traffic slot.

Clear the COMIOXC Alarm

-
- Step 1** Complete the “[Reset a Traffic Card in CTC](#)” procedure on [page 2-278](#) on the card in which the alarm is reported. For the LED behavior, see the “[2.8.2 Typical Traffic Card LED Activity During Reset](#)” section on [page 2-267](#).
- Step 2** Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
- Step 3** If the CTC reset does not clear the alarm, move traffic off the reporting cross-connect card. Complete the “[Side Switch the Active and Standby Cross-Connect Cards](#)” procedure on [page 2-278](#).
- Step 4** Complete the “[Remove and Reinsert \(Reseat\) Any Card](#)” procedure on [page 2-280](#) on the card in which the alarm is reported.
- Step 5** If the alarm does not clear, complete the “[Physically Replace an In-Service Cross-Connect Card](#)” procedure on [page 2-281](#) for the reporting cross-connect card or complete the “[Physically Replace a Traffic Card](#)” procedure on [page 2-281](#) on the card in which the alarm is reported.
- Step 6** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.
-

2.7.62 COMM-FAIL

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

SONET Logical Object: EQPT

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

Clear the COMM-FAIL Alarm

-
- Step 1** Complete the “[Reset a Traffic Card in CTC](#)” procedure on [page 2-278](#) for the reporting card.

- Step 2** If the alarm does not clear, complete the [“Physically Replace a Traffic Card” procedure on page 2-281](#) for the card.
- Step 3** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.63 CONTBUS-A-18

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

SONET Logical Object: EQPT

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

Clear the CONTBUS-A-18 Alarm

-
- Step 1** Complete the [“Remove and Reinsert \(Reseat\) the Standby TCC2/TCC2P Card” procedure on page 2-280](#) to make the TCC2/TCC2P in Slot 11 active.
- Step 2** Wait approximately 10 minutes for the TCC2/TCC2P in Slot 7 to reset as the standby TCC2/TCC2P. Verify that the ACT/SBY LED is correctly illuminated before proceeding to the next step. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
- Step 3** Position the cursor over the TCC2/TCC2P in Slot 11 and complete the [“Reset an Active TCC2/TCC2P Card and Activate the Standby Card” procedure on page 2-278](#) to return the card to the active state.
- Step 4** If the reset card has not rebooted successfully, or the alarm has not cleared, call Cisco TAC (1-800-553-2447). If the Cisco TAC technician tells you to reseat the card, complete the [“Reset an Active TCC2/TCC2P Card and Activate the Standby Card” procedure on page 2-278](#). If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the [“Physically Replace a Traffic Card” procedure on page 2-281](#).
-

2.7.64 CONTBUS-B-18

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

SONET Logical Object: EQPT

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

Clear the CONTBUS-B-18 Alarm

-
- Step 1** Complete the [“Reset an Active TCC2/TCC2P Card and Activate the Standby Card” procedure on page 2-278](#) to make the Slot 7 TCC2/TCC2P active.

- Step 2** Wait approximately 10 minutes for the Slot 11 TCC2/TCC2P to reset as the standby TCC2/TCC2P. Verify that the ACT/SBY LED is correctly illuminated before proceeding to the next step. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
- Step 3** Position the cursor over the Slot 7 TCC2/TCC2P and complete the [“Reset an Active TCC2/TCC2P Card and Activate the Standby Card” procedure on page 2-278](#) to return the Slot 11 TCC2/TCC2P to the active state.
- Step 4** If the reset card has not rebooted successfully, or the alarm has not cleared, call Cisco TAC (1-800-553-2447). If the Cisco TAC technician tells you to reseal the card, complete the [“Remove and Reinsert \(Reseat\) the Standby TCC2/TCC2P Card” procedure on page 2-280](#). If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the [“Physically Replace a Traffic Card” procedure on page 2-281](#).
-

2.7.65 CONTBUS-DISABLED

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

SONET Logical Object: EQPT

The CONTBUS-DISABLED alarm is a function of the enhanced cell bus verification feature. This alarm occurs when a defective card is installed in the shelf assembly or when a card already installed in the shelf assembly becomes defective (that is, the card fails the enhanced cell bus verification test). The alarm persists as long as the defective card remains in the chassis. When the card is removed, CONTBUS-DISABLED will remain raised for a one-minute wait time. This wait time is designed as a guard period so that the system can distinguish this outage from a briefer card reset communication outage.

If no card is reinserted into the original slot during the wait time, the alarm clears. After this time, a different, nondefective card (not the original card) should be inserted.

When CONTBUS-DISABLED is raised, no message-oriented communication is allowed to or from this slot to the TCC2/TCC2P (thus avoiding node communication failure).



Caution

CONTBUS-DISABLED clears only when the faulty card is removed for one minute. If any card at all is reinserted before the one-minute guard period expires, the alarm does not clear.

CONTBUS-DISABLED overrides the [“IMPROPRMVL” alarm on page 2-131](#) during the one-minute wait period, but afterward IMPROPRMVL can be raised because it is no longer suppressed. IMPROPRMVL is raised after CONTBUS-DISABLED clears if the card is in the node database. If CONTBUS-DISABLED has cleared but IMPROPRMVL is still active, inserting a card will clear the IMPROPRMVL alarm.

Clear the CONTBUS-DISABLED Alarm

- Step 1** If the IMPROPRMVL alarm is raised, complete the [“Physically Replace a Traffic Card” procedure on page 2-281](#). (For general information about card installation, refer to the “Install Cards and Fiber-Optic Cable” chapter in the *Cisco ONS 15454 Procedure Guide*.)

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

2.7.66 CONTBUS-IO-A

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

SONET Logical Object: EQPT

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

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

Clear the CONTBUS-IO-A Alarm

-
- Step 1** Ensure that the reporting card is physically present in the shelf. Record the card type. Click the **Inventory** tab and view the Eqpt Type column to reveal the provisioned type.
- If the actual card type and the provisioned card type do not match, see the [“MEA \(EQPT\)” alarm on page 2-188](#) for the reporting card.
- Step 2** If the alarm object is any single card slot other than the standby Slot 11 TCC2/TCC2P, perform a CTC reset of the object card. Complete the [“Reset a Traffic Card in CTC” procedure on page 2-278](#). For the LED behavior, see the [“2.8.2 Typical Traffic Card LED Activity During Reset” section on page 2-267](#).
- Step 3** If the alarm object is the standby Slot 11 TCC2/TCC2P, complete the [“Reset a Traffic Card in CTC” procedure on page 2-278](#) for it. The procedure is similar.
- Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card. (A reset standby card remains standby.)
- If CONTBUS-IO-A is raised on several cards at the same time, complete the [“Reset an Active TCC2/TCC2P Card and Activate the Standby Card” procedure on page 2-278](#).
- Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.
- Step 4** Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
- Step 5** If the CTC reset does not clear the alarm, complete the [“Remove and Reinsert \(Reseat\) Any Card” procedure on page 2-280](#) for the reporting card.
- Step 6** If the reset card has not rebooted successfully, or the alarm has not cleared, call Cisco TAC 1 800 553-2447. If the Cisco TAC technician tells you to reseat the card, complete the [“Remove and Reinsert \(Reseat\) the Standby TCC2/TCC2P Card” procedure on page 2-280](#). If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the [“Physically Replace a Traffic Card” procedure on page 2-281](#).
-

2.7.67 CONTBUS-IO-B

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

SONET Logical Object: EQPT

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

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

Clear the CONTBUS-IO-B Alarm

-
- Step 1** Ensure that the reporting card is physically present in the shelf. Record the card type. Click the **Inventory** tab and view the Eqpt Type column to reveal the provisioned type.
- If the actual card type and the provisioned card type do not match, see the [“MEA \(EQPT\)” alarm on page 2-188](#) for the reporting card.
- Step 2** If the alarm object is any single card slot other than the standby Slot 7 TCC2/TCC2P, perform a CTC reset of the object card. Complete the [“Reset a Traffic Card in CTC” procedure on page 2-278](#). For the LED behavior, see the [“2.8.2 Typical Traffic Card LED Activity During Reset” section on page 2-267](#).
- Step 3** If the alarm object is the standby Slot 7 TCC2/TCC2P, complete the [“Reset a Traffic Card in CTC” procedure on page 2-278](#) for it. The procedure is similar.
- Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card. (A reset standby card remains standby.)
- Step 4** If CONTBUS-IO-B is raised on several cards at the same time, complete the [“Reset an Active TCC2/TCC2P Card and Activate the Standby Card” procedure on page 2-278](#).
- Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.
- Step 5** Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
- Step 6** If the CTC reset does not clear the alarm, complete the [“Remove and Reinsert \(Reseat\) Any Card” procedure on page 2-280](#) for the reporting card.
- Step 7** If the reset card has not rebooted successfully, or the alarm has not cleared, call Cisco TAC 1 800 553-2447. If the Cisco TAC technician tells you to reseat the card, complete the [“Remove and Reinsert \(Reseat\) the Standby TCC2/TCC2P Card” procedure on page 2-280](#). If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the [“Physically Replace a Traffic Card” procedure on page 2-281](#).

2.7.68 CPP-INCAPABLE

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

SONET Logical Object: MLMR

The Card Port Protection (CPP) Incapable alarm indicates that the ML-MR-10 card or port is unable to provide protection. This condition occurs when the Resilient Packet Ring (RPR) interface on the ML-MR-10 card is down, or when the CPP peer slot number is not configured from the Cisco IOS command line interface or the protection group is disabled.

**Note**

For information about provisioning ML-MR-10 Ethernet cards from the Cisco IOS interface, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454*, *Cisco ONS 15454 SDH*, and *Cisco ONS 15327*.

Clear the CPP-INCAPABLE Alarm

-
- Step 1** Ensure that the RPR interface is not in the administratively shutdown state.
 - Step 2** Ensure that the RPR interface is in the line protocol UP state.
 - Step 3** Ensure that the CPP peer slot is configured in Cisco IOS under the protection group configuration.
 - Step 4** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.69 CPP-PEER-NO-RESP

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

SONET Logical Object: MLMR

The CPP Peer No Response alarm is raised if a CPP card that is active does not receive any heartbeat response from its peer card. This happens under the following conditions:

- The peer card is not present in the ONS 15454 chassis.
- The peer card is not configured for protection.
- The protection is disabled on the peer card.
- The peer card is reset.

This alarm is reported against all the ports belonging to a particular group. The ports can be either Gigabit Ethernet, POS, or RPR ports.

Clear CPP-PEER-NO-RESP Condition

-
- Step 1** Ensure that the CPP peer card has not failed, the correct protection configuration is present on both CPP cards, and protection is not disabled on the CPP peer card.
 - Step 2** If the alarm does not clear, log into the Cisco Technical Support Website at <http://www.cisco.com/techsupport> for more information or log into <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml> to obtain a directory of toll-free Technical Support numbers for your country.
-

2.7.70 CTNEQPT-MISMATCH

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

SONET Logical Object: EQPT

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

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

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



Note

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

Clear the CTNEQPT-MISMATCH Condition

-
- Step 1** Determine what kind of card is preprovisioned in the slot:
- In node view, click the **Inventory** tab.
 - View the information for the slot in the **Eqpt Type** and **Actual Eqpt Type** columns.
The Eqpt Type column contains the equipment that is provisioned in the slot. The Actual Eqpt Type contains the equipment that is physically present in the slot. For example, Slot 8 could be provisioned for an XCVT card, which is shown in the Eqpt Type column, but an XC10G XC10G card could be physically present in the slot. The XC10G would be shown in the Actual Eqpt Type column.
- Step 2** Complete the "[Physically Replace a Traffic Card](#)" procedure on page 2-281 for the mismatched card.
- Step 3** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.71 CTNEQPT-PBPROT

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

SONET Logical Object: EQPT

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

**Note**

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

**Caution**

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

Clear the CTNEQPT-PBPROT Alarm

- Step 1** If all traffic cards show CTNEQPT-PBPROT alarm, complete the following steps:
- Complete the [“Remove and Reinsert \(Reseat\) the Standby TCC2/TCC2P Card” procedure on page 2-280](#) for the standby TCC2/TCC2P.
 - If the reseat fails to clear the alarm, complete the [“Physically Replace a Traffic Card” procedure on page 2-281](#) for the standby TCC2/TCC2P.

**Caution**

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

- Step 2** If not all cards show the alarm, perform a CTC reset on the standby XC10G card. Complete the [“Reset a Traffic Card in CTC” procedure on page 2-278](#). For the LED behavior, see the [“2.8.2 Typical Traffic Card LED Activity During Reset” section on page 2-267](#).
- Step 3** Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
- If the cross-connect reset is not complete and error-free or if the TCC2/TCC2P reboots automatically, call Cisco TAC 1 800 553-2447.
- Step 4** If the alarm does not clear, complete the [“Remove and Reinsert \(Reseat\) Any Card” procedure on page 2-280](#) for the standby OC-192 card.
- Step 5** Determine whether the card is an active card or standby card in a protection group. Click the node view **Maintenance > Protection** tabs, then click the protection group. The cards and their status are displayed in the list.
- Step 6** If the reporting traffic card is the active card in the protection group, complete the [“Initiate a 1:1 Card Switch Command” procedure on page 2-272](#). After you move traffic off the active card, or if the reporting card is standby, continue with the following steps.
- Step 7** Complete the [“Reset a Traffic Card in CTC” procedure on page 2-278](#) on the reporting card. For the LED behavior, see the [“2.8.2 Typical Traffic Card LED Activity During Reset” section on page 2-267](#).
- Step 8** Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
- Step 9** If the alarm does not clear, complete the [“Remove and Reinsert \(Reseat\) Any Card” procedure on page 2-280](#) for the reporting card.
- Step 10** Complete the [“Initiate a 1:1 Card Switch Command” procedure on page 2-272](#) to switch traffic back.

- Step 11** If the alarm does not clear, complete the [“Physically Replace a Traffic Card” procedure on page 2-281](#) for the reporting traffic card.
- Step 12** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.

2.7.72 CTNEQPT-PBWORK

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

SONET Logical Object: EQPT

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



Note

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

Clear the CTNEQPT-PBWORK Alarm

- Step 1** If all traffic cards show CTNEQPT-PBWORK alarm, complete the following steps:
- Complete the [“Reset an Active TCC2/TCC2P Card and Activate the Standby Card” procedure on page 2-278](#) for the active TCC2/TCC2P and then complete the [“Remove and Reinsert \(Reseat\) the Standby TCC2/TCC2P Card” procedure on page 2-280](#).
 - If the reseat fails to clear the alarm, complete the [“Physically Replace a Traffic Card” procedure on page 2-281](#) for the TCC2/TCC2P.



Caution

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



Caution

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

- Step 2** If all cards do not show the alarm, complete the [“Side Switch the Active and Standby Cross-Connect Cards” procedure on page 2-278](#) for the active XC10G card.
- Step 3** Complete the [“Reset a Traffic Card in CTC” procedure on page 2-278](#) for the reporting card. For the LED behavior, see the [“2.8.2 Typical Traffic Card LED Activity During Reset” section on page 2-267](#).
- Step 4** Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
- Step 5** If the alarm does not clear, complete the [“Remove and Reinsert \(Reseat\) Any Card” procedure on page 2-280](#) for the standby cross-connect card.

- Step 6** If the alarm does not clear and the reporting traffic card is the active card in the protection group, complete the [“Initiate a 1:1 Card Switch Command” procedure on page 2-272](#). If the card is standby, or if you have moved traffic off the active card, proceed with the following steps.
- Step 7** Complete the [“Reset a Traffic Card in CTC” procedure on page 2-278](#) for the reporting card. For the LED behavior, see the [“2.8.2 Typical Traffic Card LED Activity During Reset” section on page 2-267](#).
- Step 8** Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
- Step 9** If the CTC reset does not clear the alarm, complete the [“Remove and Reinsert \(Reseat\) Any Card” procedure on page 2-280](#) for the reporting card.
- Step 10** If you switched traffic, complete the [“Initiate a 1:1 Card Switch Command” procedure on page 2-272](#) to revert the traffic.
- Step 11** If the alarm does not clear, complete the [“Physically Replace a Traffic Card” procedure on page 2-281](#) for the OC-192 card.
- Step 12** If the alarm does not clear, complete the [“Physically Replace a Traffic Card” procedure on page 2-281](#) for the reporting traffic card.
- Step 13** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.

2.7.73 DATA-CRC

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

SONET Logical Objects: CE100T, ML100T, ML1000, MLFX

The data cyclic redundancy check (CRC) Bad Packet Count Exceeds Threshold alarm indicates that Cisco proprietary ring-wrapping (RPR) has been triggered for an ML-Series card in high-level data link (HDLC) mode, but no SONET or data-level alarm is raised along with the [“RPRW” alarm on page 2-221](#) to indicate the failure.

In a typical scenario that triggers Cisco proprietary RPR protection, the errored node raises RPRW, and SONET or data errors such as the [“TPTFAIL \(ML100T, ML1000, MLFX\)” alarm on page 2-255](#). If, however, a packet-over-SONET (POS) port is placed in down administrative state, the card will raise an RPRW without raising any SONET B3 bit alarms or data alarms. The DATA-CRC alarm accompanies this instance of RPRW to indicate the signal interruption.

Clear the DATA-CRC Alarm

- Step 1** Determine whether the [“RPRW” alarm on page 2-221](#), is raised on the ring. If so, clear it using the appropriate trouble-clearing procedure in this chapter.
- Step 2** If the DATA-CRC alarm does not clear, check whether the alarmed card POS port is in the Down administrative state:
- Double-click the ML-Series card to display the card view.
 - Click the **Provisioning > POS Ports** tabs.

- c. View the port's setting in the Admin State column. If it is Down, verify that both POS ports are properly configured. Refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454*, *Cisco ONS 15454 SDH*, and *Cisco ONS 15327* for configuration information.

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

2.7.74 DATAFLT

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

SONET Logical Object: NE

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



Caution

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

Clear the DATAFLT Alarm

Step 1 Complete the “[Reset an Active TCC2/TCC2P Card and Activate the Standby Card](#)” procedure on [page 2-278](#).

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

2.7.75 DBOSYNC

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

SONET Logical Object: NE

The Standby Database Out Of Synchronization alarm occurs when the standby TCC2/TCC2P database does not synchronize with the active database on the active TCC2/TCC2P.



Caution

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

Clear the DBOSYNC Alarm

Step 1 Save a backup copy of the active TCC2/TCC2P database. Refer to the “Maintain the Node” chapter in the *Cisco ONS 15454 Procedure Guide* for procedures.

Step 2 Make a minor provisioning change to the active database to see if applying a provisioning change clears the alarm:

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

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

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

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

2.7.76 DCU-LOSS-FAIL

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.77 DISCONNECTED

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

SONET Logical Object: SYSTEM

The Disconnected alarm is raised when CTC has been disconnected from the node. The alarm clears when CTC reconnects to the node.

Clear the DISCONNECTED Alarm

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

2.7.78 DS3-MISM

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

SONET Logical Object: DS3

The DS-3 Frame Format Mismatch condition indicates a frame format mismatch on a signal transiting the ONS 15454 DS3XM-6, DS3XM-12, or DS3/EC1-48 card. The condition occurs when the provisioned line type and incoming signal frame format type do not match. For example, if the line type for a DS3XM-6 card is set to C Bit and the incoming signal frame format is detected as M13, then the ONS 15454 reports a DS3-MISM condition.

Clear the DS3-MISM Condition

-
- Step 1** Display the CTC card view for the reporting DS3E-12, DS3I-12, DS3XM-6, DS3XM-12, or DS3/EC1-48 card.
- Step 2** Click the **Provisioning > Line** tabs.

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

2.7.79 DSP-COMM-FAIL

For information about this alarm or condition, refer to the “Alarm Troubleshooting” in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.80 DSP-FAIL

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.81 DUP-IPADDR

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

SONET Logical Object: NE

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

Clear the DUP-IPADDR Alarm

-
- Step 1** Isolate the alarmed node from the other node having the same address:
- Connect to the alarmed node using the Craft port on the TCC2/TCC2P card.
 - Begin a CTC session.
 - In the login dialog window, uncheck the **Network Discovery** check box.
- Step 2** In node view, click the **Provisioning > Network > General** tabs.
- Step 3** In the IP Address field, change the IP address to a unique number.
- Step 4** Click **Apply**.

- Step 5** Restart any CTC sessions that are logged into either of the duplicate IP addresses. (For procedures to log in or log out, refer to the “Connect the PC and Log Into the GUI” chapter in the *Cisco ONS 15454 Procedure Guide*.
- Step 6** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.82 DUP-NODENAME

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

SONET Logical Object: NE

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

Clear the DUP-NODENAME Alarm

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

2.7.83 DUP-SHELF-ID

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.84 EFM-RFI-CE

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

SONET Logical Object: MLMR

The ML-MR-10 card does not define the Critical Event, though ML-MR-10 is capable of raising the Remote Failure Indication Critical Event (RFI CE) alarm if the peer interface defines RFI CE.



Note

If the peer device is not an ML-MR-10 card, consult the peer device manual to find the scenarios under which RFI LF is raised.

Clear the EFM-RFI-CE Alarm

Cisco devices do not generate RFI CE events. If a non-Cisco peer device generates an RFI CE event, a Cisco device can raise the EFM-RFI-CE alarm. Check the scenarios under which a non Cisco peer device generates the RFI CE and then clear the condition that lead to the RFI CE.

2.7.85 EFM-RFI-DG

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

SONET Logical Object: MLMR

The EFM Remote Failure Indication Dying Gasp alarm indicates one of the following:

- The peer interface is administratively shut.
- The Ethernet OAM protocol (EFM) is unconfigured on the peer interface.
- The peer card is reloading.

Clear the EFM-RFI-DG Alarm

- Step 1** Check if the peer Ethernet interface is administratively shut down. If it is administratively shut down, restart the Ethernet interface.
- Step 2** Check if the EFM protocol is disabled on the peer Ethernet interface. If it is disabled, enable the EFM protocol on the peer Ethernet interface.
- Step 3** Check if the peer card is rebooting. The alarm clears when the card comes up.



Note If the peer device is not a ML-MR-10, consult the peer device manual to find the scenarios under which RFI DG is raised.

2.7.86 EFM-RFI-LF

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

SONET Logical Object: MLMR

The Remote Failure Indication Link Fault alarm indicates that the peer interface has a carrier loss.

Clear the EFM-RFI-LF Alarm

Check if the CARLOSS alarm exists on the peer Ethernet interface. If it exists, clear the CARLOSS alarm on the peer Ethernet interface to clear the EFM-RFI-LF alarm.



Note If the peer device is not an ML-MR-10 card, consult the peer device manual to find the scenarios under which RFI LF is raised.

2.7.87 EHIBATVG

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

SONET Logical Object: PWR

The Extreme High Voltage Battery alarm occurs in a –48 VDC environment when a battery lead input voltage exceeds the extreme high power threshold. This threshold, with a default value of –56.5 VDC, is user-provisionable. The alarm remains raised until the voltage remains under the threshold for 120 seconds.

Clear the EHIBATVG Alarm

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

2.7.88 ELWBATVG

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

SONET Logical Object: PWR

The Extreme Low Voltage Battery alarm occurs in a –48 VDC environment when a battery lead input voltage falls below the extreme low power threshold. This threshold, with a default value of –40.5 VDC, is user-provisionable. The alarm remains raised until the voltage remains over the threshold for 120 seconds.

Clear the ELWBATVG Alarm

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

2.7.89 ENCAP-MISMATCH-P

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

SONET Logical Object: STSTRM

The Encapsulation C2 Byte Mismatch Path alarm applies to ML-Series Ethernet cards or the CE-1000 card. It occurs when the first three following conditions are met and one of the last two is false:

- The received C2 byte is not 0x00 (unequipped).
- The received C2 byte is not a PDI value.

- The received C2 does not match the expected C2.
- The expected C2 byte is not 0x01 (equipped unspecified).
- The received C2 byte is not 0x01 (equipped unspecified).

(This is in contrast to the “PLM-P” alarm on page 2-200, which must meet all five criteria.) For an ENCAP-MISMATCH-P to be raised, there is a mismatch between the received and expected C2 byte, with either the expected byte or received byte value being 0x01.

For example, an ENCAP-MISMATCH-P alarm is raised if a circuit created between two ML-Series or two CE-1000 cards has generic framing procedure (GFP) framing provisioned on one end and HDLC framing with LEX encapsulation provisioned on the other. The GFP framing card transmits and expects a C2 byte of 0x1B, while the HDLC framing card transmits and expects a C2 byte of 0x01.

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

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

This alarm is demoted by a “PLM-P” condition on page 2-200 or a “PLM-V” condition on page 2-201.



Note

By default, an ENCAP-MISMATCH-P alarm causes an ML-Series or CE-1000 card data link to go down. This behavior can be modified using the command line interface (CLI) command in interface configuration mode: **no pos trigger defect encap**.



Note

For more information about the ML-Series or CE-1000 Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Clear the ENCAP-MISMATCH-P Alarm

- Step 1** Ensure that the correct framing mode is in use on the receive card:
 - a. In node view, double-click the receive ML-Series or CE-1000 card to open the card view.
 - b. Click the **Provisioning > Card** tabs.
 - c. In the Mode drop-down list, ensure that the same mode (GFP or HDLC) is selected. If it is not, choose it and click **Apply**.
- Step 2** Ensure that the correct framing mode is in use on the transmit card, and that it is identical to the receiving card:
 - a. In node view, double-click the transmit ML-Series or CE-1000 card to open the card view.
 - b. Click the **Provisioning > Card** tabs.
 - c. In the Mode drop-down list, ensure that the same mode (GFP or HDLC) is selected. If it is not, choose it and click **Apply**.
- Step 3** If the alarm does not clear, use the CLI to ensure that the remaining settings are correctly configured on the ML-Series or CE-1000 card:

- Encapsulation
- CRC size
- Scrambling state

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

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

2.7.90 EOC

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

SONET Logical Object: OCN

DWDM Logical Object: TRUNK

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

The SDCC consists of three bytes, D1 through D3, in the SONET overhead. The bytes convey information about operation, administration, maintenance, and provisioning (OAM&P). The ONS 15454 uses the DCC on the SONET section layer to communicate network management information.



Warning

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



Warning

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



Warning

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



Note

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

Clear the EOC Alarm

- Step 1** If the “LOS (OCN)” alarm on page 2-168 is also reported, complete the “Clear the LOS (OCN) Alarm” procedure on page 2-169.



Caution

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

- Step 2** If the “SF-L” condition on page 2-229 is reported, complete the “Clear the SF-L Condition” procedure on page 2-229.

- Step 3** If the alarm does not clear on the reporting node, verify the physical connections between the cards and that the fiber-optic cables are configured to carry SDCC traffic. For more information about fiber connections and terminations, refer to the “Install Cards and Fiber-Optic Cable” chapter in the *Cisco ONS 15454 Procedure Guide*.

If the physical connections are correct and configured to carry DCC traffic, ensure that both ends of the fiber span have in-service (IS-NR) ports. Verify that the ACT/SBY LED on each card is green.

- Step 4** When the LEDs on the cards are correctly illuminated, complete the “Verify or Create Node Section DCC Terminations” procedure on page 2-283 to verify that the DCC is provisioned for the ports at both ends of the fiber span.

- Step 5** Repeat [Step 4](#) at the adjacent nodes.

- Step 6** If DCC is provisioned for the ends of the span, verify that the port is active and in service:

- Confirm that the card shows a green LED in CTC or on the physical card.
A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
- To determine whether the port is in service, double-click the card in CTC to open the card view.
- Click the **Provisioning > Line** tabs.
- Verify that the Admin State column lists the port as **IS**.
- If the Admin State column lists the port as OOS,MT or OOS,DSBLD, click the column and click **IS** in the drop-down list. Click **Apply**.



Note

If a port in the IS admin state does not receive a signal, the LOS alarm is raised and the port service state transitions to OOS-AU,FLT.

- Step 7** For all nodes, if the card is in service, use an optical test set to determine whether signal failures are present on fiber terminations. For specific procedures to use the test set equipment, consult the manufacturer.



Caution

Using an optical test set can disrupt service on the OC-N card. It could be necessary to manually switch traffic carrying circuits over to a protection path. Refer to the “2.9.2 Protection Switching, Lock Initiation, and Clearing” section on page 2-269 for commonly used switching procedures.

- Step 8** If no signal failures exist on terminations, measure power levels to verify that the budget loss is within the parameters of the receiver. See the “1.12.3 OC-N Card Transmit and Receive Levels” section on page 1-147 for non-DWDM card levels and refer to the *Cisco ONS 15454 DWDM Reference Manual* for DWDM card levels.

- Step 9** If budget loss is within parameters, ensure that fiber connectors are securely fastened and properly terminated. For more information refer to the “Install Cards and Fiber-Optic Cable” chapter in the *Cisco ONS 15454 Procedure Guide*.
- Step 10** If fiber connectors are properly fastened and terminated, complete the [“Reset an Active TCC2/TCC2P Card and Activate the Standby Card” procedure on page 2-278](#).
Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.
Resetting the active TCC2/TCC2P switches control to the standby TCC2/TCC2P. If the alarm clears when the ONS 15454 node switches to the standby TCC2/TCC2P, the user can assume that the previously active card is the cause of the alarm.
- Step 11** If the TCC2/TCC2P reset does not clear the alarm, delete the problematic SDCC termination:
- From the **View menu in card view, choose Go to Previous View** if you have not already done so.
 - Click the **Provisioning > Comm Channels > SDCC** tabs.
 - Highlight the problematic DCC termination.
 - Click **Delete**.
 - Click **Yes** in the Confirmation Dialog box.
- Step 12** Recreate the SDCC termination. Refer to the “Turn Up Network” chapter in the *Cisco ONS 15454 Procedure Guide* for procedures.
- Step 13** Verify that both ends of the DCC have been recreated at the optical ports.
- Step 14** If the alarm has not cleared, call Cisco TAC 1 800 553-2447. If the Cisco TAC technician tells you to reseal the card, complete the [“Remove and Reinsert \(Reseat\) the Standby TCC2/TCC2P Card” procedure on page 2-280](#). If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the [“Physically Replace a Traffic Card” procedure on page 2-281](#).

2.7.91 EOC-L

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

SONET Logical Object: OCN

DWDM Logical Object: TRUNK

The Line DCC (LDCC) Termination Failure alarm occurs when the ONS 15454 loses its line data communications channel (LDCC) termination. In DWDM configurations, for example, the OSCM card can raise this alarm on its OC-3 line overhead.

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



Warning

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

**Warning**

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

**Warning**

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

**Note**

If a circuit shows a partial status when the [“EOC” alarm on page 2-86](#), or EOC-L is raised, it occurs when the logical circuit is in place. The circuit is able to carry traffic when the DCC termination issue is resolved. You do not need to delete the circuit when troubleshooting this alarm.

Clear the EOC-L Alarm

- Step 1** Complete the [“Clear the EOC Alarm” procedure on page 2-87](#).
- Step 2** If the alarm has not cleared, call Cisco TAC 1 800 553-2447. If the Cisco TAC technician tells you to reseat the card, complete the [“Remove and Reinsert \(Reseat\) the Standby TCC2/TCC2P Card” procedure on page 2-280](#). If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the [“Physically Replace a Traffic Card” procedure on page 2-281](#).

2.7.92 EQPT

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

SONET Logical Objects: AICI-AEP, AICI-AIE, EQPT

DWDM Logical Object: PPM

An Equipment Failure alarm indicates that a hardware failure has occurred on the reporting card. If the EQPT alarm occurs with a BKUPMEMP alarm, refer to the [“BKUPMEMP” alarm on page 2-58](#). The BKUPMEMP procedure also clears the EQPT alarm.

This alarm is also invoked if a diagnostic circuit detects a card application-specific integrated circuit (ASIC) failure. In this case, if the card is part of a protection group, an APS switch occurs. If the card is the protect card, switching is inhibited and a [“PROTNA” alarm on page 2-203](#) is raised. The standby path generates a path-type alarm.

Clear the EQPT Alarm

- Step 1** If traffic is active on the alarmed port, you could need to switch traffic away from it. See the [“2.9.2 Protection Switching, Lock Initiation, and Clearing” section on page 2-269](#) for commonly used traffic-switching procedures.
- Step 2** Complete the [“Reset a Traffic Card in CTC” procedure on page 2-278](#) for the reporting card. For LED behavior, see the [“2.8.2 Typical Traffic Card LED Activity During Reset” section on page 2-267](#).

- Step 3** Verify that the reset is complete and error-free and that no new related alarms appear in CTC. Verify the LED status. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
 - Step 4** If the CTC reset does not clear the alarm, complete the [“Remove and Reinsert \(Reseat\) Any Card” procedure on page 2-280](#) for the reporting card.
 - Step 5** If the physical reseat of the card fails to clear the alarm, complete the [“Physically Replace a Traffic Card” procedure on page 2-281](#) for the reporting card.
 - Step 6** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.
-

2.7.93 EQPT-DIAG

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

SONET Logical Object: EQPT

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

Clear the EQPT-DIAG Alarm

-
- Step 1** If traffic is active on the alarmed card, you could need to switch traffic away from it. Refer to the [“2.9.2 Protection Switching, Lock Initiation, and Clearing” section on page 2-269](#) for procedures.
 - Step 2** Complete the [“Remove and Reinsert \(Reseat\) Any Card” procedure on page 2-280](#) for the alarmed card.
 - Step 3** If the alarm does not clear, complete the [“Physically Replace a Traffic Card” procedure on page 2-281](#) if it is raised against a traffic card, or complete the [“Physically Replace an In-Service Cross-Connect Card” procedure on page 2-281](#) if the alarm is raised against the cross-connect card.
 - Step 4** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.94 EQPT-MISS

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

SONET Logical Object: FAN

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



Caution

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

Clear the EQPT-MISS Alarm

-
- | | |
|---------------|---|
| Step 1 | If the alarm is reported against the fan, verify that the fan-tray assembly is present. |
| Step 2 | If the fan-tray assembly is present, complete the “Replace the Fan-Tray Assembly” procedure on page 2-288 . |
| Step 3 | If no fan-tray assembly is present, obtain a fan-tray assembly and refer to the “Install the Fan-Tray Assembly,” procedure in the <i>Cisco ONS 15454 Procedure Guide</i> . |
| Step 4 | If the alarm does not clear, replace the ribbon cable from the AIP to the system board with a known-good ribbon cable. |
| Step 5 | If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem. |
-

2.7.95 ERFI-P-CONN

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

SONET Logical Objects: STSMON, STSTRM

The Three-Bit (Enhanced) Remote Failure Indication (ERFI) Path Connectivity condition is triggered on DS-1, DS-3, or VT circuits when the [“UNEQ-P” alarm on page 2-258](#) and the [“TIM-P” alarm on page 2-251](#) are raised on the transmission signal.

Clear the ERFI-P-CONN Condition

-
- | | |
|---------------|---|
| Step 1 | Complete the “Clear the UNEQ-P Alarm” procedure on page 2-259 . This should clear the ERFI condition. |
| Step 2 | If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC 1 800 553-2447. |
-

2.7.96 ERFI-P-PAYLD

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

SONET Logical Objects: STSMON, STSTRM

The Three-Bit ERFI Path Payload condition is triggered on DS-1, DS-3, or VT circuits when the [“PLM-P” alarm on page 2-200](#) is raised on the transmission signal.

Clear the ERFI-P-PAYLD Condition

-
- | | |
|---------------|--|
| Step 1 | Complete the “Clear the PLM-P Alarm” procedure on page 2-201 . This should clear the ERFI condition. |
|---------------|--|
-

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

2.7.97 ERFI-P-SRVR

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

SONET Logical Objects: STSMON, STSTRM

The Three-Bit ERFI Path Server condition is triggered on DS-1, DS-3, or VT circuits when the “AIS-P” condition on page 2-39 or the “LOP-P” alarm on page 2-158 is raised on the transmission signal.

Clear the ERFI-P-SRVR Condition

- Step 1** Complete the “Clear the LOP-P Alarm” procedure on page 2-159. This should clear the ERFI condition.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

2.7.98 ERROR-CONFIG

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

SONET Logical Object: EQPT

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

The typical reasons for an errored startup file are:

- The user stored the configuration for one type of ML-Series card in the database and then installed another type in its slot.
- The configuration file contained a syntax error on one of the lines.
- The user stored the configuration for the ML-Series card and then changed the card mode from RPR-IEEE mode to another mode, or vice versa.



Note

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

Clear the ERROR-CONFIG Alarm

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

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

- Step 2** Upload the configuration file to the TCC2/TCC2P:
- In node view, right-click the ML-Series card graphic.
 - Choose **IOS Startup Config** from the shortcut menu.
 - Click **Local > TCC** and navigate to the file location in the Open dialog box.
- Step 3** Complete the “[Reset a Traffic Card in CTC](#)” procedure on page 2-278.
- Step 4** If the alarm does not clear or if your configuration file was correct according to the installed card, start a Cisco IOS CLI for the card:
- Right click the ML-Series card graphic in node view.
 - Choose **Open IOS Connection** from the shortcut menu.



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

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

- Step 5** Execute the CLI command:
- ```
router(config)#copy run start
```
- The command copies the new card configuration into the database and clears the alarm.
- Step 6** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

## 2.7.99 ETH-LINKLOSS

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

SONET Logical Object: NE

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

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



**Note**

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

## Clear the ETH-LINKLOSS Condition

- 
- Step 1** To clear this condition, reconnect the backplane LAN cable. Refer to the “Install the Shelf and Backplane Cable” chapter in the *Cisco ONS 15454 Procedure Guide* for procedures to install this cable.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
- 

## 2.7.100 E-W-MISMATCH

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

SONET Logical Object: OCN

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



### Note

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



### Note

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



### Note

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

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

- 
- Step 1** Diagram the ring setup, including nodes and spans, on a piece of paper or white board.
- Step 2** In node view, click **View > Go to Network View**.
- Step 3** Click the circuit and click **Edit**. The network map detailed view window appears. This window contains the node name, slot, and port for each end of each span.
- Step 4** Label each of the nodes on the diagram with the same name that appears on the network map.

- Step 5** Label the span ends on the diagram with the same information. For example, with Node 1/Slot 12/Port 1—Node 2/Slot 6/Port 1 (2F BLSR OC48, ring name=0), label the end of the span that connects Node 1 and Node 2 at the Node 1 end as Slot 12/Port 1. Label the Node 2 end of that same span Slot 6/Port 1.
- Step 6** Repeat Steps 4 and 5 for each span on your diagram.
- Step 7** Label the highest slot at each node east and the lowest slot at each node west.
- Step 8** Examine the diagram. You should see a clockwise pattern of west slots connecting to east slots for each span. Refer to the “Install Cards and Fiber-Optic Cable” chapter in the *Cisco ONS 15454 Procedure Guide* for more information about cabling the system.
- Step 9** If any span has an east-to-east or west-to-west connection, physically switching the fiber connectors from the card that does not fit the pattern to the card that continues the pattern should clear the alarm.

**Warning**

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

**Warning**

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

**Warning**

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

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

## Clear the E-W-MISMATCH Alarm in CTC

- Step 1** Log into the misconnected node. A misconnected node has both ring fibers connecting it to its neighbor nodes misconnected.
- Step 2** Click the **Maintenance > BLSR** tabs.
- Step 3** From the row of information for the fiber span, complete the “[Identify a BLSR Ring Name or Node ID Number](#)” procedure on page 2-268 to identify the node ID, ring name, and the slot and port in the East Line column and West Line column. Record the above information.
- Step 4** Click **View > Go to Network View**.
- Step 5** Delete and recreate the BLSR:
- Click the **Provisioning > BLSR** tabs.
  - Click the row from Step 3 to select it and click **Delete**.
  - Click **Create**.

- d. Fill in the ring name and node ID from the information collected in [Step 3](#).
- e. Click **Finish**.

- Step 6** Display node view and click the **Maintenance > BLSR** tabs.
- Step 7** Change the West Line field to the slot you recorded for the East Line in [Step 3](#).
- Step 8** Change the East Line field to the slot you recorded for the West Line in [Step 3](#).
- Step 9** Click **OK**.
- Step 10** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.
- 

## 2.7.101 EXCCOL

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

SONET Logical Object: EQPT

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

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

### Clear the EXCCOL Alarm

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

## 2.7.102 EXERCISE-RING-FAIL

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

SONET Logical Object: OCN

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

**Note**

If the exercise command gets rejected due to the existence of a higher-priority condition in the ring, EXERCISE-RING-FAIL is Not Reported (NR).

## Clear the EXERCISE-RING-FAIL Condition

- Step 1** Look for and clear, if present, the “LOF (OCN)” alarm on page 2-155, the “LOS (OCN)” alarm on page 2-168, or a BLSR alarm.
- Step 2** Complete the “Initiate an Exercise Ring Switch on a BLSR” procedure on page 2-276.
- Step 3** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

## 2.7.103 EXERCISE-SPAN-FAIL

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

SONET Logical Object: OCN

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

**Note**

If the exercise command gets rejected due to the existence of a higher-priority condition in the span or ring, EXERCISE-SPAN-FAIL is Not Reported (NR).

## Clear the EXERCISE-SPAN-FAIL Condition

- Step 1** Look for and clear, if present, the “LOF (OCN)” alarm on page 2-155, the “LOS (OCN)” alarm on page 2-168, or a BLSR alarm.
- Step 2** Complete the “Initiate an Exercise Ring Switch on a BLSR” procedure on page 2-276.
- Step 3** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

## 2.7.104 EXT

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

SONET Logical Object: ENVALRM

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

## Clear the EXT Alarm

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

## 2.7.105 EXTRA-TRAF-PREEMPT

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

SONET Logical Object: OCN

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

## Clear the EXTRA-TRAF-PREEMPT Alarm

- 
- Step 1** Verify that the protection switch has occurred by checking the Conditions tab.
  - Step 2** If a ring switch has occurred, clear the ring switch on the working system by following the appropriate alarm in this chapter. For more information about protection switches, refer to the “[2.9.2 Protection Switching, Lock Initiation, and Clearing](#)” section on page 2-269 or the “Maintain the Node” chapter in the *Cisco ONS 15454 Procedure Guide*.
  - Step 3** If the alarm occurred on a four-fiber BLSR and the span switch occurred on this OC-N, clear the span switch on the working system.
  - Step 4** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.
- 

## 2.7.106 FAILTOSW

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

SONET Logical Objects: EQPT, OCN

DWDM Logical Objects: 2R, ESCON, FC, GE, ISC, TRUNK

The Failure to Switch to Protection Facility condition occurs when a working or protect electrical or optical facility switches to its companion port by using a MANUAL command. For example, if you attempt to manually switch traffic from an unused protect port to an in-service working port, the switch will fail (because traffic is already present on the working port) and you will see the FAILTOSW condition.

## Clear the FAILTOSW Condition

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



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

- Step 2** If the condition does not clear, replace the working electrical or optical card that is reporting the higher-priority alarm by following the [“Physically Replace a Traffic Card” procedure on page 2-281](#). This card is the working electrical or optical card using the protect card and not reporting FAILTOSW. Replacing the working electrical or optical card that is reporting the higher-priority alarm allows traffic to revert to the working slot and the card reporting the FAILTOSW to switch to the protect card.
- Step 3** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

## 2.7.107 FAILTOSW-PATH

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

SONET Logical Objects: STSMON, VT-MON

The Fail to Switch to Protection Path condition occurs when the working circuit does not switch to the protection circuit on a path protection configuration. Common causes of the FAILTOSW-PATH alarm include a missing or defective protect port, a lockout set on one of the path protection nodes, or path-level alarms that would cause a path protection switch to fail including the [“AIS-P” condition on page 2-39](#), the [“LOP-P” alarm on page 2-158](#), the [“SD-P” condition on page 2-226](#), the [“SF-P” condition on page 2-230](#), and the [“UNEQ-P” alarm on page 2-258](#).

The [“LOF \(OCN\)” alarm on page 2-155](#), the [“LOS \(OCN\)” alarm on page 2-168](#), the [“SD-L” condition on page 2-226](#), or the [“SF-L” condition on page 2-229](#) can also occur on the failed path.

## Clear the FAILTOSW-PATH Condition in a Path Protection Configuration

- Step 1** Look up and clear the higher-priority alarm. Clearing this alarm frees the standby card and clears the FAILTOSW-PATH condition. If the [“AIS-P” condition on page 2-39](#), the [“LOP-P” alarm on page 2-158](#), the [“UNEQ-P” alarm on page 2-258](#), the [“SF-P” condition on page 2-230](#), the [“SD-P” condition on page 2-226](#), the [“LOF \(OCN\)” alarm on page 2-155](#), the [“LOS \(OCN\)” alarm on page 2-168](#), the [“SD-L” condition on page 2-226](#), or the [“SF-L” condition on page 2-229](#) are also occurring on the reporting port, complete the applicable alarm clearing procedure.



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

- Step 2** If the condition does not clear, replace the active OC-N card that is reporting the higher-priority alarm. Complete the [“Physically Replace a Traffic Card” procedure on page 2-281](#). Replacing the active OC-N card that is reporting the higher-priority alarm allows traffic to revert to the active slot. Reverting frees the standby card, which can then take over traffic from the card reporting the lower-priority alarm and the FAILTOSW-PATH condition.
- Step 3** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

## 2.7.108 FAILTOSWR

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

SONET Logical Object: OCN

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

FAILTOSWR clears in any of the following situations:

- A physical card pull of the active TCC2/TCC2P (done under Cisco TAC supervision).
- A node power cycle.
- A higher-priority event such as an external switch command.
- The next ring switch succeeds.
- The cause of the APS switch (such as the [“SD-L” condition on page 2-226](#) or the [“SF-L” condition on page 2-229](#)) clears.



### Warning

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



### Warning

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



### Warning

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

## Clear the FAILTOSWR Condition in a BLSR Configuration

- Step 1** Perform the Exercise Ring command on the reporting card:
- Click the **Maintenance > BLSR** tabs.
  - Click the row of the affected ring under the West Switch column.
  - Select **Exercise Ring** in the drop-down list.

- Step 2** If the condition does not clear, from the view menu, choose **Go to Network View**.
- Step 3** Look for alarms on OC-N cards that make up the ring or span and troubleshoot these alarms.
- Step 4** If clearing other alarms does not clear the FAILTOSWR condition, log into the near-end node.
- Step 5** Click the **Maintenance > BLSR** tabs.
- Step 6** Record the OC-N cards listed under West Line and East Line. Ensure that these OC-N cards and ports are active and in service:
- Verify the LED status: A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
  - Double-click the card in CTC to open the card view.
  - Click the **Provisioning > Line** tabs.
  - Verify that the Admin State column lists the port as IS.
  - If the Admin State column lists the port as OOS,MT or OOS,DSBLD, click the column and choose **IS**. Click **Apply**.



**Note** If a port in the IS admin state does not receive a signal, the LOS alarm is raised and the port service state transitions to OOS-AU,FLT.

- Step 7** If the OC-N cards are active and in service, verify fiber continuity to the ports on the recorded cards. To verify fiber continuity, follow site practices.
- Step 8** If fiber continuity to the ports is good, use an optical test set to verify that a valid signal exists on the line. For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving card as possible.



**Caution**

Using an optical test set disrupts service on the OC-N card. It could be necessary to manually switch traffic carrying circuits over to a protection path. Refer to the [“2.9.2 Protection Switching, Lock Initiation, and Clearing”](#) section on page 2-269 for commonly used switching procedures.

- Step 9** If the signal is valid, clean the fiber according to site practice. If no site practice exists, complete the procedure in the “Maintain the Node” chapter in the *Cisco ONS 15454 Procedure Guide*.
- Step 10** If cleaning the fiber does not clear the condition, verify that the power level of the optical signal is within the OC-N card receiver specifications. The [“1.12.3 OC-N Card Transmit and Receive Levels”](#) section on page 1-147 lists these specifications.
- Step 11** Repeat Steps 7 through 10 for any other ports on the card.
- Step 12** If the optical power level for all OC-N cards is within specifications, complete the [“Physically Replace a Traffic Card”](#) procedure on page 2-281 for the protect standby OC-N card.
- Step 13** If the condition does not clear after you replace the BLSR cards on the node one by one, repeat Steps 4 through 12 for each of the nodes in the ring.
- Step 14** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

## 2.7.109 FAILTOSWS

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

SONET Logical Object: OCN

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

- A physical card pull of the active TCC2/TCC2P done under Cisco TAC supervision.
- A node power cycle.
- A higher-priority event such as an external switch command occurs.
- The next span switch succeeds.
- The cause of the APS switch (such as the [“SD-L” condition on page 2-226](#) or the [“SF-L” condition on page 2-229](#)) clears.

### 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 list.
- Step 2** If the condition does not clear, from the view menu, choose **Go to Network View**.
- Step 3** Look for alarms on OC-N cards that make up the ring or span and troubleshoot these alarms.
- Step 4** If clearing other alarms does not clear the FAILTOSWS condition, log into the near-end node.
- Step 5** Click the **Maintenance > BLSR** tabs.
- Step 6** Record the OC-N cards listed under West Line and East Line. Ensure that these OC-N cards are active and in service:
- a. Verify the LED status: A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
  - b. To determine whether the OC-N port is in service, double-click the card in CTC to open the card view.
  - c. Click the **Provisioning > Line** tabs.
  - d. Verify that the Admin State column lists the port as IS.
  - e. If the Admin State column lists the port as OOS,MT or OOS,DSBLD, click the column and choose **IS**. Click **Apply**.



**Note**

If a port in the IS admin state does not receive a signal, the LOS alarm is raised and the port service state transitions to OOS-AU,FLT.

- Step 7** If the OC-N cards are active and in service, verify fiber continuity to the ports on the recorded cards. To verify fiber continuity, follow site practices.
- Step 8** If fiber continuity to the ports is good, use an optical test set to verify that a valid signal exists on the line. For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving card as possible.

**Caution**

Using an optical test set disrupts service on the OC-N card. It could be necessary to manually switch traffic carrying circuits over to a protection path. Refer to the [“2.9.2 Protection Switching, Lock Initiation, and Clearing” section on page 2-269](#) for commonly used switching procedures.

- Step 9** If the signal is valid, clean the fiber according to site practice. If no site practice exists, complete the procedure in the “Maintain the Node” chapter in the *Cisco ONS 15454 Procedure Guide*.
- Step 10** If cleaning the fiber does not clear the condition, verify that the power level of the optical signal is within the OC-N card receiver specifications. The [“1.12.3 OC-N Card Transmit and Receive Levels” section on page 1-147](#) lists these specifications.
- Step 11** Repeat Steps [7](#) through [10](#) for any other ports on the card.
- Step 12** If the optical power level for all OC-N cards is within specifications, complete the [“Physically Replace a Traffic Card” procedure on page 2-281](#) for the protect standby OC-N card.
- Step 13** If the condition does not clear after you replace the BLSR cards on the node one by one, follow Steps [4](#) through [12](#) for each of the nodes in the ring.
- Step 14** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

## 2.7.110 FAN

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

SONET Logical Object: FAN

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

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

**Caution**

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

### Clear the FAN Alarm

- Step 1** Determine whether the air filter needs replacement. Complete the [“Inspect, Clean, and Replace the Reusable Air Filter” procedure on page 2-286](#).
- Step 2** If the filter is clean, complete the [“Remove and Reinsert a Fan-Tray Assembly” procedure on page 2-287](#).

- Step 3** If the fan does not run or the alarm persists, complete the “[Replace the Fan-Tray Assembly](#)” procedure on page 2-288. The fan should run immediately when correctly inserted.
- Step 4** If the replacement fan-tray assembly does not operate correctly, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC to report a Service-Affecting (SA) problem 1 800 553-2447.
- 

## 2.7.111 FAPS

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

SONET Logical Object: FCMR

DWDM Logical Objects: TRUNK

The Fast Automatic Protection Switching condition is applicable to GEXP/10GEXP cards. This condition occurs when the protection port, on the master card, switches from blocking to forwarding state.

### Clear the FAPS Alarm

- Step 1** When the cause of switching disappears, the protection port switches from the forwarding to the blocking state, and the FAPS alarm clears.
- Step 2** If the alarm does not clear even after the protection port switches back to the blocking state, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
- 

## 2.7.112 FAPS-CONFIG-MISMATCH

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

## 2.7.113 FC-DE-NES

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

SONET Logical Object: FCMR

The Fiber Channel Distance Extension Function Not Established condition occurs when the Fiber Channel client setup or distance extension configuration is incorrect.

### Clear the FC-DE-NES Alarm

- Step 1** Ensure that the FC client setup and distance extension configuration is correct.
-

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

## 2.7.114 FC-NO-CREDITS

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

SONET Logical Object: FCMR

DWDM Logical Objects: FC, TRUNK

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

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

### Clear the FC-NO-CREDITS Alarm

- Step 1** If the port is connected to a Fibre Channel/FICON switch, make sure it is configured for interoperation mode using the manufacturer's instructions.
- Step 2** If the port is not connected to a switch, turn off Autodetect Credits:
- Double-click the FC\_MR-4 card.
  - Click **Provisioning > Port > General**.
  - Under Admin State, click the cell and choose **OOS,MT**.
  - Click **Apply**.
  - Click the **Provisioning > Port > Distance Extension** tabs.
  - Uncheck the **Autodetect Credits** column check box.
  - Click **Apply**.
  - Click **Provisioning > Port > General**.
  - Under Admin State, click the cell and choose **IS**.
  - Click **Apply**.



**Note**

If a port in the IS admin state does not receive a signal, the LOS alarm is raised and the port service state transitions to OOS-AU,FLT.

- Step 3** Program the Credits Available value based on the buffers available on the connected equipment:



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

- a. Double-click the FC\_MR-4 card.
- b. Click the **Provisioning > Port > Distance Extension** tabs.
- c. Enter a new value in the Credits Available column.
- d. Click **Apply**.

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

## 2.7.115 FDI

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

## 2.7.116 FE-AIS

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

SONET Logical Object: DS3

The Far-End AIS condition occurs when an AIS has occurred at the far-end node. FE-AIS usually occurs in conjunction with a downstream LOS alarm (see the “[LOS \(OCN\)](#)” alarm on page 2-168).

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

### Clear the FE-AIS Condition

- Step 1** Complete the “[Clear the AIS Condition](#)” procedure on page 2-38.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

## 2.7.117 FEC-MISM

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

## 2.7.118 FE-DS1-MULTLOS

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

SONET Logical Object: DS3

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

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

### Clear the FE-DS1-MULTLOS Condition

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

## 2.7.119 FE-DS1-NSA

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

SONET Logical Object: DS3

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

### Clear the FE-DS1-NSA Condition

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

## 2.7.120 FE-DS1-SA

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

SONET Logical Object: DS3

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

### Clear the FE-DS1-SA Condition

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

## 2.7.121 FE-DS1-SNGLLOS

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

SONET Logical Object: DS3

The Far-End Single DS-1 LOS condition occurs when a single DS-1 signal is lost on far-end DS-1 equipment (within a DS3). Signal loss also causes the “[LOS \(OCN\)](#)” alarm on [page 2-168](#).

### Clear the FE-DS1-SNGLLOS Condition

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

## 2.7.122 FE-DS3-NSA

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

SONET Logical Object: DS3

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

## Clear the FE-DS3-NSA Condition

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

## 2.7.123 FE-DS3-SA

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

SONET Logical Object: DS3

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

## Clear the FE-DS3-SA Condition

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

## 2.7.124 FE-EQPT-NSA

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

SONET Logical Object: DS3

The Far End Common Equipment Failure condition occurs when a Non-Service-Affecting (NSA) equipment failure is detected on far-end DS-3 equipment.

## Clear the FE-EQPT-NSA Condition

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

## 2.7.125 FE-FRCDWKSWBK-SPAN

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

SONET Logical Object: OCN

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



**Note**

---

WKSWBK-type conditions apply only to revertive circuits.

---

## Clear the FE-FRCDWKSWBK-SPAN Condition

- 
- Step 1** Complete the [“Clear a 1+1 Force or Manual Switch Command” procedure on page 2-270](#) for the far-end port.
  - Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
- 

## 2.7.126 FE-FRCDWKSWPR-RING

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

SONET Logical Object: EC1, OCN

The Far End Ring Working Facility Forced to Switch to Protection condition occurs from a far-end node when a BLSR is forced from working to protect using the Force Ring command. This condition is only visible on the network view Conditions tab.

## Clear the FE-FRCDWKS WPR-RING Condition

- 
- Step 1** To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an FE-AIS condition from the OC-48 card in Slot 12 of Node 1 could link to the main AIS condition from an OC-48 card in Slot 6 of Node 2.
- Step 2** Log into the node that links directly to the card reporting the FE condition.
- Step 3** Clear the main alarm.
- Step 4** If the FE-FRCDWKS WPR-RING condition does not clear, complete the [“Clear a BLSR External Switching Command” procedure on page 2-277](#).
- Step 5** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
- 

## 2.7.127 FE-FRCDWKS WPR-SPAN

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

SONET Logical Object: OCN

The Far End Working Facility Forced to Switch to Protection Span condition occurs from a far-end node when a span on a four-fiber BLSR is forced from working to protect using the Force Span command. This condition is only visible on the network view Conditions tab. The port where the Force Switch occurred is indicated by an “F” on the network view detailed circuit map. This condition is accompanied by WKS WPR.

## Clear the FE-FRCDWKS WPR-SPAN Condition

- 
- Step 1** To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an FE-AIS condition from the OC-48 card in Slot 12 of Node 1 could link to the main AIS condition from an OC-48 card in Slot 6 of Node 2.
- Step 2** Log into the node that links directly to the card reporting the FE condition.
- Step 3** Clear the main alarm.
- Step 4** If the FE-FRCDWKS WPR-SPAN condition does not clear, complete the [“Clear a BLSR External Switching Command” procedure on page 2-277](#).
- Step 5** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
- 

## 2.7.128 FE-IDLE

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

SONET Logical Object: DS3

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

## Clear the FE-IDLE Condition

- 
- Step 1** To troubleshoot the FE condition, determine which node and card link directly to the card reporting the FE condition. For example, an FE condition on a card in Slot 12 of Node 1 could relate to a main alarm from a card in Slot 6 of Node 2.
  - Step 2** Log into the node that links directly to the card reporting the FE condition.
  - Step 3** Clear the main alarm by clearing the protection switch. See the [“2.9.2 Protection Switching, Lock Initiation, and Clearing” section on page 2-269](#) for commonly used traffic-switching procedures.
  - Step 4** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
- 

## 2.7.129 FE-LOCKOUTOFPR-SPAN

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

SONET Logical Object: OCN

The Far-End Lock Out of Protection Span condition occurs when a BSLR span is locked out of the protection system from a far-end node using the Lockout Protect Span command. This condition is only seen on the network view Conditions tab and is accompanied by LKOUTPR-S. The port where the lockout originated is marked by an “L” on the network view detailed circuit map.

## Clear the FE-LOCKOUTOFPR-SPAN Condition

- 
- Step 1** To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an FE-AIS condition from the OC-48 card in Slot 12 of Node 1 could link to the main AIS condition from an OC-48 card in Slot 6 of Node 2.
  - Step 2** Log into the node that links directly to the card reporting the FE condition.
  - Step 3** Ensure there is no lockout set. Complete the [“Clear a BLSR External Switching Command” procedure on page 2-277](#).
  - Step 4** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
- 

## 2.7.130 FE-LOF

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

SONET Logical Object: DS3

The Far End LOF condition occurs when a far-end node reports the [“LOF \(DS3\)” alarm on page 2-153](#) in C-bit framing mode.

## Clear the FE-LOF Condition

- 
- Step 1** To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE condition. For example, an FE condition on a card in Slot 12 of Node 1 could relate to a main alarm from a card in Slot 6 of Node 2.
- Step 2** Log into the node that links directly to the card reporting the FE condition.
- Step 3** Complete the “[Clear the LOF \(DS1\) Alarm](#)” procedure on page 2-152. It also applies to FE-LOF.
- Step 4** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
- 

## 2.7.131 FE-LOS

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

SONET Logical Object: DS3

The Far End LOS condition occurs in C-bit framing mode when a far-end node reports the “[LOS \(DS3\)](#)” alarm on page 2-163.

## Clear the FE-LOS Condition

- 
- Step 1** To troubleshoot the FE condition, determine which node and card link directly to the card reporting the FE condition. For example, an FE condition on a card in Slot 12 of Node 1 could relate to a main alarm from a card in Slot 6 of Node 2.
- Step 2** Log into the node that links directly to the card reporting the FE condition.
- Step 3** Complete the “[Clear the LOS \(DS1\) Alarm](#)” procedure on page 2-162.
- Step 4** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
- 

## 2.7.132 FE-MANWKSWBK-SPAN

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

SONET Logical Object: OCN

The Far End Manual Switch Back to Working—Span condition occurs when a far-end span with a Manual switch reverts to working.



### Note

---

WKSWBK-type conditions such as FE-MANWKSWBK-SPAN apply only to nonrevertive spans.

---

## Clear the FE-MANWKSWBK-SPAN Condition

- 
- Step 1** To troubleshoot the FE condition, determine which node and card link directly to the card reporting the FE condition. For example, an FE condition on a card in Slot 12 of Node 1 could relate to a main alarm from a card in Slot 6 of Node 2.
  - Step 2** Log into the node that links directly to the card reporting the FE condition.
  - Step 3** Complete the [“Clear a BLSR External Switching Command” procedure on page 2-277](#).
  - Step 4** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
- 

## 2.7.133 FE-MANWKSWPR-RING

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

SONET Logical Object: EC1, OCN

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

## Clear the FE-MANWKSWPR-RING Condition

- 
- Step 1** To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an FE-AIS condition from the OC-48 card in Slot 12 of Node 1 could link to the main AIS condition from an OC-48 card in Slot 6 of Node 2.
  - Step 2** Log into the node that links directly to the card reporting the FE condition.
  - Step 3** Complete the [“Clear a BLSR External Switching Command” procedure on page 2-277](#).
  - Step 4** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
- 

## 2.7.134 FE-MANWKSWPR-SPAN

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

SONET Logical Object: OCN

The Far-End Span Manual Switch Working Facility to Protect condition occurs when a four-fiber BLSR span is switched from working to protect at the far-end node using the Manual Span command. This condition is only visible on the network view Conditions tab and is accompanied by WKSWPR. The port where the Manual Switch occurred is indicated by an “M” on the network view detailed circuit map.

## Clear the FE-MANWKSWPR-SPAN Condition

- 
- Step 1** To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an FE-AIS condition from the OC-48 card in Slot 12 of Node 1 could link to the main AIS condition from an OC-48 card in Slot 6 of Node 2.
- Step 2** Log into the node that links directly to the card reporting the FE condition.
- Step 3** Complete the “[Clear a BLSR External Switching Command](#)” procedure on page 2-277.
- Step 4** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
- 

## 2.7.135 FEPRLF

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

SONET Logical Object: OCN

The Far End Protection Line Failure alarm occurs when an APS channel “[SF-L](#)” condition on page 2-229 occurs on the protect card coming into the node.



**Note**

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

---

## Clear the FEPRLF Alarm on a Four-Fiber BLSR

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

## 2.7.136 FIBERTEMP-DEG

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

## 2.7.137 FORCED-REQ

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

SONET Logical Objects: EQPT, ML1000, ML100T, MLFX, STSMON, VT-MON

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

FORCED-REQ is raised for an IEEE 802.17b-based RPR span if the force was requested in the Cisco IOS CLI using the “rpr-ieee protection request force-switch {east | west}” command. It clears from the IEEE 802.17b-based RPR span when you remove the switch in the CLI. For the IEEE 802.17b-based RPR interface, FORCED-REQ is suppressed by the “RPR-PASSTHR” alarm on page 2-215. It also suppresses the following alarms:

- MAN-REQ, page 183
- RPR-SF, page 220
- RPR-SD, page 219
- WTR, page 266

## Clear the FORCED-REQ Condition

- 
- Step 1** If the condition is raised on a SONET entity, complete the “Clear a 1+1 Force or Manual Switch Command” procedure on page 2-270.
- Step 2** If the condition is raised on an IEEE-802.17b-based RPR span, enter the following command in the CLI in RPR-IEEE interface configuration mode:
- ```
router(config-if)#no rpr-ieee protection request force-switch {east | west}
```
- Step 3** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.138 FORCED-REQ-RING

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

SONET Logical Object: OCN

The Force Switch Request Ring condition applies to optical trunk cards when the Force Ring command is applied to BLSRs to move traffic from working to protect. This condition is visible on the network view Alarms, Conditions, and History tabs and is accompanied by the “WKSWPR” alarm on page 2-265. The port where the FORCE RING command originated is marked with an “F” on the network view detailed circuit map.

Clear the FORCED-REQ-RING Condition

-
- Step 1** Complete the “Clear a BLSR External Switching Command” procedure on page 2-277.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.139 FORCED-REQ-SPAN

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

SONET Logical Object: EC1, OCN

DWDM Logical Objects: 2R, ESCON, FC, GE, ISC, TRUNK

The Force Switch Request Span condition can apply to optical trunk cards in two-fiber or four-fiber BLSRs when the Force Span command is applied to a BLSR SPAN to force traffic from working to protect or from protect to working. This condition appears on the network view Alarms, Conditions, and History tabs. The port where the FORCE SPAN command was applied is marked with an “F” on the network view detailed circuit map.

FORCED-REQ can be raised in 1+1 facility protection groups. If traffic is present on a working port and you use the FORCE command to prevent it from switching to the protect port (indicated by “FORCED TO WORKING”), FORCED-REQ-SPAN indicates this force switch. In this case, the force is affecting not only the facility, but the span.

Clear the FORCED-REQ-SPAN Condition

-
- Step 1** Complete the [“Clear a BLSR External Switching Command” procedure on page 2-277](#).
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.140 FP-LINK-LOSS

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

SONET Logical Object: EQPT

The Front Port Link Loss condition occurs when a LAN cable is not connected to the front port of the TCC2/TCC2P card.

Clear the FP-LINK-LOSS Condition

-
- Step 1** Connect a LAN cable to the front port of the TCC2/TCC2P card.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.141 FRCDSWTOINT

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

SONET Logical Object: NE-SREF

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

**Note**

FRCDSWTOINT is an informational condition and does not require troubleshooting.

2.7.142 FRCDSWTOPRI

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

SONET Logical Objects: EXT-SREF, NE-SREF

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

**Note**

FRCDSWTOPRI is an informational condition and does not require troubleshooting.

2.7.143 FRCDSWTOSEC

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

SONET Logical Objects: EXT-SREF, NE-SREF

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

**Note**

FRCDSWTOSEC is an informational condition and does not require troubleshooting.

2.7.144 FRCDSWTOTHIRD

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

SONET Logical Objects: EXT-SREF, NE-SREF

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

**Note**

FRCDSWTOTHIRD is an informational condition and does not require troubleshooting.

2.7.145 FRNGSYNC

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

SONET Logical Object: NE-SREF

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

**Note**

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

Clear the FRNGSYNC Condition

-
- Step 1** If the ONS 15454 is configured to operate from an external timing source, verify that the BITS timing source is valid. Common problems with a BITS timing source include reversed wiring and bad timing cards. Refer to the “Timing” chapter in the *Cisco ONS 15454 Reference Manual* for more information.
- Step 2** If the BITS source is valid, clear alarms related to the failures of the primary and secondary reference sources, such as the “SYNCPRI” alarm on page 2-247 and the “SYNCSEC” alarm on page 2-248.
- Step 3** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.146 FSTSYNC

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

SONET Logical Object: NE-SREF

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

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

**Note**

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

2.7.147 FTA-MISMATCH

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.148 FULLPASSTHR-BI

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

SONET Logical Object: OCN

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

Clear the FULLPASSTHR-BI Condition

-
- Step 1** Complete the “[Clear a BLSR External Switching Command](#)” procedure on page 2-277.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.149 GAIN-HDEG

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.150 GAIN-HFAIL

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.151 GAIN-LDEG

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.152 GAIN-LFAIL

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.153 GCC-EOC

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.154 GE-OOSYNC

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.155 GFP-CSF

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

SONET Logical Objects: CEMR, CE1000, CE100T, FCMR, GFP-FAC, ML1000, ML100T, MLFX

The GFP Client Signal Fail Detected alarm is a secondary alarm raised on local GFP data ports when a remote Service-Affecting (SA) alarm causes invalid data transmission. The alarm is raised locally on FC_MR-4, ML100T, ML1000, ML100X-8, MXP_MR_25G, and MXPP_MR_25G GFP data ports and does not indicate that a Service-Affecting (SA) failure is occurring at the local site, but that a CARLOSS, LOS, or SYNCLOSS alarm caused by an event such as a pulled receive cable is affecting a remote data port's transmission capability. This alarm can be demoted when a facility loopback is placed on the FC_MR-4 port.

**Note**

For more information about provisioning MXP or TXP cards, refer to the *Cisco ONS 15454 DWDM Reference Manual*. For more information about Ethernet cards, refer to the Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.

Clear the GFP-CSF Alarm

-
- Step 1** Clear the Service-Affecting (SA) alarm at the remote data port.
- Step 2** If the GFP-CSF alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 to report a Service-Affecting (SA) problem.
-

2.7.156 GFP-DE-MISMATCH

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

SONET Logical Objects: FCMR, GFP-FAC

The GFP Fibre Channel Distance Extension Mismatch alarm indicates that a port configured for Distance Extension is connected to a port that is not operating in Cisco's proprietary Distance Extension mode. It is raised on Fibre Channel and FICON card GFP ports supporting distance extension. The alarm occurs when distance extension is enabled on one side of the transport but not on the other. To clear, distance extension must be enabled on both ports connected by a circuit.

**Note**

For more information about Ethernet cards, refer to the Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.

Clear the GFP-DE-MISMATCH Alarm

-
- Step 1** Ensure that the distance extension protocol is configured correctly on both sides:
- a. Double-click the card to open the card view.
 - b. Click the **Provisioning > Port > General** tabs.
 - c. Under Admin State, click the cell and choose **OOS,MT**.
 - d. Click **Apply**.
 - e. Click the **Provisioning > Port > Distance Extension** tabs.

- f. Check the check box in the **Enable Distance Extension** column.
- g. Click **Apply**.
- h. Click the **Provisioning > Port > General** tabs.
- i. Under Admin State, click the cell and choose **IS**.
- j. Click **Apply**.

**Note**

If ports managed into IS admin state are not receiving signals, the LOS alarm is either raised or remains, and the port service state transitions to OOS-AU,FLT.

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

2.7.157 GFP-EX-MISMATCH

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

SONET Logical Objects: CE1000, FCMR, GFP-FAC

The GFP Extension Header Mismatch alarm is raised on Fibre Channel/FICON cards when it receives frames with an extension header that is not null. The alarm occurs when a provisioning error causes all GFP frames to be dropped for 2.5 seconds.

Ensure that both end ports are sending a null extension header for a GFP frame. The FC_MR-4 card always sends a null extension header, so if the equipment is connected to other vendors' equipment, those need to be provisioned appropriately.

**Note**

For more information about Ethernet cards, refer to the Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.

Clear the GFP-EX-MISMATCH Alarm

- Step 1** Ensure that the vendor equipment is provisioned to send a null extension header in order to interoperate with the FC_MR-4 card. (The FC_MR-4 card always sends a null extension header.)
- Step 2** If the GFP-EX-MISMATCH alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 to report a Service-Affecting (SA) problem.

2.7.158 GFP-LFD

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

SONET Logical Objects: CEMR, CE1000, CE100T, FCMR, GFP-FAC, ML1000, ML100T, MLFX

The GFP Loss of Frame Delineation alarm applies to Fibre Channel, FICON GFP, and Ethernet ports. This alarm occurs if there is a bad SONET connection, if SONET path errors cause GFP header errors in the check sum calculated over payload length (PLI/cHEC) combination, or if the GFP source port sends an invalid PLI/cHEC combination. The loss causes traffic stoppage.

**Note**

For more information about Ethernet cards, refer to the Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.

Clear the GFP-LFD Alarm

-
- Step 1** Look for and clear any associated SONET path errors such as LOS or AIS-L originating at the transmit node.
- Step 2** If the GFP-LFD alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 to report a Service-Affecting (SA) problem.
-

2.7.159 GFP-NO-BUFFERS

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

SONET Logical Objects: FCMR, GFP-FAC

The GFP Fibre Channel Distance Extension Buffer Starvation alarm is raised on Fibre Channel/FICON card ports supporting GFP and the distance extension protocol when the GFP transmitter cannot send GFP frames due to lack of remote GFP receiver buffers. This occurs when the remote GFP-T receiver experiences congestion and is unable to send frames over the Fibre Channel/FICON link.

This alarm could be raised in conjunction with the [“FC-NO-CREDITS” alarm on page 2-105](#). For example, if the FC-NO-CREDITS alarm is generated at an FC_MR-4 data port, a GFP-NO-BUFFERS alarm could be raised at the upstream remote FC_MR-4 data port.

**Note**

For more information about Ethernet cards, refer to the Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.

Clear the GFP-NO-BUFFERS Alarm

-
- Step 1** Complete the [“Clear the FC-NO-CREDITS Alarm” procedure on page 2-105](#).
- Step 2** If the GFP-CSF alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) to report a Service-Affecting (SA) problem.
-

2.7.160 GFP-UP-MISMATCH

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

SONET Logical Objects: CEMR, CE1000, CE100T, FCMR, GFP-FAC, ML1000, ML100T, MLFX

The GFP User Payload Mismatch is raised against Fibre Channel/FICON ports supporting GFP. It occurs when the received frame user payload identifier (UPI) does not match the transmitted UPI and all frames are dropped. The alarm is caused by a provisioning error, such as the port media type not matching the remote port media type. For example, the local port media type could be set to Fibre Channel—1 Gbps ISL or Fibre Channel—2 Gbps ISL and the remote port media type could be set to FICON—1 Gbps ISL or FICON—2 Gbps ISL.



Note

For more information about Ethernet cards, refer to the Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.

Clear the GFP-UP-MISMATCH Alarm

-
- Step 1** Ensure that the transmit port and receive port are identically provisioned for distance extension by completing the following steps:
- Double-click the card to open the card view.
 - Click the **Provisioning > Port > Distance Extension** tabs.
 - Check the check box in the **Enable Distance Extension** column.
 - Click **Apply**.
- Step 2** Ensure that both ports are set for the correct media type. For each port, complete the following steps:
- Double-click the card to open the card view (if you are not already in card view).
 - Click the **Provisioning > Port > General** tabs.
 - Choose the correct media type (**Fibre Channel - 1Gbps ISL**, **Fibre Channel - 2 Gbps ISL**, **FICON - 1 Gbps ISL**, or **FICON - 2 Gbps ISL**) from the drop-down list.
 - Click **Apply**.
- Step 3** If the GFP-UP-MISMATCH alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 to report a Service-Affecting (SA) problem.
-

2.7.161 HELLO

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

SONET Logical Object: OCN

DWDM Logical Object: TRUNK

The Open Shortest Path First (OSPF) Hello alarm is raised when the two end nodes cannot bring an OSPF neighbor up to the full state. Typically, this problem is caused by an area ID mismatch, and/or an OSPF HELLO packet loss over the DCC.

Clear the HELLO Alarm

-
- Step 1** Ensure that the area ID is correct on the missing neighbor:
- In node view, click the **Provisioning > Network > OSPF** tabs.
 - Ensure that the IP address in the Area ID column matches the other nodes.
 - If the address does not match, click the incorrect cell and correct it.
 - Click **Apply**.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.162 HIBATVG

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

SONET Logical Object: PWR

The High Voltage Battery alarm occurs in a –48 VDC environment when a battery lead input voltage exceeds the high power threshold. This threshold, with a default value of –52 VDC, is user-provisionable. The alarm remains raised until the voltage remains under the threshold for 120 seconds. (For information about changing this threshold, refer to the “Turn Up Node” chapter in the *Cisco ONS 15454 Procedure Guide*.)

Clear the HIBATVG Alarm

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

2.7.163 HI-CCVOLT

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

SONET Logical Object: BITS

The 64K Composite Clock High NE Voltage alarm occurs when the 64K signal peak voltage exceeds 1.1 VDC.

Clear the HI-CCVOLT Condition

-
- Step 1** Lower the source voltage to the clock.
- Step 2** If the condition does not clear, add more cable length or add a 5 dBm attenuator to the cable.

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

2.7.164 HI-LASERBIAS

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

SONET Logical Objects: EQPT, OCN

DWDM Logical Objects: 2R, ESCON, FC, GE, ISC, PPM, TRUNK

The Equipment High Transmit Laser Bias Current alarm is raised against TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, MXP_2.5G_10G, MRC-12, MRC-4, and OC192-XFP card laser performance. The alarm indicates that the card laser has reached the maximum laser bias tolerance.

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



Note

For more information about provisioning MXP or TXP PPMs, refer to the “Provision Transponders and Muxponders” chapter of the *Cisco ONS 15454 DWDM Procedure Guide*. For more information about the cards themselves, refer to the *Cisco ONS 15454 DWDM Reference Manual*.

Clear the HI-LASERBIAS Alarm

- Step 1** Complete the “[Clear the LASEREOL Alarm](#)” procedure on page 2-141, which can include replacing the card. Replacement is not urgent and can be scheduled during a maintenance window.



Caution

Removing an active card can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the “[2.9.2 Protection Switching, Lock Initiation, and Clearing](#)” section on page 2-269 for commonly used traffic-switching procedures.

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

2.7.165 HI-LASERTEMP

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

SONET Logical Objects: EQPT, OCN

DWDM Logical Object: PPM

The Equipment High Laser Optical Transceiver Temperature alarm applies to the TXP and MXP cards. HI-LASERTEMP occurs when the internally measured transceiver temperature exceeds the card setting by 35.6 degrees F (2 degrees C). A laser temperature change affects the transmitted wavelength.

When the TXP or MXP card raises this alarm, the laser is automatically shut off. The [“LOS \(OCN\)” alarm on page 2-168](#) is raised at the far-end node and the [“DUP-IPADDR” alarm on page 2-81](#) is raised at the near end.

**Note**

For more information about provisioning MXP or TXP PPMs, refer to the “Provision Transponder and Muxponder Cards” chapter of the *Cisco ONS 15454 DWDM Procedure Guide*. For more information about the cards themselves, refer to the *Cisco ONS 15454 DWDM Reference Manual*.

Clear the HI-LASERTEMP Alarm

-
- Step 1** In node view, double-click the TXP or MXP card to open the card view.
 - Step 2** Click the **Performance > Optics PM > Current Values** tabs.
 - Step 3** Verify the card laser temperature levels. Maximum, minimum, and average laser temperatures are shown in the Current column entries in the Laser Temp rows.
 - Step 4** Complete the [“Reset a Traffic Card in CTC” procedure on page 2-278](#) for the MXP or TXP card.
 - Step 5** If the alarm does not clear, complete the [“Physically Replace a Traffic Card” procedure on page 2-281](#) for the reporting MXP or TXP card.
 - Step 6** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.166 HI-RXPOWER

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

SONET Logical Object: OCN

DWDM Logical Objects: 2R, ESCON, FC, GE, ISC, TRUNK

The Equipment High Receive Power alarm is an indicator of the optical signal power that is transmitted to the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, MXP_2.5G_10G, MRC-12, MRC-4, or OC192-XFP card. HI-RXPOWER occurs when the measured optical power of the received signal exceeds the threshold. The threshold value is user-provisionable.

**Note**

For more information about MXP or TXP cards, refer to the *Cisco ONS 15454 DWDM Reference Manual*.

**Note**

When you upgrade a node to Software Release 6.0 or later, this enables received optical power PMs for the OC3-8, OC192-SR, OC192-IR, OC192-ITU, OC-192-XFP, MRC-12, and MRC25G-4 cards. The newly enabled HI-RXPOWER and LO-RXPOWER alarms require that you initialize a site-accepted optical power (OPR0) nominal value after the upgrade. (To do this, refer to the procedure in the “Turn

Up a Node” chapter in the *Cisco ONS 15454 Procedure Guide*.) When you apply the value change, CTC uses the new OPR0 value to calculate PM percentage values. If you do not change the nominal value, the HI-RXPOWER or LO-RXPOWER may be raised in response to the unmodified setting.

Clear the HI-RXPOWER Alarm

-
- Step 1** Find out whether gain (the amplification power) of any amplifiers has been changed. This change also causes channel power to need adjustment.
- Step 2** Find out whether channels have been dropped from the fiber. Increasing or decreasing channels can affect power. If channels have been dropped, the power levels of all channels have to be adjusted.
-  **Note** If the card is part of an amplified DWDM system, dropping channels on the fiber affects the transmission power of each channel more than it would in an unamplified system.
-
- Step 3** At the transmit end of the errored circuit, decrease the transmit power level within safe limits.
- Step 4** If neither of these problems cause the HI-RXPOWER alarm, there is a slight possibility that another wavelength is drifting on top of the alarmed signal. In this case, the receiver gets signals from two transmitters at the same time and data alarms would be present. If wavelengths are drifting, the data is garbled and receive power increases by about +3 dBm.
- Step 5** If the alarm does not clear, add fiber attenuators to the receive ports. Start with low-resistance attenuators and use stronger ones as needed, depending on factors such as the transmission distance, according to standard practice.
- Step 6** If the alarm does not clear and no faults are present on the other port(s) of the transmit or receive card, use a known-good loopback cable to complete the “[1.6.1 Perform a Facility Loopback on a Source-Node FC_MR Port](#)” procedure on page 1-94 and test the loopback.
- Step 7** If a port is bad and you need to use all the port bandwidth, complete the “[Physically Replace a Traffic Card](#)” procedure on page 2-281. If the port is bad but you can move the traffic to another port, replace the card at the next available maintenance window.
- Step 8** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.167 HITEMP

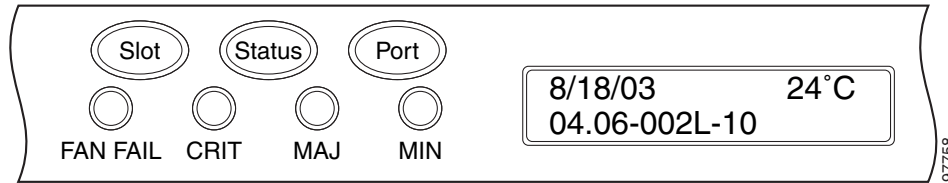
Default Severity: Critical (CR), Service-Affecting (SA) for NE; Default Severity: Minor (MN), Non-Service-Affecting (NSA) for EQPT

SONET Logical Objects: EQPT, NE

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

Clear the HITEMP Alarm

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

Figure 2-2 Shelf LCD Panel

- Step 2** Verify that the environmental temperature of the room is not abnormally high.
- Step 3** If the room temperature is not abnormal, physically ensure that nothing prevents the fan-tray assembly from passing air through the ONS 15454 shelf.
- Step 4** If airflow is not blocked, physically ensure that blank faceplates fill the ONS 15454 shelf empty slots. Blank faceplates help airflow.
- Step 5** If faceplates fill the empty slots, determine whether the air filter needs replacement. Refer to the [“Inspect, Clean, and Replace the Reusable Air Filter” procedure on page 2-286](#).
- Step 6** If the fan does not run or the alarm persists, complete the [“Replace the Fan-Tray Assembly” procedure on page 2-288](#).



Note The fan should run immediately when correctly inserted.

- Step 7** If the replacement fan-tray assembly does not operate correctly, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC to report a Service-Affecting (SA) problem 1 800 553-2447 if it applies to the NE, or a Non-Service-Affecting (NSA) problem if it applies to equipment.

2.7.168 HI-TXPOWER

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

SONET Logical Objects: EQPT, OCN

DWDM Logical Objects: 2R, ESCON, FC, GE, ISC, PPM, TRUNK

The Equipment High Transmit Power alarm is an indicator on the TXP_MR_E, TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, MXP_2.5G_10G, MRC-12, MRC-4, or OC192-XFP card transmitted optical signal power. HI-TXPOWER occurs when the measured optical power of the transmitted signal exceeds the threshold.



Note For more information about provisioning MXP or TXP PPMs, refer to the “Provision Transponders and Muxponders” chapter of the *Cisco ONS 15454 DWDM Procedure Guide*. For more information about the cards themselves, refer to the *Cisco ONS 15454 DWDM Reference Manual*.

Clear the HI-TXPOWER Alarm

- Step 1** In node view, double-click the card view for the TXP_MR_10E, TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, MXP_2.5G_10G, or OC192-XFP card.

- Step 2** Click the **Provisioning > Optics Thresholds > Current Values** tabs.
- Step 3** Decrease (change toward the negative direction) the OPT-HIGH column value by 0.5 dBm.
- Step 4** If the card transmit power setting cannot be lowered without disrupting the signal, complete the “Physically Replace a Traffic Card” section on page 2-281.
- Step 5** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.169 HLDVRSYNC

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

SONET Logical Object: NE-SREF

The Holdover Synchronization Mode condition is caused by loss of the primary and second timing references in the node. Timing reference loss occurs when line coding on the timing input is different from the configuration on the node, and it often occurs during the selection of a new node reference clock. The condition clears when primary or second timing is reestablished. After the 24-hour holdover period expires, timing slips could begin to occur on an ONS 15454 relying on an internal clock.

Clear the HLDVRSYNC Condition

- Step 1** Clear additional alarms that relate to timing, such as:
- [2.7.145 FRNGSYNC, page 2-118](#)
 - [2.7.146 FSTSYNC, page 2-119](#)
 - [2.7.204 LOF \(BITS\), page 2-151](#)
 - [2.7.221 LOS \(BITS\), page 2-161](#)
 - [2.7.269 MANSWTOINT, page 2-184](#)
 - [2.7.270 MANSWTOPRI, page 2-184](#)
 - [2.7.271 MANSWTOSEC, page 2-184](#)
 - [2.7.272 MANSWTOTHIRD, page 2-184](#)
 - [2.7.412 SWTOPRI, page 2-245](#)
 - [2.7.413 SWTOSEC, page 2-245](#)
 - [2.7.414 SWTOTHIRD, page 2-245](#)
 - [2.7.415 SYNC-FREQ, page 2-246](#)
 - [2.7.417 SYNCPRI, page 2-247](#)
 - [2.7.418 SYNCSEC, page 2-248](#)
 - [2.7.419 SYNCTHIRD, page 2-248](#)
- Step 2** Reestablish a primary and secondary timing source according to local site practice. If none exists, refer to the “Change Node Settings” chapter in the *Cisco ONS 15454 Procedure Guide*.

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

2.7.170 I-HITEMP

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

SONET Logical Object: NE

The Industrial High Temperature alarm occurs when the temperature of the ONS 15454 is above 149 degrees F (65 degrees C) or below –40 degrees F (–40 degrees C). This alarm is similar to the HITEMP alarm but is used for the industrial environment. If this alarm is used, you can customize your alarm profile to ignore the lower-temperature HITEMP alarm.

Clear the I-HITEMP Alarm

- Step 1** Complete the [“Clear the HITEMP Alarm” procedure on page 2-128](#).
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.
-

2.7.171 ILK-FAIL

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.172 IMPROPRMVL

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

SONET Logical Object: EQPT

DWDM Logical Object: PPM

The Improper Removal equipment (IMPROPRMVL) alarm occurs under the following conditions:

- A card is removed when the card was rebooting. It is recommended that after the card completely reboots, delete the card in CTC and only then remove the card physically. When you delete the card, CTC loses connection with the node view (single-shelf mode) or shelf view (multishelf mode), and goes to network view.
- When a card is physically removed from its slot before it is deleted from CTC. It is recommended that any card be deleted in CTC before physically removing the card from the chassis.



Note

CTC provides the user approximately 15 seconds to physically remove the card before it begins rebooting the card.
It can take up to 30 minutes for software to be updated on a standby TCC2/TCC2P card.

- A card is inserted into a slot but is not fully plugged into the backplane.
- A PPM (SFP) is provisioned but the physical module is not inserted into the port.
- Electrical issues such as short circuit or failure of DC-DC conversion.

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, does have circuits mapped to it, is paired in a working protection scheme, has DCC enabled, or is used as a timing reference.

Step 3 If any ports on the card are in service, place them out of service (OOS,MT):



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

- In node view, double-click the reporting card to open the card view.
- Click the **Provisioning > Line** tab.
- Click the Admin State column of any in-service (IS) ports.
- Choose **OOS,MT** to take the ports out of service.

Step 4 If a circuit has been mapped to the card, complete the [“Delete a Circuit” procedure on page 2-283](#).



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:

- Click **View > Go to Previous View** to return to node view.
- If you are already in node view, click the **Provisioning > Protection** tabs.
- Click the protection group of the reporting card.
- Click **Delete**.

Step 6 If the card is provisioned for DCC, delete the DCC provisioning:

- Click the ONS 15454 **Provisioning > Comm Channels > SDCC** tabs.
- Click the slots and ports listed in DCC terminations.
- 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:

- Click the **Provisioning > Timing > General** tabs.
- Under NE Reference, click the drop-down arrow for **Ref-1**.
- Change Ref-1 from the listed OC-N card to **Internal Clock**.
- Click **Apply**.

- Step 8** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.
-

2.7.173 INCOMPATIBLE-SEND-PDIP

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

SONET Logical Object: SYSTEM

The Incompatible Software alarm is raised when the PDIP provisioning on CTC differs from the provisioning on the host node.

Clear the INCOMPATIBLE-SEND-PDIP Alarm

- Step 1** Reconfigure the send-PDI-P-alarm capability in CTC to align with the host node settings.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call TAC (1-800-553-2447).
-

2.7.174 INCOMPATIBLE-SW

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

SONET Logical Object: SYSTEM

The Incompatible Software alarm is raised when CTC cannot connect to the NE due to incompatible versions of software between CTC and the NE. The alarm is cleared by restarting CTC in order to redownload the CTC jar files from the NE.

Clear the INCOMPATIBLE-SW Alarm

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

2.7.175 INC-ISD

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

SONET Logical Object: DS3

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

**Note**

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

2.7.176 INHSWPR

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

SONET Logical Object: EQPT

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

Clear the INHSWPR Condition

-
- Step 1** If the condition is raised against a 1+1 port, complete the [“Initiate a 1+1 Manual Switch Command” section on page 2-270](#).
 - Step 2** If the condition is raised against a 1:1 card, complete the [“Initiate a 1:1 Card Switch Command” procedure on page 2-272](#) to switch it back.
 - Step 3** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.177 INHSWWKG

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

SONET Logical Object: EQPT

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

Clear the INHSWWKG Condition

-
- Step 1** If the condition is raised against a 1+1 port, complete the [“Initiate a 1+1 Manual Switch Command” section on page 2-270](#).
 - Step 2** If it is raised against a 1:1 card, complete the [“Initiate a 1:1 Card Switch Command” procedure on page 2-272](#) to switch traffic back.
 - Step 3** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.178 INTRUSION-PSWD

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

SONET Logical Object: NE

The Security Intrusion Incorrect Password condition occurs after a user attempts a provisionable (by Superuser) number of unsuccessful logins, a login with an expired password, or an invalid password. The alarmed user is locked out of the system, and INTRUSION-PSWD condition is raised. This condition is only shown in Superuser login sessions, not in login sessions for lower-level users. The INTRUSION-PSWD condition is automatically cleared when a provisionable lockout timeout expires, or it can be manually cleared in CTC by the Superuser if the lockout is permanent.

Clear the INTRUSION-PSWD Condition

-
- | | |
|---------------|---|
| Step 1 | Click the Provisioning > Security > Users tabs. |
| Step 2 | Click Clear Security Intrusion Alarm . |
| Step 3 | If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC 1 800 553-2447. |
-

2.7.179 INVMACADR

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

SONET Logical Object: AIP

The Equipment Failure Invalid MAC Address alarm occurs when the ONS 15454 MAC address is invalid. Each ONS 15454 has a unique, permanently assigned MAC address. The address resides on an AIP EEPROM. The TCC2/TCC2P reads the address value from the AIP chip during boot-up and keeps this value in its synchronous dynamic RAM (SDRAM).

Under normal circumstances, the read-only MAC address can be viewed in the Provisioning/Network tab in CTC.

The ONS 15454 uses both IP and MAC addresses for circuit routing. When an INVMACADR alarm exists on a node, you see a PARTIAL circuit in the CTC circuit status column. The circuit works and is able to carry traffic, but CTC cannot logically display the circuit end-to-end information.

An invalid MAC address can be caused when:

- There is a read error from the AIP during bootstrap; in this case, the reading TCC2/TCC2P uses the default MAC address (00-10-cf-ff-ff-ff).
- There is a read error occurring on one of the redundant TCC2/TCC2Ps that read the address from the AIP; these cards read the address independently and could therefore each read different address values.
- An AIP component failure causes a read error.
- The ribbon cable connecting the AIP card to the backplane is bad.

Clear the INVMACADR Alarm

- Step 1** Check for any outstanding alarms that were raised against the active and standby TCC2/TCC2P and resolve them.
- Step 2** If the alarm does not clear, determine whether the LCD display on the fan tray ([Figure 2-2 on page 2-129](#)) is blank or if the text is garbled. If so, proceed to [Step 8](#). If not, continue with [Step 3](#).
- Step 3** At the earliest maintenance window, reset the standby TCC2/TCC2P:



Note The reset requires approximately five minutes. Do not perform any other step until the reset is complete.

- a. Log into a node on the network. If you are already logged in, continue with [Step b](#).
- b. Identify the active TCC2/TCC2P.
A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
- c. Right-click the standby TCC2/TCC2P in CTC.
- d. Choose **Reset Card** from the shortcut menu.
- e. Click **Yes** in the Are You Sure dialog box.
The card resets, the FAIL LED blinks on the physical card, and connection to the node is lost. CTC switches to network view.
- f. Verify that the reset is complete and error-free, and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
- g. Double-click the node and ensure that the reset TCC2/TCC2P is still in standby mode and that the other TCC2/TCC2P is active.
A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
- h. Ensure that no new alarms associated with this reset appear in the CTC Alarms window.

If the standby TCC2/TCC2P fails to boot into standby mode and reloads continuously, the AIP is probably defective. In this case, the standby TCC2/TCC2P is unsuccessfully attempting to read the EEPROM located on the AIP. The TCC2/TCC2P reloads until it reads the EEPROM. Proceed to [Step 8](#).

- Step 4** If the standby TCC2/TCC2P rebooted successfully into standby mode, complete the [“Remove and Reinsert \(Reseat\) the Standby TCC2/TCC2P Card” procedure on page 2-280](#).
Resetting the active TCC2/TCC2P causes the standby TCC2/TCC2P to become active. The standby TCC2/TCC2P keeps a copy of the chassis MAC address. If its stored MAC address is valid, the alarm should clear.
- Step 5** After the reset, note whether or not the INVMACADR alarm has cleared or is still present.
- Step 6** Complete the [“Reset an Active TCC2/TCC2P Card and Activate the Standby Card” procedure on page 2-278](#) again to place the standby TCC2/TCC2P back into active mode.
After the reset, note whether or not the INVMACADR alarm has cleared or is still present. If the INVMACADR alarm remains standing through both TCC2/TCC2P resets, this indicates that the AIP is probably defective. Proceed to [Step 8](#).
If the INVMACADR was raised during one TCC2/TCC2P reset and cleared during the other, the TCC2/TCC2P that was active while the alarm was raised needs to be replaced. Continue with [Step 7](#).

- Step 7** If the faulty TCC2/TCC2P is currently in standby mode, complete the “[Physically Replace a Traffic Card](#)” procedure on page 2-281 for this card. If the faulty TCC2/TCC2P is currently active, during the next available maintenance window complete the “[Reset an Active TCC2/TCC2P Card and Activate the Standby Card](#)” procedure on page 2-278 and then complete the “[Physically Replace a Traffic Card](#)” procedure on page 2-281.

**Note**

If the replacement TCC2/TCC2P is loaded with a different software version from the current TCC2/TCC2P, the card bootup could take up to 30 minutes. During this time, the card LEDs flicker between Fail and Act/Sby as the active TCC2/TCC2P version software is copied to the new standby card.

- Step 8** Open a case with Cisco TAC (1 800 553-2447) for assistance with determining the node’s previous MAC address.
- Step 9** Replace the ribbon cable between the system board and the AIP with a known-good cable.
- Step 10** If the alarm persists, complete the “[Replace the Alarm Interface Panel](#)” procedure on page 2-289.
- Step 11** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

2.7.180 IOSCFGCOPY

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

SONET Logical Object: EQPT

The IOS Configuration Copy in Progress condition occurs on ML-Series Ethernet cards when a Cisco IOS startup configuration file is being uploaded or downloaded to or from an ML-Series card. (This condition is very similar to the “[SFTWDOWN](#)” condition on page 2-230 but it applies to ML-Series Ethernet cards rather than to the TCC2/TCC2P.)

The condition clears after the copy operation is complete. (If it does not complete correctly, the “[NO-CONFIG](#)” condition on page 2-192 could be raised.)

**Note**

IOSCFGCOPY is an informational condition.

**Note**

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

2.7.181 ISIS-ADJ-FAIL

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

SONET Logical Object: OCN

The Open System Interconnection (OSI) Intermediate System to Intermediate-System (IS-IS) Adjacency Failure alarm is raised by an intermediate system (node routing IS Level 1 or Level 1 and 2) when no IS or end system (ES) adjacency is established on a point-to-point subnet. The Intermediate-System Adjacency Failure alarm is not supported by ES. It is also not raised by IS for disabled routers.

The alarm is typically caused by a misconfigured router manual area adjacency (MAA) address. For more information about IS-IS OSI routing and MAA configuration, refer to the “Management Network Connectivity” chapter in the *Cisco ONS 15454 Reference Manual*. For more information about configuring OSI, refer to the “Turn Up Node” chapter in the *Cisco ONS 15454 Procedure Guide*.

Clear the ISIS-ADJ-FAIL Alarm

-
- Step 1** Ensure that both ends of the communication channel are using the correct Layer 2 protocol and settings (LAPD or PPP). To do this, complete the following steps:
- At the local node, in node view, click the **Provisioning > Comm Channels > SDCC** tabs.
 - Click the row of the circuit. Click **Edit**.
 - In the Edit SDCC termination dialog box, view and record the following selections: Layer 2 protocol (LAPD or PPP); Mode radio button selection (AITS or UITS); Role radio button selection (Network or User); MTU value; T200 value, and T203 selections.
 - Click **Cancel**.
 - Login to the remote node and follow the same steps, also recording the same information for this node.
- Step 2** If both nodes do not use the same Layer 2 settings, you will have to delete the incorrect termination and recreate it. To delete it, click the termination and click **Delete**. To recreate it, refer to the “Turn Up Node” chapter in the *Cisco ONS 15454 Procedure Guide* for the procedure.
- Step 3** If the nodes use PPP Layer 2, complete the “[Clear the EOC Alarm](#)” procedure on page 2-87. If the alarm does not clear, go to [Step 7](#).
- Step 4** If both nodes use the LAPD Layer 2 protocol but have different Mode settings, change the incorrect node’s entry by clicking the correct setting radio button in the Edit SDCC termination dialog box and clicking **OK**.
- Step 5** If the Layer 2 protocol and Mode settings are correct, ensure that one node is using the Network role and the other has the User role. If not (that is, if both have the same mode settings), correct the incorrect one by clicking the correct radio button in the Edit SDCC termination dialog box and clicking **OK**.
- Step 6** If the Layer 2, Mode, and Role settings are correct, compare the MTU settings for each node. If one is incorrect, choose the correct value in the Edit SDCC dialog box and click **OK**.
- Step 7** If all of the preceding settings are correct, ensure that OSI routers are enabled for the communications channels at both ends:
- Click **Provisioning > OSI > Routers > Setup** tabs.
 - View the router entry under the **Status** column. If the status is Enabled, check the other end.
 - If the Status is Disabled, click the router entry and click **Edit**.
 - Check the **Enabled** check box and click **OK**.
- Step 8** If the routers on both ends are enabled and the alarm still has not cleared, ensure that both ends of the communications channel have a common MAA:
- Click the **Provisioning > OSI > Routers > Setup** tabs.
 - Record the primary MAA and secondary MAAs, if configured.



Tip

You can record long strings of information such as the MAA address by using the CTC export and print functions. Export it by choosing File > Export > html. Print it by choosing File > Print.

- c. Log into the other node and record the primary MAA and secondary MAAs, if configured.
- d. Compare this information. There should be at least one common primary or secondary MAA in order to establish an adjacency.
- e. If there is no common MAA, one must be added to establish an adjacency. Refer to the “Turn Up Node” chapter in the *Cisco ONS 15454 Procedure Guide* for procedures.

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

2.7.182 KB-PASSTHR

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

SONET Logical Object: OCN

The K Bytes Pass Through Active condition occurs on a nonswitching node in a BLSR when the protect channels on the node are not active and the node is in K Byte pass-through state. It also occurs when a BLSR ring is being exercised using the Exercise Ring command.

Clear the KB-PASSTHR Condition

Step 1 Complete the [“Clear a BLSR External Switching Command” procedure on page 2-277](#).

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

2.7.183 KBYTE-APS-CHAN-FAIL

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

SONET Logical Object: OCN

The APS Channel Failure alarm is raised when a span is provisioned for different APS channels on each side. For example, the alarm is raised if K3 is selected on one end and F1, E2, or Z2 is selected on the other end.

This alarm is also raised during checksum failure if the K1 and K2 bytes are overwritten by test equipment. It is not raised in bidirectional full pass-through or K-byte pass-through states. The alarm is overridden by the [“AIS-P” alarm on page 2-39](#), the [“LOF \(OCN\)” alarm on page 2-155](#), the [“LOS \(OCN\)” alarm on page 2-168](#) or the [“SF-P” alarm on page 2-230](#).

Clear the KBYTE-APS-CHAN-FAIL Alarm

Step 1 The alarm is most frequently raised due to mismatched span provisioning. In this case, reprovision one side of the span with the same parameters. To do this, refer to the “Turn Up Network” chapter in the *Cisco ONS 15454 Procedure Guide*.

- Step 2** If the error is not caused by misprovisioning, it is due to checksum errors within an OC-N, cross-connect, or TCC2/TCC2P. In this case, complete the “[Side Switch the Active and Standby Cross-Connect Cards](#)” procedure on page 2-278 to allow CTC to resolve the issue.
- Step 3** If third-party equipment is involved, ensure that it is configured for the same APS channel as the Cisco ONS equipment.
- Step 4** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

2.7.184 LAN-POL-REV

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

SONET Logical Object: NE

The LAN Connection Polarity Reversed condition is not raised in shelves that contain TCC2 cards. It is raised during a software upgrade when the card detects that a connected Ethernet cable has reversed receive wire pairs. The card automatically compensates for this reversal, but LAN-POL-REV stays active.



Note

For more information about Ethernet cards, refer to the Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.

Clear the LAN-POL-REV Condition

- Step 1** Replace the connected Ethernet cable with a cable that has the correct pinout. For correct pin mapping, refer to the “Maintain the Node” chapter in the *Cisco ONS 15454 Procedure Guide*.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

2.7.185 LASER-APR

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.186 LASERBIAS-DEG

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.187 LASERBIAS-FAIL

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.188 LASEREOL

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

SONET Logical Object: OCN

The Laser Approaching End of Life alarm applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards. It is typically accompanied by the “[HI-LASERBIAS](#)” alarm on page 2-126. It is an indicator that the laser in the card must be replaced. How soon the replacement must happen depends upon the HI-LASERBIAS alarm’s threshold. If the threshold is set under 100 percent, the laser replacement can usually be done during a maintenance window. But if the HI-LASERBIAS threshold is set at 100 percent and is accompanied by data errors, LASEREOL indicates the card must be replaced sooner.

**Note**

For more information about MXP or TXP cards, refer to the *Cisco ONS 15454 DWDM Reference Manual*.

Clear the LASEREOL Alarm

-
- | | |
|---------------|---|
| Step 1 | Complete the “ Physically Replace a Traffic Card ” procedure on page 2-281. |
| Step 2 | If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC 1 800 553-2447. |
-

2.7.189 LASERTEMP-DEG

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.190 LCAS-CRC

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

SONET Logical Objects: STSTRM, VT-TERM

The Link Capacity Adjustment Scheme (LCAS) Control Word CRC Failure condition is raised against ML-Series Ethernet and CE-series cards. It occurs when there is an equipment, path, or provisioning error on the virtual concatenation group (VCG) that causes consecutive 2.5 second CRC failures in the LCAS control word.

Transmission errors would be reflected in CV-P, ES-P, or SES-P performance monitoring statistics. If these errors do not exist, an equipment failure is indicated.

If LCAS is not supported on the peer node, the condition does not clear.

LCAS-CRC can also occur if the VCG source node is not LCAS-enabled, but the receiving node does have the capability enabled. Both source and destination nodes must have LCAS enabled. Otherwise, the LCAS-CRC condition persists on the VCG.

**Note**

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

Clear the LCAS-CRC Condition

-
- Step 1** Look for and clear any associated equipment failures, such as the EQPT alarm, on the receive node or transmit node.
- Step 2** Look for and clear any bit error rate alarms at the transmit node.
- Step 3** If no equipment or SONET path errors exist, ensure that the remote node has LCAS enabled on the circuit:
- In node view, click the **Circuits** tab.
 - Choose the VCAT circuit and click **Edit**.
 - In the Edit Circuit window, click the **General** tab.
 - Verify that the Mode column says **LCAS**.
- Step 4** If the column does not say LCAS, complete the [“Delete a Circuit” procedure on page 2-283](#) and recreate it in LCAS mode using the instructions in the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.
- Step 5** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.191 LCAS-RX-DNU

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

SONET Logical Objects: STSTRM, VT-TERM

The LCAS VCG Member Receive-Side-In Do Not Use condition is raised on CE-MR-10 cards and ML-MR-10 Ethernet cards when the receive side of an LCAS VCG member is in the do-not use state. For a unidirectional failure, this condition is only raised at the source node.

The node reporting this condition likely reports an [“RFI-P” alarm on page 2-210](#) and [“RFI-V” alarm on page 2-211](#) for CE-MR-10, and [“RFI-P” alarm on page 2-210](#) for ML-MR-10.

**Note**

For more information about the CE-MR-10 and ML-MR-10 Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Clear the LCAS-RX-DNU Condition

-
- Step 1** Look for any SONET failures, such as the RFI-P and RFI-V alarms, on the source node. If any are present, clear them using the relevant procedures in this chapter.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.192 LCAS-RX-FAIL

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

SONET Logical Objects: STSTRM, VT-TERM

The LCAS VCG Member Receive-Side-In Fail condition is raised against FC_MR-4 cards, CE-series and ML-Series Ethernet cards with LCAS-enabled VCG.

LCAS VCGs treat failures unidirectionally, meaning that failures of the transmit or receive points occur independently of each other. The LCAS-RX-FAIL condition can occur on the receive side of an LCAS VCG member for the following reasons:

- SONET path failure (a unidirectional failure as seen by the receive side)
- VCAT member is set out of group at the transmit side, but is set in group at the receive side
- VCAT member does not exist at the transmit side but does exist and is in group at the receive side

The condition can be raised during provisioning operations on LCAS VCGs but should clear when the provisioning is completed.

Software-enabled LCAS VCGs treat failure bidirectionally, meaning that both directions of a VCG member are considered failed if either transmit or receive fails. The LCAS-RX-FAIL condition is raised on these VCG members when a member receive side fails due to a SONET path failure.



Note

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



Note

ML-Series cards are LCAS-enabled. ML-Series and FC_MR-4 cards are SW-LCAS enabled.

Clear the LCAS-RX-FAIL Condition

-
- Step 1** Check for and clear any line or path alarms (typically ending in “-L” or “-P”).
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.193 LCAS-RX-GRP-ERR

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

SONET Logical Objects: STSTRM, VT-TERM

The LCAS Sink Group Error condition is raised against ML-MR-10 and CE-MR-10 Ethernet cards. This condition is raised if the LCAS member sink has a group error.

Clear the LCAS-RX-GRP-ERR Condition

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

2.7.194 LCAS-TX-ADD

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

SONET Logical Objects: STSTRM, VT-TERM

The LCAS VCG Member Transmit-Side-In Add State condition is raised against ML-Series Ethernet and CE-series cards when the transmit side of an LCAS VCG member is in the add state. The condition clears after provisioning is completed. The remote likely reports a path condition such as the [“AIS-P” condition on page 2-39](#) or the [“UNEQ-P” alarm on page 2-258](#)



Note

LCAS-TX-ADD is an informational condition and does not require troubleshooting.



Note

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

2.7.195 LCAS-TX-DNU

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

SONET Logical Objects: STSTRM, VT-TERM

The LCAS VCG Member Transmit-Side-In Do Not Use condition is raised on FC_MR-4 cards, CE-series and ML-Series Ethernet cards when the transmit side of an LCAS VCG member is in the do-not use state. For a unidirectional failure, this condition is only raised at the source node. The LCAS-TX-DNU condition is raised when the cable is unplugged.

The node reporting this condition likely reports an [“RFI-P” alarm on page 2-210](#), and the remote node likely reports a path alarm such as the [“AIS-P” alarm on page 2-39](#) or the [“UNEQ-P” alarm on page 2-258](#).



Note

LCAS-TX-DNU is an informational condition and does not require troubleshooting.

**Note**

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

2.7.196 LINK-KEEPALIVE

Default Severity: Critical (CR), Non-Service-Affecting (NSA)

SONET Logical Objects: ML1000, ML100T, MLFX, OCN

The LINK-KEEPALIVE alarm indicates that a span is not receiving a defined number of keep-alive messages on the ML card's IEEE 802.17b-based interface or Cisco proprietary RPR interface within allotted keep-alive timeout period. Although this alarm defaults to a Critical (CR) severity, it can be downgraded if the span is protected.

A LINK-KEEPALIVE alarm causes the “RPR-SF” alarm on page 2-220 to be raised also. LINK-KEEPALIVE is suppressed by the “RPR-PASSTHR” alarm on page 2-215. This alarm clears when a defined number of consecutive keep-alive messages is received on the interface.

**Note**

In the Cisco IOS CLI “show ons alarms” command display, this alarm is called KEEP-ALIVE-FAIL.

**Note**

The GFP-UP-MISMATCH, GFP-CSF, GFP-LFD, and TPTFAIL alarms suppress the LINK-KEEPALIVE alarm even though the LINK-KEEPALIVE alarm has higher severity than the other alarms. The GFP alarms are promoted because the LINK-KEEPALIVE alarm information is contained within a GFP frame. The TPTFAIL alarm is promoted because it is a layer 1 alarm while LINK-KEEPALIVE is a layer 2 alarm.

Clear the LINK-KEEPALIVE Alarm

- Step 1** Verify that no SONET or GFP circuit alarms that could impact Ethernet data traffic are present. If any are present, clear them using the relevant procedures in this chapter.
- Step 2** Verify that the “DATA-CRC” alarm on page 2-78 is not present. If it is present, complete the trouble-clearing procedure.
- Step 3** Verify that the keep-alive timer on this IEEE RPR 802.17b-based station has the same value as its neighboring RPR-IEEE stations.
- Step 4** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

2.7.197 LKOUTPR-S

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

SONET Logical Object: OCN

The Lockout of Protection Span condition occurs when span traffic is locked out of a protect span using the Lockout of Protect command. This condition is visible on the network view Alarms, Conditions, and History tabs after the lockout has occurred and accompanies the [“FE-LOCKOUTOFPR-SPAN” alarm on page 2-112](#). The port where the lockout originated is marked by an “L” on the network view detailed circuit map.

Clear the LKOUTPR-S Condition

-
- Step 1** Complete the [“Clear a BLSR External Switching Command” procedure on page 2-277](#).
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.198 LMP-FAIL

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

SONET Logical Objects: CLIENT, CTRL, TLINK

The Link Management Protocol Fail alarm is raised by the TCC2/TCC2P card when an LMP control channel fails or when there is a traffic engineering (TE) link correlation error. When the alarm is raised against a control channel, it uses a control channel (CTRLx) AID. When the alarm is raised against a TE link, a TE link AID (TLINKx) is used.

The alarm clears when the control channel or TE link is restored.



Note

LMP-FAIL occurs independently of the condition hierarchy between the [“LMP-SD” alarm on page 2-147](#), the [“LMP-SF” alarm on page 2-148](#), or the [“LMP-UNALLOC” alarm on page 2-149](#).



Note

When the LMP-FAIL alarm is reported against a control channel (CTRLx) AID, it only refers to control channel failure. It does not directly indicate data link or traffic engineering link status.



Note

When the LMP-FAIL alarm is reported against a TE link AID (TLINKx), it refers only to TE link status, not to control channel or data link status.

Clear the LMP-FAIL Alarm

-
- Step 1** Verify the AID (CTRLx or TLINKx) of the alarm.
- Step 2** If the alarm is against the control channel AID, this is caused by mismatched control channel parameters between the near-end ONS 15454 and the far-end node (which may be another vendor’s equipment). Complete the following steps:
- a. Determine whether both near-end and far-end sides of the control channel are in the IS administrative state:

- Click the **Provisioning > Comm Channels > LMP > Control Channel** tabs and view the Admin State column content for the channel.
 - If the status does not say IS, change it and click **Apply**.
- b. Determine whether the near-end node LMP configuration contains the far-end node's IP address as its remote node IP. Also verify that the near-end node's LMP configuration uses the LMP node ID as its own remote node ID. If one or more of these values is incorrect, enter it correctly.
 - c. Determine whether the far-end node LMP configuration contains the near-end node's IP address as its remote node IP. Also verify that the far-end node's LMP configuration uses the LMP node ID as its own remote node ID. If one or more of these values is incorrect, enter it correctly.
 - d. Verify that the far-end node is using the near-end node's IP address as its remote node IP address, and that the far end is also using the LMP node ID as its remote node ID. Update the far end's values if they are incorrect.
- Step 3** If instead the alarm is raised against the TE link AID, complete the following steps:
- a. Determine whether both near-end and far-end sides of the TE link are in the IS administrative state. If either end is currently down, update its administrative state to IS:
 - Click the **Provisioning > Comm Channels > LMP > TE link** tab.
 - If the status does not say IS, change it and click **Apply**.
 - b. Determine whether the near-end node's remote TE link ID matches the far-end node's local TE link ID. If the near-end node's remote value is incorrect, enter it correctly.
 - c. Determine whether the far-end node's remote TE link ID corresponds to the near-end node's local TE link ID. If the far-end node's remote value is incorrect, enter it correctly.
- Step 4** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

2.7.199 LMP-SD

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

SONET Logical Object: OCN

DWDM Logical Object: GE

The LMP Data Link Signal Degrade condition occurs for when the TCC2/TCC2P receives an LMP link summary or channel status message that the control channel is not available from the far end, so the data link level of service is not guaranteed. The degrade range is provisionable.

LMP-SD clears when the TCC2/TCC2P receives a link summary or channel status message reporting that the data link is in the Signal Okay (OK) state.

LMP-SD is part of an alarm hierarchy that includes the “[LMP-SF](#)” alarm on page 2-148 and the “[LMP-UNALLOC](#)” alarm on page 2-149. The hierarchy is as follows: If LMP-UNALLOC is raised, LMP-SF and LMP-SD are suppressed. If LMP-SF is raised, it suppresses LMP-SD. LMP-SF and LMP-UNALLOC both suppress near-end LOS-type alarms for DWDM clients. LMP-SD, however, does not suppress LOS alarms.

This condition clears when the far-end trouble has been cleared.

Clear the LMP-SD Condition

- Step 1** Look for and clear any of the following alarms in [Table 2-13](#) and [Table 2-14](#) occurring on the far-end port. Refer to the *Cisco ONS 15454 DWDM Troubleshooting Guide, R7.x* for DWDM trunk ([Table 2-13](#)) and client ([Table 2-14](#)) alarm trouble-clearing procedures.

Table 2-13 Transponder Trunk Alarms that Cause LMP-SD

Trunk Port Alarm	LMP Failure	Direction
SD	SD	Tx
OTUK-SD	SD	Tx
ODUK-SD-PM	SD	Tx
ODUK-SD-TCM1	SD	Tx
ODUK-SD-TCM2	SD	Tx

Table 2-14 Transponder Client Alarm that Causes LMP-SD

Client Port Alarm	LMP Failure	Direction
SD	SD	Rx

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

2.7.200 LMP-SF

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

SONET Logical Object: OCN

DWDM Logical Object: GE

The LMP Data Link Signal Fail condition notifies the near-end user of a far-end problem (and thus is NSA for the near end). The near-end's TCC2/TCC2P receives an LMP link summary or channel status message that the data link service has failed. The signal fail threshold is provisionable.

LMP-SF clears when the TCC2/TCC2P receives a link summary or channel status message reporting that the data link is in the Signal Okay (OK) state.

LMP-SF is part of an alarm hierarchy that includes the [“LMP-SD” alarm on page 2-147](#) and the [“LMP-UNALLOC” alarm on page 2-149](#). The hierarchy is as follows: If LMP-UNALLOC is raised, LMP-SF and LMP-SD are suppressed. If LMP-SF is raised, it suppresses LMP-SD. LMP-SF and LMP-UNALLOC both suppress near-end LOS-type alarms for DWDM clients, but LMP-SD does not suppress LOS-type alarms.

This condition clears when the far-end trouble has been cleared.

Clear the LMP-SF Condition

- Step 1** Look for and clear any of the following alarms in [Table 2-15](#), [Table 2-16](#), or [Table 2-17](#) occurring on the far-end port. The card alarms are located in this chapter. The *Cisco ONS 15454 DWDM Troubleshooting Guide, R7.x* contains trouble-clearing procedures for DWDM trunk ([Table 2-16](#)) and client ([Table 2-17](#)) alarms.

Table 2-15 Transponder Card Alarms that Cause LMP-SF

Card Alarm	LMP Failure	Direction
EQPT, page 89	SF	Tx
IMPROPRMVL, page 131	SF	Tx

Table 2-16 Transponder Trunk Alarms that Cause LMP-SF

Trunk Port Alarm	LMP Failure	Direction
LOS	SF	Tx
OTUK-LOF	SF	Tx
OTUK-AIS	SF	Tx
LOM	SF	Tx
OTUK-SF	SF	Tx
ODUK-SF-PM	SF	Tx
ODUK-SF-TCM1	SF	Tx
ODUK-SF-TCM2 SF	SF	Tx
FEC-MISM	SF	Tx

Table 2-17 Transponder Client Alarms that Cause LMP-SF

Client Alarm	LMP Failure	Direction
LOS	SF	Rx
SIGLOSS	SF	Rx
SYNCLOSS	SF	Rx
CARLOSS	SF	Rx
LOF	SF	Rx

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

2.7.201 LMP-UNALLOC

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

SONET Logical Object: OCN

DWDM Logical Object: GE

The LMP Data Link Unallocated condition is raised when the TCC2/TCC2P receives an LMP link summary or channel status message reporting that the data link is unallocated for data traffic. The condition clears when the data link is allocated and sends an LMP link summary or channel status message to this effect. If a data link has the LMP-UNALLOC alarm raised against it, this should suppress all other alarms on the client port, since the far-end node is not using the errored port. (Consequently you do not have to clear any alarms on the far-end node's unused port.)

LMP-UNALLOC is part of an alarm hierarchy that includes the [“LMP-SD” alarm on page 2-147](#) and the [“LMP-SF” alarm on page 2-148](#). The hierarchy is as follows: If LMP-UNALLOC is raised, LMP-SF and LMP-SD are suppressed. If LMP-SF is raised, it suppresses LMP-SD. LMP-SF and LMP-UNALLOC both suppress near-end LOS-type DWDM client alarms, but LMP-SD does not.

In most cases, this condition is an informational notice at the near-end node that the far-end port is not being utilized. If, however, the far-end port should be allocated for traffic, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

2.7.202 LOA

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

SONET Logical Object: VCG

The Loss of Alignment on a VCG is a VCAT member alarm. (VCAT member circuits are independent circuits that are concatenated from different time slots into a higher-rate signal.) The alarm occurs when members of a VCG travel over different paths in the network (due to initial operator provisioning or to protection or restoration events) and the differential delays between the paths cannot be recovered by terminating hardware buffers.



Note

This alarm occurs only if you provision circuits outside of CTC, such as by using TL1.

Clear the LOA Alarm

- Step 1** In network view, click the **Circuits** tab.
- Step 2** Click the alarmed VCG and then click **Edit**.
- Step 3** In the Edit Circuit window, view the source and destination circuit slots, ports, and STSs.
- Step 4** Identify whether the STS travels across different fibers. If it does, complete the [“Delete a Circuit” procedure on page 2-283](#).
- Step 5** Recreate the circuit using the procedure in the “Create Circuits and VT Tunnels” chapter in the *Cisco ONS 15454 Procedure Guide*.
- Step 6** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.

2.7.203 LOCKOUT-REQ

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

SONET Logical Objects: EQPT, OCN, STSMON, VT-MON

DWDM Logical Objects: 2R, ESCON, FC, GE, ISC, TRUNK

The Lockout Switch Request on Facility or Equipment condition occurs when a user initiates a lockout switch request for an OC-N port in a 1+1 facility protection group. This can be accomplished by locking traffic onto the working port with the LOCK ON command (thus locking it off the protect port), or locking it off the protect port with the LOCK OUT command. In either case, the protect port will show “Lockout of Protection,” and the Conditions window will show the LOCKOUT-REQ condition.

A lockout prevents protection switching. Clearing the lockout again allows protection switching and clears the LOCKOUT-REQ condition.

Clear the LOCKOUT-REQ Condition

-
- Step 1** Complete the [“Clear a Lock-On or Lockout Command” procedure on page 2-272](#).
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.204 LOF (BITS)

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

SONET Logical Object: BITS

The Loss of Frame (LOF) BITS alarm occurs when a port on the TCC2/TCC2P BITS input detects an LOF on the incoming BITS timing reference signal. LOF indicates that the receiving ONS 15454 has lost frame delineation in the incoming data.



Note

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

Clear the LOF (BITS) Alarm

-
- Step 1** Verify that the line framing and line coding match between the BITS input and the TCC2/TCC2P:
- In node or card view, note the slot and port reporting the alarm.
 - Find the coding and framing formats of the external BITS timing source. The formats should be in the user documentation for the external BITS timing source or on the timing source itself.
 - Click the **Provisioning > Timing > BITS Facilities** tabs.
 - Verify that the Coding setting matches the coding of the BITS timing source, either B8ZS or AMI.
 - If the coding does not match, click **Coding** and choose the appropriate coding from the drop-down list.

- f. Verify that Framing matches the framing of the BITS timing source, either ESF or SF (D4).
- g. If the framing does not match, click **Framing** and choose the appropriate framing from the drop-down list.

**Note**

On the timing subtab, the B8ZS coding field is normally paired with ESF in the Framing field and the AMI coding field is normally paired with SF (D4) in the Framing field.

- Step 2** If the alarm does not clear when the line framing and line coding match between the BITS input and the TCC2/TCC2P, complete the [“Physically Replace a Traffic Card” procedure on page 2-281](#) for the TCC2/TCC2P.
- Step 3** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.

2.7.205 LOF (DS1)

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

SONET Logical Object: DS1

The DS-1 LOF alarm indicates that the receiving ONS 15454 has lost frame delineation in an incoming DS-1 data stream.

Clear the LOF (DS1) Alarm

- Step 1** Verify that the line framing and line coding match between the DS1 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 could need to contact your network administrator for the format information.
 - c. Display the card view of the reporting card.
 - d. Click the **Provisioning > Line** tabs.
 - e. Verify that the line type of the reporting port matches the line type of the signal source (DS4 and DS4, unframed and unframed, or ESF and ESF). If the signal source line type does not match the reporting port, click the **Line Type** cell to reveal a drop-down list and choose the matching type.
 - f. Verify that the reporting Line Coding matches the signal source line coding (AMI and AMI or B8ZS and B8ZS). If the signal source line coding does not match the reporting port, click the **Line Coding** cell and choose the correct type from the drop-down list.
 - g. Click **Apply**.

**Note**

On the Line tab, the B8ZS coding field is normally paired with ESF in the Framing field. AMI coding is normally paired with SF (D4) in the Framing field.

**Note**

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

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

2.7.206 LOF (DS3)

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

SONET Logical Object: DS3

The DS-3 LOF alarm indicates that the receiving ONS 15454 has lost frame delineation in the incoming DS-3 data stream on DS3XM-6, DS3XM-12, or add DS3/EC1-48 cards. The framing of the transmitting equipment could be set to a format that differs from the receiving system. On DS3XM cards, the alarm occurs only on cards with the provisionable framing format set to C Bit or M13 and not on cards with the provisionable framing format is set to unframed.

Clear the LOF (DS3) Alarm

- Step 1** Change the line type of the non-ONS equipment attached to the reporting card to C Bit:
- Display the card view of the reporting card.
 - Click the **Provisioning > Line** tabs.
 - Verify that the line type of the reporting port matches the line type of the signal source.
 - If the signal source line type does not match the reporting port, click **Line Type** and choose **C Bit** from the drop-down list.
 - Click **Apply**.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.

2.7.207 LOF (E1)

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

SONET Logical Object: E1

The E1 LOF alarm appears on the DS1/E1-56 card when the card is placed in All E1 mode. It indicates that the receiving ONS 15454 has lost frame delineation in an incoming E1 data stream. The transmitting equipment could possibly have its framing set to a format that differs from the receiving node. For more information about the DS1/E1-56 card, refer to the “Electrical Cards” chapter in the *Cisco ONS 15454 Reference Manual*.

**Note**

The DS1/E1-56 card only carries an E1 signal within an STS-3c/VT2 circuit.

Clear the LOF (E1) Alarm

- Step 1** Verify that the line framing and line coding match between the DS1/E1-56 port and the signal source:
- In CTC, note the slot and port reporting the alarm.
 - Find the coding and framing formats of the signal source for the card reporting the alarm. You could need to contact your network administrator for this information.
 - Double-click the DS1/E1-56 card to open the card view.
 - Click the **Provisioning > Line** tabs.
 - Verify that the line type of the reporting port matches the line type (E1_MF, E1_CRCMF, AUTOFRAMED, UNFRAMED) of the signal source. If the signal source line type does not match the reporting port, click the **Line Type** cell to reveal a drop-down list and choose the matching type.
 - Verify that the reporting Line Coding matches the signal source line coding. If the signal source line coding does not match the reporting port, click the **Line Coding** cell and choose the correct type from the drop-down list.
 - Click **Apply**.

**Note**

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

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

2.7.208 LOF (EC1)

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

SONET Logical Object: EC1

The EC1/EC1-12 LOF alarm occurs when a port on the reporting EC1/EC1-12 or DS3/EC1-48 card has an LOF condition. LOF indicates that the receiving ONS 15454 has lost frame delineation in the incoming data. LOF occurs when the SONET overhead loses a valid framing pattern for 3 milliseconds. Receiving two consecutive valid A1/A2 framing patterns clears the alarm.

Clear the LOF (EC1) Alarm

- Step 1** Verify cabling continuity to the port reporting the alarm. To verify cable continuity, follow site practices.

**Caution**

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

- Step 2** If cabling continuity is good, clean the fiber according to site practice. If no site practice exists, complete the procedure in the “Maintain the Node” chapter in the *Cisco ONS 15454 Procedure Guide*.
- Step 3** If the alarm does not clear, see the loopback procedures in [Chapter 1, “General Troubleshooting”](#) to isolate the fault causing the LOF alarm.
- Step 4** If the alarm does not clear, or if you need assistance conducting network troubleshooting tests, call Cisco TAC to report a Service-Affecting (SA) problem 1 800 553-2447.

2.7.209 LOF (OCN)

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

SONET Logical Object: OCN

The LOF alarm occurs when a port on the reporting card has an LOF condition. It can also occur on ONS 15454 MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, TXP_MR_10E, or TXPP_MR_2.5G cards reporting LOF. The alarm indicates that the receiving ONS 15454 has lost frame delineation in the incoming data. LOF occurs when the SONET overhead loses a valid framing pattern for 3 milliseconds. Receiving two consecutive valid A1/A2 framing patterns clears the alarm.

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



Note

For information about MXP or TXP cards, refer to the *Cisco ONS 15454 DWDM Reference Manual*.

Clear the LOF (OCN) Alarm

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



Caution

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

- Step 2** If cabling continuity is good, clean the fiber according to site practice. If no site practice exists, complete the procedure in the “Maintain the Node” chapter of the *Cisco ONS 15454 Procedure Guide*.
- Step 3** If the alarm does not clear, see the loopback procedures in [Chapter 1, “General Troubleshooting”](#) to isolate the fault causing the LOF alarm.
- Step 4** If the alarm does not clear, or if you need assistance conducting network troubleshooting tests, call Cisco TAC to report a Service-Affecting (SA) problem 1 800 553-2447.

2.7.210 LOF (STSTRM)

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

SONET Logical Object: STSTRM

A Loss of Frame alarm for an STS circuit termination indicates that the LOF has occurred at the terminating point of the circuit (such as an OC-N port). It is similar to the “LOF (OCN)” alarm on [page 2-155](#).

Clear the LOF (STSTRM) Alarm

-
- Step 1** Complete the “[Clear the LOF \(OCN\) Alarm](#)” procedure on [page 2-155](#).
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.
-

2.7.211 LOF (TRUNK)

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.212 LOGBUFR90

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

SONET Logical Object: SYSTEM

The Log Buffer Over 90 alarm indicates that the per-NE queue of incoming alarm, event, or update capacity of 5000 entries is over 90% full. LOGBUFR90 will clear if CTC recovers. If it does not clear, the LOGBUFROVFL alarm occurs.



Note

LOGBUFR90 is an informational alarm and does not require troubleshooting.

2.7.213 LOGBUFROVFL

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

SONET Logical Object: SYSTEM

The Log Buffer Overflow alarm indicates that the CTC per-NE queue of incoming alarm, event, or updates, which has a capacity of 5000 entries, has overflowed. This happens only very rarely; if the alarm does occur, you must restart the CTC session. If this alarm occurs, it is likely that some updates are missing.

Clear the LOGBUFROVFL Alarm

-
- Step 1** Restart the CTC session.

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

2.7.214 LO-LASERBIAS

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

SONET Logical Objects: EQPT, OCN

DWDM Logical Object: PPM

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

If the LO-LASERBIAS alarm threshold is set at 0 percent (the default), the laser's usability has ended. If the threshold is set at 5 percent to 10 percent, the card is still usable for several weeks or months before you need to replace it.



Note

For more information about provisioning MXP or TXP PPMs, refer to the “Provision Transponders and Muxponders” chapter of the *Cisco ONS 15454 DWDM Procedure Guide*. For more information about the cards themselves, refer to the *Cisco ONS 15454 DWDM Reference Manual*.

Clear the LO-LASERBIAS Alarm

- Step 1** Complete the [“Physically Replace a Traffic Card” procedure on page 2-281](#).
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.215 LO-LASERTEMP

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

SONET Logical Objects: EQPT, OCN

DWDM Logical Object: PPM

The Equipment Low Laser Optical Transceiver Temperature alarm applies to the TXP and MXP cards. LO-LASERTEMP occurs when the internally measured transceiver temperature falls below the card setting by 35.6 degrees F or 2 degrees C. A laser temperature change affects the transmitted wavelength. (Two degrees Celsius is equivalent to about 200 picometers in the wavelength.)

When the TXP or MXP card raises this alarm, the laser is automatically shut off. The [“LOS \(OCN\)” alarm on page 2-168](#) is raised at the far-end node and the [“DUP-IPADDR” alarm on page 2-81](#) is raised at the near end. To verify the card laser temperature level, double-click the card in node view and click the **Performance > Optics PM > Current Values** tabs. Maximum, minimum, and average laser temperatures are shown in the Current column entries in the Laser Temp rows.

**Note**

For more information about provisioning MXP or TXP PPMs, refer to the “Provision Transponder and Muxponder Cards” chapter of the *Cisco ONS 15454 DWDM Procedure Guide*. For more information about the cards themselves, refer to the *Cisco ONS 15454 DWDM Reference Manual*.

Clear the LO-LASERTEMP Alarm

-
- Step 1** Complete the “[Reset a Traffic Card in CTC](#)” procedure on page 2-278 for the reporting MXP or TXP card.
- Step 2** If the alarm does not clear, complete the “[Physically Replace a Traffic Card](#)” procedure on page 2-281 for the reporting MXP or TXP card.
- Step 3** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.216 LOM

Default Severity: Critical (CR), Service-Affecting (SA) for STSMON, STSTRM, TRUNK;
Major (MJ) for VT-TERM

SONET Logical Objects: STSMON, STSTRM, VT-TERM

DWDM Logical Object: TRUNK

The Optical Transport Unit (OTU) Loss of Multiframe is a VCAT member alarm. (VCAT member circuits are independent circuits that are concatenated from different time slots into a higher-rate signal.) The alarm applies to MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, TXP_MR_10E, or TXPP_MR_2.5G cards when the Multi Frame Alignment Signal (MFAS) overhead field is errored for more than five frames and persists for more than 3 milliseconds.

**Note**

For more information about MXP or TXP cards, refer to the *Cisco ONS 15454 DWDM Reference Manual*.

Clear the LOM Alarm

-
- Step 1** Complete the “[Clear the SD-L Condition](#)” procedure on page 2-226. To clear this alarm against the DWDM trunk, refer to the *Cisco ONS 15454 DWDM Troubleshooting Guide*.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.
-

2.7.217 LOP-P

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

SONET Logical Objects: STSMON, STSTRM

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

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

For the FC_MR-4 card, an LOP-P is raised if a port is configured for a SONET signal but receives an SONET signal instead. (This information is contained in the H1 byte bits 5 and 6.)

Clear the LOP-P Alarm



Caution

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

-
- Step 1** In node view, click the **Circuits** tab and view the alarmed circuit.
 - Step 2** Verify the circuit size listed in the Size column. If the size is different from what is expected, such as an STS3c instead of an STS1, this causes the alarm.
 - Step 3** If you have been monitoring the circuit with optical test equipment, a mismatch between the provisioned circuit size and the size expected by the test set can cause this alarm. For specific procedures to use the test set equipment, consult the manufacturer. Ensure that the test set monitoring is set up for the same size as the circuit provisioning.

Refer to the manufacturer's instructions for test-set use.
 - Step 4** If the error is not due to an incorrectly configured test set, the error is in the provisioned CTC circuit size. Complete the [“Delete a Circuit” procedure on page 2-283](#).
 - Step 5** Recreate the circuit for the correct size. For procedures, refer to the “Create Circuits and VT Tunnels” chapter in the *Cisco ONS 15454 Procedure Guide*.
 - Step 6** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.
-

2.7.218 LOP-V

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

SONET Logical Objects: VT-MON, VT-TERM

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

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

Clear the LOP-V Alarm

Step 1 Complete the “Clear the LOP-P Alarm” procedure on page 2-159.



Caution

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

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

2.7.219 LO-RXPOWER

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

SONET Logical Object: OCN

DWDM Logical Objects: 2R, ESCON, FC, GE, ISC, TRUNK

The Equipment Low Receive Power alarm is an indicator for TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, MXP_2.5G_10G, MRC-12, MRC-4, and OC192-XFP card received optical signal power. LO-RXPOWER occurs when the measured optical power of the received signal falls below the threshold value, which is user-provisionable.



Note

For more information about MXP or TXP cards, refer to the *Cisco ONS 15454 DWDM Reference Manual*.



Note

When you upgrade a node to Software Release 6.0 or later, this enables received optical power PMs for the OC3-8, OC192-SR, OC192-IR, OC192-ITU, OC-192-XFP, MRC-12, and MRC25G-4 cards. The newly enabled HI-RXPOWER and LO-RXPOWER alarms require that you initialize a site-accepted optical power (OPR0) nominal value after the upgrade. (To do this, refer to the procedure in the “Turn Up a Node” chapter in the *Cisco ONS 15454 Procedure Guide*.) When you apply the value change, CTC uses the new OPR0 value to calculate PM percentage values. If you do not change the nominal value, the HI-RXPOWER or LO-RXPOWER may be raised in response to the unmodified setting.

Clear the LO-RXPOWER Alarm

Step 1 At the transmit end of the errored circuit, increase the transmit power level within safe limits.

Step 2 Find out whether new channels have been added to the fiber. Up to 32 channels can be transmitted on the same fiber, but the number of channels affects power. If channels have been added, power levels of all channels need to be adjusted.



Note

If the card is part of an amplified DWDM system, adding channels on the fiber affects the transmission power of each channel more than it would in an unamplified system.

- Step 3** Find out whether gain (the amplification power) of any amplifiers has been changed. Changing amplification also causes channel power to need adjustment.
- Step 4** If the alarm does not clear, remove any receive fiber attenuators or replace them with lower-resistance attenuators.
- Step 5** If the alarm does not clear, inspect and clean the receive and transmit node fiber connections according to site practice. If no site practice exists, complete the procedure in the “Maintain the Node” chapter in the *Cisco ONS 15454 Procedure Guide*.
- Step 6** If the alarm does not clear, ensure that the fiber is not broken or damaged by testing it with an optical test set. If no test set is available, use the fiber for a facility (line) loopback on a known-good port. The error reading you get is not as precise, but you generally know whether the fiber is faulty. For specific procedures to use the test set equipment, consult the manufacturer.
- Step 7** If the alarm does not clear, and no faults are present on the other port(s) of the transmit or receive card, do a facility loopback on the transmit and receive ports with known-good loopback cable. Complete the [“1.4.1 Perform a Facility Loopback on a Source-Node Optical Port” procedure on page 1-48](#) or the [“1.4.4 Perform a Facility Loopback on an Intermediate-Node Optical Port” procedure on page 1-57](#) to test the loopback.
- Step 8** If a port is bad and you need to use all the port bandwidth, complete the [“Physically Replace a Traffic Card” procedure on page 2-281](#). If the port is bad but you can move the traffic to another port, replace the card at the next available maintenance window.
- Step 9** If no ports are shown bad and the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

2.7.220 LOS (2R)

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.221 LOS (BITS)

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

SONET Logical Object: BITS

The LOS (BITS) alarm indicates that the TCC2/TCC2P has an LOS from the BITS timing source. The LOS (BITS) means the BITS clock or the connection to it failed.

Clear the LOS (BITS) Alarm



Caution

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

- Step 1** Verify the wiring connection from the BITS clock pin fields on the ONS 15454 backplane to the timing source.
- Step 2** If wiring is good, verify that the BITS clock is operating properly.

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

2.7.222 LOS (DS1)

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

SONET Logical Object: DS1

A LOS (DS1) alarm for a DS-1 port occurs when the port on the card is in service but no signal is being received. A cabling issue or a configuration issue could cause this alarm. If an upstream equipment failure causes a transmission failure, the LOS (DS1) will likely be demoted by a card-level alarm (to the DS1/E1-56).

Clear the LOS (DS1) Alarm



Caution

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

- Step 1** Verify that the fiber cable is properly connected and attached from the correct transmitting port to the correct receiving port. For more information about fiber connections and terminations, refer to the “Install Cards and Fiber-Optic Cable” chapter in the *Cisco ONS 15454 Procedure Guide*.
- Step 2** Clean the cable ends using site practices or, if none exists, complete the procedure in the “Maintain the Node” chapter of the *Cisco ONS 15454 Procedure Guide*.
- Step 3** If the alarm is raised on a DS1/E1-56 card, verify that the card is placed in the correct service mode by completing the following steps:
- Double-click the card to open the card view.
 - Click the **Provisioning > Card** tabs.
 - Verify that the **Operating Mode** column says All DS1 for your errored circuit.
- Step 4** For any other DS-1 or DS-3 card, consult site records to determine whether the port raising the alarm has been assigned.
- Step 5** If the port is not currently assigned, place the port out of service using the following steps:
- Double-click the card to open the card view.
 - For a DS-1 card, click the **Maintenance > Loopback** tabs. For a DS-1 line on a DS3XM-6 or DS3XM-12 card, click the **Maintenance > DS1** tabs.
 - Under Admin State, click **OOS,DSBLD**.
 - Click **Apply**.
- Step 6** For any card, if the port is assigned, verify that the correct one is in service:
- To confirm this physically, confirm that the LED is correctly illuminated on the physical card.
A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

- b. To determine this virtually, double-click the card in CTC to open the card view and complete the following substeps:
- Click the **Provisioning > Line** tabs.
 - Verify that the Admin State column lists the port as IS.
 - If the Admin State column lists the port as OOS,MT or OOS,DSBLD, click the column and choose **IS**. Click **Apply**.

**Note**

If ports managed into IS admin state are not receiving signals, the LOS alarm is either raised or remains, and the port service state transitions to OOS-AU,FLT.

- Step 7** Use a test set to confirm that a valid signal exists on the line. Test the line as close to the receiving card as possible. For specific procedures to use the test set equipment, consult the manufacturer.
- Step 8** Ensure that the transmit and receive outputs from the DSx patch panel to your equipment are properly connected. For more information about cable connections and terminations, refer to the “Install Cards and Fiber-Optic Cable” chapter in the *Cisco ONS 15454 Procedure Guide*.
- Step 9** If there is a valid signal but the alarm does not clear, replace the electrical connector on the ONS 15454.
- Step 10** If a valid electrical signal is not present and the transmitting device is operational, replace the fiber cable connecting the transmitting device to the Ethernet port. To do this, refer to the “Install Cards and Fiber-Optic Cable” chapter in the *Cisco ONS 15454 Procedure Guide*.
- Step 11** Repeat Steps 1 to 10 for any other port on the card that reports the LOS.
- Step 12** If the alarm does not clear, check for any card-level alarm that could affect this port.
- Step 13** If the alarm does not clear, complete the [“Physically Replace a Traffic Card” procedure on page 2-281](#) for the reporting card.
- Step 14** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.

2.7.223 LOS (DS3)

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

SONET Logical Object: DS3

The LOS (DS3) for a DS-3 port occurs when the port on a DS3XM-6, DS3XM-12, or DS3/EC1-48 card is in service but no signal is being received. The alarm is caused by incorrect or dirty cabling, a fiber break, or upstream equipment failure.

**Note**

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

Clear the LOS (DS3) Alarm

- Step 1** Check for any upstream failures in the transmitting equipment.
- Step 2** Verify that the cable is properly connected from the transmitting port and attached to the correct receiving port at the node with the LOS. For more information about fiber connections and terminations, refer to the “Install Cards and Fiber-Optic Cable” chapter in the *Cisco ONS 15454 Procedure Guide*.



Caution

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

- Step 3** Clean the cable ends using site practices or, if none exists, complete the procedure in the “Maintain the Node” chapter in the *Cisco ONS 15454 Procedure Guide*.
- Step 4** Consult site records to determine whether the port raising the alarm has been assigned.
- Step 5** If the port is not currently assigned, place the port out of service using the following steps:
- Double-click the card to open the card view.
 - Click the **Maintenance > DS3** tabs.
 - Under Admin State, click **OOS,DSBLD**.
 - Click **Apply**.
- Step 6** If the port is assigned, verify that the correct one is in service:
- To confirm this physically, confirm that the LED is correctly illuminated on the physical card.
A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
 - To determine this virtually, double-click the card in CTC to open the card view and complete the following substeps:
 - Click the **Provisioning > Line** tabs.
 - Verify that the Admin State column lists the port as IS.
 - If the Admin State column lists the port as OOS,MT or OOS,DSBLD, click the column and choose **IS**. Click **Apply**.



Note

If ports managed into IS admin state are not receiving signals, the LOS alarm is either raised or remains, and the port service state transitions to OOS-AU,FLT.

- Step 7** Use a test set to confirm that a valid signal exists on the line. Test the line as close to the receiving card as possible. (For specific procedures to use the test set equipment, consult the manufacturer.)
- Step 8** Ensure that the transmit and receive outputs from the DSx patch panel to your equipment are properly connected. For more information about cable connections and terminations, refer to the “Install Cards and Fiber-Optic Cable” chapter in the *Cisco ONS 15454 Procedure Guide*.
- Step 9** If there is a valid signal but the alarm does not clear, replace the electrical connector on the ONS 15454.
- Step 10** If the test set shows signal errors but the cabling is correctly installed and the transmitting device is operational, the existing cabling could still be faulty. Use the test set to locate the bad cable and replace it. To do this, refer to the “Install Cards and Fiber-Optic Cable” chapter in the *Cisco ONS 15454 Procedure Guide*.
- Step 11** Repeat Steps 1 to 10 for any other port on the card that reports the LOS.

- Step 12** If the alarm does not clear, complete the “[Physically Replace a Traffic Card](#)” procedure on page 2-281 for the reporting card.
- Step 13** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.
-

2.7.224 LOS (E1)

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

SONET Logical Object: E1

An LOS (E1) alarm for a DS1/E1-56 card port occurs when the card is placed in All E1 mode and is in service, but the alarmed port is not receiving a signal due to a physical or provisioning problem. The physical causes for the alarm could be incorrectly connected or faulty cabling. The software causes could be improperly configured card or circuit size.

For more information about the DS1/E1-56 card, refer to the “Electrical Cards” chapter in the *Cisco ONS 15454 Reference Manual*.

Clear the LOS (E1) Alarm



Caution

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

- Step 1** Verify that the cable is properly connected and attached to the correct port. For more information about connecting cable, refer to the “Install Cards and Fiber-Optic Cable” chapter in the *Cisco ONS 15454 Procedure Guide*. Also refer to site records for your specific cabling scheme.
- Step 2** Ensure that the transmit and receive outputs from the patch panel to your equipment are properly connected. For more information about cable connections and terminations, refer to the “Install Cards and Fiber-Optic Cable” chapter in the *Cisco ONS 15454 Procedure Guide*.
- Step 3** Clean the cable using your site practices. If none exists, complete the procedure in the “Maintain the Node” chapter in the *Cisco ONS 15454 Procedure Guide*.
- Step 4** Confirm that the card is properly provisioned to carry the E1 payload:
- Double-click the card to open the card view.
 - Click the **Provisioning > Card** tabs.
 - Under the **Operating Mode** column, you should see “All E1.” If you see “All DS1,” click the drop-down to change it and click **Apply**.
- Step 5** Use a test set to confirm that a valid E1 signal exists on the line. Test the line as close to the receiving card as possible. (For specific procedures to use the test set equipment, consult the manufacturer.) If the test set shows errors, the cabling could still be faulty despite being correctly installed. Use the tester to isolate the bad section of cable and replace it. Refer to the “Install Cards and Fiber-Optic Cable” chapter in the *Cisco ONS 15454 Procedure Guide* for procedures.
- Step 6** Repeat Steps 1 to 5 for any other port on the card that reports the LOS (E1).
- Step 7** If the alarm does not clear, look for any card-level alarm that could cause this alarm.

- Step 8** If the alarm does not clear, complete the “[Physically Replace a Traffic Card](#)” procedure on page 2-281 for the reporting card.
- Step 9** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.

2.7.225 LOS (EC1)

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

SONET Logical Object: EC1

LOS on an EC1/EC1-12 or DS3/EC1-48 port occurs when a SONET receiver detects an all-zero pattern for 10 microseconds or longer. An LOS (EC1) most likely means that the upstream transmitter has failed. If an EC1 LOS alarm is not accompanied by additional alarms, a cabling problem (such as an incorrect attachment, fiber cut, or other fiber error) usually causes this alarm. The condition clears when the problem is corrected, allowing two consecutive valid frames to be received.



Note

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

Clear the LOS (EC1) Alarm



Caution

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

- Step 1** Check for any upstream equipment failures that could cause the LOS (EC1) in this node.
- Step 2** If there is no cause upstream, verify cabling continuity from the transmitting port to the receiving port reporting LOS (EC1). To verify cable continuity, follow site practices.
- If the continuity is good, clean the fiber according to site practice. If none exists, complete the procedure in the “Maintain the Node” chapter in the *Cisco ONS 15454 Procedure Guide*.
- Step 3** If the cabling is good, verify that the correct EC1-12 port is in service:
- Confirm that the LED is correctly lit on the physical card.
A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
 - To determine whether the port is in service, double-click the card in CTC to open the card view.
 - Click the **Provisioning > Line** tabs.
 - Verify that the Admin State column lists the port as IS.
 - If the Admin State column lists the port as OOS, MT or OOS, DSBLD, click the column and choose **IS**. Click **Apply**.

**Note**

If ports managed into IS admin state are not receiving signals, the LOS alarm is either raised or remains, and the port service state transitions to OOS-AU,FLT.

- 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 patch panel to your equipment are properly connected. For more information about fiber connections and terminations, refer to the “Install Cards and Fiber-Optic Cable” chapter in the *Cisco ONS 15454 Procedure Guide*.
- Step 6** If a valid signal exists but the alarm does not clear, replace the cable connector on the ONS 15454.
- Step 7** Repeat Steps 2 through 6 for any other port on the card that reports the LOS (EC1).
- Step 8** If the alarm does not clear, the cabling could still be faulty despite correct attachments. Use the test set to locate the bad cable and replace it using the “Install Cards and Fiber-Optic Cable” chapter in the *Cisco ONS 15454 Procedure Guide*.
- Step 9** If the alarm does not clear, look for any card-level alarm that could cause this port alarm.
- Step 10** If the alarm does not clear, complete the “Physically Replace a Traffic Card” procedure on page 2-281 for the reporting card.
- Step 11** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.

2.7.226 LOS (ESCON)

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.227 LOS (FUDC)

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

SONET Logical Object: FUDC

The LOS (FUDC) alarm is raised if there is a UDC circuit created on an AIC-I UDC port but the port is not receiving signal input. The downstream node has an AIS condition raised against the AIC-I port transmitting the UDC. FUDC refers to the 64-kb user data channel using the F1 byte.

Clear the LOS (FUDC) Alarm

- Step 1** Verify cable continuity to the AIC-I UDC port. To verify cable continuity, follow site practices.
- Step 2** Verify that there is a valid input signal using a test set. For specific procedures to use the test set equipment, consult the manufacturer.
- Step 3** If there is a valid signal, clean the fiber according to site practice. If no site practice exists, complete the procedure in the “Maintain the Node” chapter in the *Cisco ONS 15454 Procedure Guide*.

- Step 4** If the alarm does not clear, verify that the UDC is provisioned:
- At the network view, click the **Provisioning > Overhead Circuits** tabs.
 - If no UDC circuit exists, create one. Refer to the “Create Circuits and VT Tunnels” chapter in the *Cisco ONS 15454 Procedure Guide*.
 - If a user data circuit exists (shown as User Data F1 under the Type column), check the source and destination ports. These must be located on AIC-I cards to function.
- Step 5** If the alarm does not clear, look for and troubleshoot any other alarm that could identify the source of the problem.
- Step 6** If no other alarms exist that could be the source of the LOS (FUDC), or if clearing another alarm did not clear the LOS, complete the [“Physically Replace a Traffic Card” procedure on page 2-281](#) for the reporting card.
- Step 7** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.228 LOS (ISC)

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.229 LOS (MSUDC)

The LOS (MSUDC) alarm is not used in this platform in this release. It is reserved for future development.

2.7.230 LOS (OCN)

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

SONET Logical Object: OCN

An LOS alarm on an OC-N port occurs when a SONET receiver detects an all-zero pattern for 10 microseconds or longer. An LOS alarm means the upstream transmitter has failed. If an OC-N LOS alarm is not accompanied by additional alarms, a fiber break is usually the cause of the alarm. It clears when two consecutive valid frames are received.



Warning

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



Warning

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

**Warning**

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

**Note**

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

Clear the LOS (OCN) Alarm

**Caution**

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

Step 1

Using site practices, verify fiber continuity to the port.

Step 2

If the cabling is good, verify that the correct port is in service:

- a. Confirm that the LED is correctly illuminated on the physical card.
A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
- b. To determine whether the OC-N port is in service, double-click the card in CTC to open the card view.
- c. Click the **Provisioning > Line** tabs.
- d. Verify that the Admin State column lists the port as IS.
- e. If the Admin State column lists the port as OOS,MT or OOS,DSBLD, click the column and choose **IS**.
- f. Click **Apply**.

**Note**

If ports managed into IS admin state are not receiving signals, the LOS alarm is either raised or remains, and the port service state transitions to OOS-AU,FLT.

Step 3

If the correct port is in service, clean the fiber according to site practice. If no site practice exists, complete the procedure in the “Maintain the Node” chapter of the *Cisco ONS 15454 Procedure Guide*.

Step 4

If the alarm does not clear, verify that the power level of the optical signal is within the OC-N card receiver specifications. The [“1.12.3 OC-N Card Transmit and Receive Levels” section on page 1-147](#) lists these specifications for each OC-N card. For DWDM cards, refer to the *Cisco ONS 15454 DWDM Reference Manual* for levels.

Step 5

If the optical power level is within specifications, use an optical test set to verify that a valid signal exists on the line. For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving card as possible.

Step 6

If a valid signal exists, replace the connector on the backplane.

Step 7

Repeat Steps 1 to 6 for any other port on the card reporting the LOS (OC-N).

Step 8

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

- Step 9** If no other alarms exist that could be the source of the LOS, or if clearing an alarm did not clear the LOS, complete the [“Physically Replace a Traffic Card” procedure on page 2-281](#) for the reporting card.
- Step 10** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.
-

2.7.231 LOS (OTS)

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.232 LOS (TRUNK)

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.233 LOS-0

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.234 LOS-P (OCH)

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.235 LOS-P (OMS, OTS)

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.236 LOS-P (TRUNK)

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.237 LOS-RAMAN (OTS)

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

SONET Logical Objects: OTS

The Loss of Raman signal alarm indicates that the Raman signal has not been received by the RX RAMAN port.

Clear the LOS-RAMAN Condition

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



Caution

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

- Step 2** Consult site records to determine whether the port raising the alarm has been assigned. If the port is not assigned, assign it.

- Step 3** If the port is assigned, verify that the correct port is in service by completing the following steps:
- To confirm this physically, confirm that the card shows a green LED on the physical card.
A green LED indicates an active card. An amber LED indicates a standby card.
 - To determine this virtually, double-click the card in CTC to display the card view and complete the following substeps:
 - Click the **Provisioning > Line** tabs.
 - Verify that the **Admin State** column lists the port as IS.
 - If the **Admin State** column lists the port as OOS,MT or OOS,DSBLD, click the column and choose **IS**.



Note

If a port in the unlocked admin state does not receive a signal, the LOS alarm is raised and the port service state transitions to Locked-disabled, automaticInService & failed.

- Click **Apply**.

- Step 4** Use a test set to confirm that a valid signal exists on the line. Test the line as close to the receiving card as possible. For specific procedures to use the test set equipment, consult the manufacturer.

- Step 5** If a valid signal is not present and the transmitting device is operational, replace the cable connecting the transmitting device to the port. To do this, refer to the “Install Hardware” chapter in the *Cisco ONS 15454 Procedure Guide*.

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

- Step 7** If no other alarms are present that could be the source of the LOS, or if clearing an alarm did not clear the LOS, complete the [“Physically Replace a Traffic Card” procedure on page 2-281](#) for the reporting card.



Note

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

- Step 8** If the alarm does not clear, log into the Cisco Technical Support Website at <http://www.cisco.com/techsupport> for more information or log into <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml> to obtain a directory of toll-free Technical Support numbers for your country in order to report a Service-Affecting (SA) problem.

2.7.238 LO-TXPOWER

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

SONET Logical Objects: EQPT, OCN

DWDM Logical Objects: 2R, ESCON, FC, GE, ISC, PPM

The Equipment Low Transmit Power alarm is an indicator for the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, MXP_2.5G_10G, MRC-12, MRC-4, and OC192-XFP card transmitted optical signal power. LO-TXPOWER occurs when the measured optical power of the transmitted signal falls under the threshold. The threshold value is user-provisionable.



Note

For more information about provisioning MXP or TXP PPMs, refer to the “Provision Transponders and Muxponders” chapter of the *Cisco ONS 15454 DWDM Procedure Guide*. For more information about the cards themselves, refer to the *Cisco ONS 15454 DWDM Reference Manual*.

Clear the LO-TXPOWER Alarm

- Step 1** Display the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, MXP_2.5G_10G, or OC192-XFP card view.
- Step 2** Click the **Provisioning > Optics Thresholds > Current Values** tabs.
- Step 3** Increase the TX Power Low column value by 0.5 dBm.
- Step 4** If the card transmit power setting cannot be increased without affecting the signal, complete the [“Physically Replace a Traffic Card” procedure on page 2-281](#).
- Step 5** If no ports are shown bad and the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

2.7.239 LPBKCRS

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

SONET Logical Objects: STSMON, STSTRM

The Loopback Cross-Connect condition indicates that there is a software cross-connect loopback active between the optical cards. A cross-connect loopback test occurs below line speed and does not affect traffic.

For more information on loopbacks, see the [“1.4 Troubleshooting Optical Circuit Paths With Loopbacks” section on page 1-47](#).

**Note**

Cross-connect loopbacks occur below line speed. They do not affect traffic.

Clear the LPBKCRS Condition

- Step 1** To remove the loopback cross-connect condition, double-click the optical card in CTC to open the card view.
- Step 2** Complete the [“Clear an OC-N Card Cross-Connect \(XC\) Loopback Circuit” procedure on page 2-284.](#)
- Step 3** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

2.7.240 LPBKDS3FEAC

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

SONET Logical Object: DS3

A Loopback Due to FEAC Command DS-3 condition occurs when a DS3XM-6, DS3XM-12, DS3-12E, or DS3/EC1-48 port loopback signal is received in C-bit framing mode from the far-end node because of an FEAC command. An FEAC command is often used with loopbacks. LPBKDS3FEAC is only reported by these DS cards. DS3XM-6, DS3XM-12, and DS3/EC1-48 cards generate and report FEAC alarms or conditions, but a DS3-12E card only reports FEAC alarms or conditions.

**Caution**

CTC permits loopbacks on an in-service (IS) circuit. Loopbacks are Service-Affecting (SA).

**Note**

LPBKDS3FEAC is an informational condition and does not require troubleshooting.

Clear the LPBKDS3FEAC Condition

- Step 1** In node view, double-click the DS-3 card to open the card view.
- Step 2** Click the **Maintenance > DS3** tabs.
- Step 3** Click the cell for the port in the Send Code column and click **No Code** from the drop-down list.
- Step 4** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

2.7.241 LPBKDS3FEAC-CMD

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

SONET Logical Object: DS3

The DS-3 Loopback Command Sent To Far End condition occurs on the near-end node when you send a DS-3 FEAC loopback on DS3XM-6, DS3XM-12, or DS3/EC1-48 cards. For more information about FEAC loopbacks, see the “[1.3 Troubleshooting DS3XM-6 or DS3XM-12 Card Electrical Paths With FEAC Loopbacks](#)” section on page 1-45.

**Note**

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

2.7.242 LPBKFACILITY (CEMR, CE1000, CE100T)

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

SONET Logical Objects: CEMR, CE1000, CE100T

A Loopback Facility condition on a CE-Series port occurs when a software facility (line) loopback is active for a port on the card.

**Note**

For information about troubleshooting Ethernet circuits with loopbacks, refer to the “[1.5 Troubleshooting Ethernet Circuit Paths With Loopbacks](#)” section on page 1-68.

**Note**

For more information about Ethernet cards, refer to the Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.

Clear the LPBKFACILITY (CEMR, CE1000, CE100T) Condition

- Step 1** Complete the “[Clear Other Electrical Card or Ethernet Card Loopbacks](#)” procedure on page 2-284.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

2.7.243 LPBKFACILITY (DS1, DS3)

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

SONET Logical Objects: DS1, DS3

A Loopback Facility condition on a DS-1 or DS-3 port occurs when a software facility (line) loopback is active for the reporting DS3XM-6 card, DS3XM-12 card, a DS1/E1-56 card operating in All DS1 mode, or a DS3/EC1-48 card.

For information about troubleshooting electrical circuits with loopbacks, refer to the “[1.5 Troubleshooting Ethernet Circuit Paths With Loopbacks](#)” section on page 1-68.

**Note**

CTC permits loopbacks to be performed on an in-service (IS) circuit. Performing a loopback is Service-Affecting (SA). If you did not perform a lockout or Force switch to protect traffic, the LPBKFACILITY condition can be accompanied by a more serious alarms such as the “[LOS \(DS1\)](#)” alarm on page 2-162, or the “[LOS \(DS3\)](#)” alarm on page 2-163.

**Note**

ONS 15454 DS-3 terminal (inward) loopbacks do not transmit an “AIS” alarm on page 2-38, in the direction away from the loopback. Instead of AIS, a continuance of the signal transmitted into the loopback is provided. A DS3/EC1-48 card can be provisioned to transmit AIS for a terminal loopback if desired.

Clear the LPBKFACILITY (DS1, DS3) Condition

- Step 1** Complete the “[Clear a DS3XM-6, DS3XM-12, or DS3E-12 Card Loopback Circuit](#)” procedure on page 2-284.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

2.7.244 LPBKFACILITY (E1)

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

SONET Logical Object: E1

A Loopback Facility on an E1 port condition occurs when a software facility (line) loopback is active for a DS1/E1-56 card port operating in All E1 mode.

For information about troubleshooting electrical circuits with loopbacks, refer to the “[1.2 Troubleshooting Electrical Circuit Paths With Loopbacks](#)” section on page 1-9.

**Note**

CTC permits loopbacks to be performed on an in-service (IS) circuit. Performing a loopback is Service-Affecting (SA). If you did not perform a lockout or Force switch to protect traffic, the LPBKFACILITY condition can be accompanied by a more serious alarms such as LOS.

**Note**

E1 facility (line) loopbacks transmit an AIS in the direction away from the loopback, but this is provisionable.

Clear the LPBKFACILITY (E1) Condition

- Step 1** Complete the “[Clear Other Electrical Card or Ethernet Card Loopbacks](#)” procedure on page 2-284.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

2.7.245 LPBKFACILITY (EC1)

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

2.7.246 LPBKFACILITY (ESCON)

SONET Logical Object: EC1

A Loopback Facility condition on an EC-1 port occurs when a software facility (line) loopback is active for a port on the reporting EC1/EC1-12 or DS3/EC1-48 card.

For information about troubleshooting electrical circuits with loopbacks, refer to the [“1.2 Troubleshooting Electrical Circuit Paths With Loopbacks”](#) section on page 1-9.



Caution

CTC permits loopbacks on an in-service (IS) circuit. Loopbacks are Service-Affecting (SA).

Clear the LPBKFACILITY (EC1) Condition

-
- Step 1** Complete the [“Clear Other Electrical Card or Ethernet Card Loopbacks”](#) procedure on page 2-284.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.246 LPBKFACILITY (ESCON)

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.247 LPBKFACILITY (FC)

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.248 LPBKFACILITY (FCMR)

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

SONET Logical Object: FCMR

A Loopback Facility for FCMR condition occurs when a facility loopback is provisioned on an FC_MR-4 card.

For information about troubleshooting these circuits with loopbacks, refer to the [“1.6 Troubleshooting FC_MR Circuit Paths With Loopbacks”](#) section on page 1-94.

Clear the LPBKFACILITY (FCMR) Condition

-
- Step 1** Complete the [“Clear an MXP, TXP, or FC_MR-4 Card Loopback Circuit”](#) procedure on page 2-285.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.249 LPBKFACILITY (G1000)

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

SONET Logical Object: G1000

A Loopback Facility condition for the G1000 object occurs when a software facility (line) loopback is active for a port on the reporting G-Series Ethernet card.

For information about troubleshooting Ethernet circuits with loopbacks, refer to the [“1.5 Troubleshooting Ethernet Circuit Paths With Loopbacks”](#) section on page 1-68.

**Caution**

CTC permits loopbacks on an in-service (IS) circuit. Loopbacks are Service-Affecting (SA).

**Note**

For more information about Ethernet cards, refer to the Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.

Clear the LPBKFACILITY (G1000) Condition

- Step 1** Complete the [“Clear Other Electrical Card or Ethernet Card Loopbacks”](#) procedure on page 2-284.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

2.7.250 LPBKFACILITY (GE)

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.251 LPBKFACILITY (ISC)

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.252 LPBKFACILITY (OCN)

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

SONET Logical Object: OCN

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

For information about troubleshooting optical circuits with loopbacks, refer to the [“1.4 Troubleshooting Optical Circuit Paths With Loopbacks”](#) section on page 1-47.

2.7.253 LPBKFACILITY (TRUNK)

**Note**

OC-3 facility loopbacks do not transmit an AIS in the direction away from the loopback. Instead of AIS, a continuance of the signal transmitted to the loopback is provided.

**Caution**

CTC permits loopbacks on an in-service (IS) circuit. Loopbacks are Service-Affecting (SA).

**Caution**

Before performing a facility (line) loopback on an OC-N card, ensure that the card contains at least two DCC paths to the node where the card is installed. A second DCC path provides a nonlooped path to log into the node after the loopback is applied, thus enabling you to remove the facility loopback. Ensuring a second DCC is not necessary if you are directly connected to the ONS 15454 containing the loopback OC-N.

Clear the LPBKFACILITY (OCN) Condition

- Step 1** Complete the [“Clear an OC-N Card Facility or Terminal Loopback Circuit” procedure on page 2-283](#).
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

2.7.253 LPBKFACILITY (TRUNK)

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.254 LPBKTERMINAL (CEMR, CE1000, CE100T)

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

SONET Logical Objects: CEMR, CE1000, CE100T,

A Loopback Terminal condition on a CE-Series port occurs when a software terminal loopback is active for a port on the card.

**Note**

For information about troubleshooting Ethernet circuits with loopbacks, refer to the [“1.5 Troubleshooting Ethernet Circuit Paths With Loopbacks” section on page 1-68](#).

**Note**

For more information about Ethernet cards, refer to the Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.

Clear the LPBKTERMINAL (CEMR, CE1000, CE100T) Condition

-
- Step 1** Complete the [“Clear Other Electrical Card or Ethernet Card Loopbacks” procedure on page 2-284](#).
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.255 LPBKTERMINAL (DS1, DS3)

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

SONET Logical Objects: DS1, DS3

A Loopback Terminal condition for a DS-1 or DS-3 occurs when a software terminal (inward) loopback is active for a DS1 or DS3 port on the reporting DS3XM-6, DS3XM-12, or DS3/EC1-48 card. DS-1 and DS-3 terminal loopbacks do not typically return an AIS signal, but you can provision one for the DS3/EC1-48 card.

For information about troubleshooting electrical circuits with loopbacks, refer to the [“1.3 Troubleshooting DS3XM-6 or DS3XM-12 Card Electrical Paths With FEAC Loopbacks” section on page 1-45](#).

Clear the LPBKTERMINAL (DS1, DS3) Condition

-
- Step 1** Complete the [“Clear a DS3XM-6, DS3XM-12, or DS3E-12 Card Loopback Circuit” procedure on page 2-284](#).
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.256 LPBKTERMINAL (E1)

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

SONET Logical Object: E1

A Loopback Terminal condition for an E-1 signal on a DS1/E1-56 card occurs when the card is operating in All E1 mode and a software terminal (inward) loopback is active for a port.

For information about troubleshooting electrical circuits with loopbacks, refer to the [“1.3 Troubleshooting DS3XM-6 or DS3XM-12 Card Electrical Paths With FEAC Loopbacks” section on page 1-45](#).

Clear the LPBKTERMINAL (E1) Condition

-
- Step 1** Complete the [“Clear Other Electrical Card or Ethernet Card Loopbacks” procedure on page 2-284](#).
-

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

2.7.257 LPBKTERMINAL (EC1)

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

SONET Logical Object: EC1

A Loopback Terminal condition on an EC-1 signal occurs when a software terminal (inward) loopback is active for a port on the reporting EC1/EC1-12 or DS3/EC1-48 card.

For information about troubleshooting electrical circuits with loopbacks, refer to the [“1.2 Troubleshooting Electrical Circuit Paths With Loopbacks”](#) section on page 1-9.



Caution

CTC permits loopbacks on an in-service (IS) circuit. Loopbacks are Service-Affecting (SA).

Clear the LPBKTERMINAL (EC1) Condition

- Step 1** Complete the [“Clear Other Electrical Card or Ethernet Card Loopbacks”](#) procedure on page 2-284.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

2.7.258 LPBKTERMINAL (ESCON)

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.259 LPBKTERMINAL (FC)

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.260 LPBKTERMINAL (FCMR)

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

SONET Logical Object: FCMR

A Loopback Terminal for FCMR condition occurs when a terminal loopback is provisioned on an FC_MR-4 card.

For information about troubleshooting these circuits with loopbacks, refer to the [“1.6 Troubleshooting FC_MR Circuit Paths With Loopbacks”](#) section on page 1-94.

Clear the LPBKTERMINAL (FCMR) Condition

-
- Step 1** Complete the [“Clear an MXP, TXP, or FC_MR-4 Card Loopback Circuit” procedure on page 2-285](#).
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.261 LPBKTERMINAL (G1000)

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

SONET Logical Object: G1000

A Loopback Terminal condition for the G1000 occurs when a software terminal (inward) loopback is active for a port on the reporting G-Series Ethernet card.

When a port in terminal (inward) loopback, its outgoing signal is redirected into the receive direction on the same port, and the externally received signal is ignored. On the G1000-4 card, the outgoing signal is not transmitted; it is only redirected in the receive direction.

For more information about troubleshooting Ethernet circuits, refer to the [“1.5 Troubleshooting Ethernet Circuit Paths With Loopbacks” section on page 1-68](#).

**Caution**

CTC permits loopbacks on an in-service (IS) circuit. Loopbacks are Service-Affecting (SA).

**Note**

For more information about Ethernet cards, refer to the Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.

Clear the LPBKTERMINAL (G1000) Condition

-
- Step 1** Complete the [“Clear Other Electrical Card or Ethernet Card Loopbacks” procedure on page 2-284](#).
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.262 LPBKTERMINAL (GE)

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.263 LPBKTERMINAL (ISC)

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.264 LPBKTERMINAL (OCN)

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

SONET Logical Object: OCN

A Loopback Terminal condition for an OC-N port occurs when a software terminal (inward) loopback is active for a port on the reporting card.



Note

OC-N terminal loopbacks do not typically return an AIS.



Note

Performing a loopback on an in-service circuit is Service-Affecting (SA). If you did not perform a lockout or Force switch to protect traffic, the LPBKTERMINAL condition can also be accompanied by a more serious alarm such as LOS.

For information about troubleshooting circuits, refer to the loopback procedures in [Chapter 1, “General Troubleshooting.”](#)

Clear the LPBKTERMINAL (OCN) Condition

- Step 1** Complete the [“Clear an OC-N Card Facility or Terminal Loopback Circuit” procedure on page 2-283.](#)
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

2.7.265 LPBKTERMINAL (TRUNK)

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.266 LWBATVG

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

SONET Logical Object: PWR

The Low Voltage Battery alarm occurs in a –48 VDC environment when a battery lead input voltage falls below the low power threshold. This threshold, with a default value of –44 VDC, is user-provisionable. The alarm remains raised until the voltage remains above the threshold for 120 seconds. (For information about changing this threshold, refer to the “Turn Up Node” chapter in the *Cisco ONS 15454 Procedure Guide*.)

Clear the LWBATVG Alarm

- Step 1** The problem is external to the ONS 15454. Troubleshoot the power source supplying the battery leads.

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

2.7.267 MAN-REQ

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

SONET Logical Objects: EQPT, ML1000, ML100T, MLFX, STSMON, VT-MON

The Manual Switch Request condition occurs on a SONET entity when a user initiates a Manual switch request on an OC-N port. Clearing the Manual switch clears the MAN-REQ condition. You do not need to clear the switch if you want the Manual switch to remain.

MAN-REQ is raised for an IEEE 802.17b-based RPR span if the manual switch was requested in the Cisco IOS CLI with the “`rpr-ieee protection request manual-switch {east | west}`” command. It clears from the IEEE 802.17b-based RPR span when you remove the switch in the CLI. For the RPR-IEEE, MAN-REQ suppresses the “RPR-SD” alarm on page 2-219, and the “WTR” alarm on page 2-266. This condition is suppressed by the following alarms:

- [FORCED-REQ, page 115](#)
- [RPR-PASSTHR, page 215](#)
- [RPR-SF, page 220](#)

Clear the MAN-REQ Condition

- Step 1** If the condition is raised against a SONET entity, complete the “[Initiate a 1+1 Manual Switch Command](#)” procedure on page 2-270.
- Step 2** If the condition is raised on an IEEE 802.17b-based RPR span, enter the following CLI command in RPR-IEEE interface configuration mode:
- ```
router(config-if)#no rpr-ieee protection request manual-switch {east | west}
```
- Step 3** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

## 2.7.268 MANRESET

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

SONET Logical Object: EQPT

A User-Initiated Manual Reset condition occurs when you right-click a card in CTC and choose Reset.



#### Note

MANRESET is an informational condition and does not require troubleshooting.

## 2.7.269 MANSWTOINT

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

SONET Logical Object: NE-SREF

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



**Note**

MANSWTOINT is an informational condition and does not require troubleshooting.

## 2.7.270 MANSWTOPRI

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

SONET Logical Objects: EXT-SREF, NE-SREF

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



**Note**

MANSWTOPRI is an informational condition and does not require troubleshooting.

## 2.7.271 MANSWTOSEC

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

SONET Logical Objects: EXT-SREF, NE-SREF

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



**Note**

MANSWTOSEC is an informational condition and does not require troubleshooting.

## 2.7.272 MANSWTOTHIRD

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

SONET Logical Objects: EXT-SREF, NE-SREF

The Manual Switch To Third Reference condition occurs when the NE timing source is manually switched to a third timing source.



**Note**

MANSWTOTHIRD is an informational condition and does not require troubleshooting.

## 2.7.273 MANUAL-REQ-RING

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

SONET Logical Object: OCN

The Manual Switch Request on Ring condition occurs when a user initiates a MANUAL RING command on BLSR rings to switch from working to protect or protect to working. This condition is visible on the network view Alarms, Conditions, and History tabs and is accompanied by WKSWPR. The port where the MANUAL RING command originated is marked with an “M” on the network view detailed circuit map.

## Clear the MANUAL-REQ-RING Condition

- 
- Step 1** Complete the “[Clear a BLSR External Switching Command](#)” procedure on page 2-277.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
- 

## 2.7.274 MANUAL-REQ-SPAN

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

SONET Logical Object: EC1, OCN

DWDM Logical Objects: 2R, ESCON, FC, GE, ISC, TRUNK

The Manual Switch Request on Ring condition occurs on BLSRs when a user initiates a Manual Span command to move BLSR traffic from a working span to a protect span. This condition appears on the network view Alarms, Conditions, and History tabs. The port where the MANUAL SPAN command was applied is marked with an “M” on the network view detailed circuit map.

## Clear the MANUAL-REQ-SPAN Condition

- 
- Step 1** Complete the “[Clear a BLSR External Switching Command](#)” procedure on page 2-277.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
- 

## 2.7.275 MAX-STATIONS

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

SONET Logical Object: RPRIF

The Maximum IEEE 802.17b-based RPR Station Number Exceeded alarm can be raised by all ML card stations on a ring when the maximum quantity of stations, 255, is exceeded. This excess causes the IEEE 802.17b-based RPR scheme—and traffic—to break down.

IEEE 802.17b-based RPR messaging uses time-to-live (TTL), an 8-bit value. The maximum value these 8 bits (one byte) can have is 255. As a message travels (or hops) from station to station, the TTL is decremented by each station. Thus one station cannot communicate with another station more than 255 hops away.

If you are creating a large ring (more than 127 nodes), the MAX-STATIONS alarm might be raised until the ring is closed and stable.

MAX-STATIONS does not suppress any other alarms. However, this alarm is suppressed by the “RPR-PASSTHR” alarm on page 2-215.

## Clear the MAX-STATIONS Alarm

- 
- Step 1** Remove the extra stations from the ring to clear this alarm in all other stations and to restore traffic in the ring. For procedures to add or remove IEEE 802.17b-based RPR stations, refer to the *Cisco ONS 15454 and Cisco ONS 15454 SDH Ethernet Card Software Feature and Configuration Guide*.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 to report a Service-Affecting (SA) problem.
- 

## 2.7.276 MCAST-MAC-TABLE-FULL (EQPT)

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

## 2.7.277 MEA (AIP)

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

SONET Logical Object: AIP

If the Mismatch of Equipment Attributes (MEA) alarm is reported against the AIP, the fuse in the AIP board blew or is missing. The MEA alarm also occurs when an old AIP board with a 2-A fuse is installed in a newer ANSI 10-Gbps-compatible shelf assembly (15454-SA-ANSI or 15454-SA-HD).

## Clear the MEA (AIP) Alarm

- 
- Step 1** Complete the “[Replace the Alarm Interface Panel](#)” procedure on page 2-289.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.
- 

## 2.7.278 MEA (BIC)

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

SONET Logical Object: BIC

The Missing Equipment Attributes alarm for the backplane interface connector (BIC) indicates a compatibility issue in using high-density DS-3 cards with universal backplane interface connectors (UBIC) and an older shelf backplane. The backplane on the high-density shelf assembly, 15454-SA-HD, is compatible with the UBIC with horizontal connectors (UBIC-H) and UBIC with vertical connectors (UBIC-V) that the high-density EC-1, DS-1, and DS-3 electrical connections require. The MEA alarm is raised if you attempt to install a high-density card in Slot 4, 5, 6, 12, 13, or 14 in a shelf assembly with an older, incompatible backplane. The card is not usable in this case. It is also raised if you attempt to use an older BIC (also known as electrical interface assemblies [EIAs]) with the newer shelf assembly.

## Clear the MEA (BIC) Alarm

- Step 1** Click the **Provisioning > Inventory** tabs to determine your backplane model. If the backplane is not a 15454-SA-HD, replace the backplane or do not attempt to use high-density DS-3 cards. The following tables list the EIA Types that are compatible with various backplanes.

**Table 2-18** *EIA Types Compatible with the 15454-SA-ANSI Only*

| EIA Type          | A-Side Product Number | B-Side Product Number |
|-------------------|-----------------------|-----------------------|
| BNC               | 15454-EIA-BNC-A24=    | 15454-EIA-BNC-A24=    |
| High- Density BNC | 15454-EIA-BNC-A48=    | 15454-EIA-BNC-B48=    |
| SMB               | 15454-EIA-SMB-A84=    | 15454-EIA-SMB-B84=    |
| AMP Champ         | 15454-EIA-AMP-A84=    | 15454-EIA-AMP-B84=    |

**Table 2-19** *EIA Types Compatible with the 15454-SA-ANSI and the 15454-SA-HD*

| EIA Type          | A-Side Product Number | B-Side Product Number |
|-------------------|-----------------------|-----------------------|
| BNC               | 15454-EIA-BNC-A24=    | 15454-EIA-BNC-B24=    |
| High- Density BNC | 15454-EIA-1BNCA48=    | 15454-EIA-1BNCB48=    |
| Mini(BNC)         | 15454-EIA-BNC-A96=    | 15454-EIA-BNC-A96=    |
| SMB               | 15454-EIA-1SMBA84=    | 15454-EIA-1SMBB84=    |
| AMP Champ         | 15454-EIA-1AMPA84=    | 15454-EIA-1AMPB84=    |
| UBIC-V            | 15454-EIA-UBICV-A     | 15454-EIA-UBICV-B     |
| UBIC-H            | 15454-EIA-UBICH-A     | 15454-EIA-UBICH-B     |

- Step 2** If you determine that your BIC type and backplane are compatible despite the MEA alarm, or if the alarm does not clear after you resolve the incompatibilities, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.

## 2.7.279 MEA (EQPT)

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

SONET Logical Object: EQPT

The MEA alarm for equipment is reported against a card slot when the physical card inserted into a slot does not match the card type that is provisioned for that slot in CTC. The alarm also occurs when certain cards introduced in Release 3.1 or later are inserted into an older shelf assembly or when older Ethernet cards (E1000-2 and E100T-12) are used in a newer 10-Gbps-compatible shelf assembly.

Removing the incompatible cards clears the alarm.



**Note**

For more information about Ethernet cards, refer to the Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.



**Note**

If an OC3-8 card is installed in Slot 5 to 6 and Slot 12 to 13, it does not appear in CTC and raises an MEA.

### Clear the MEA (EQPT) Alarm

- Step 1** Physically verify the type of card that is installed in the slot reporting the MEA alarm. In node view, click the **Inventory** tab and compare it to the actual installed card.
- Step 2** Determine whether the ONS 15454 shelf assembly is a newer 10-Gbps-compatible shelf assembly (15454-SA-ANSI or 15454-SA-HD) or an earlier shelf assembly. Under the HW Part # column, if the part number is 800-19857-XX or 800-19856-XX, then you have a 15454-SA-ANSI shelf. If the part number is 800-24848-XX, then you have a 15454-SA-HD shelf. If the number is not one of those listed above, then you are using an earlier shelf assembly.



**Note**

On the 15454-SA-HD (P/N: 800-24848), 15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1 (P/N: 800-07149) shelves, the AIP cover is clear plastic. On the 15454-SA-ANSI shelf (P/N: 800-19857), the AIP cover is metal.

- Step 3** Verify the type of card that sits in the slot reported in the object column of the MEA row on the Alarms window by reading the name at the top of the card faceplate.
- If you have a newer 10-Gbps-compatible shelf assembly (15454-SA-ANSI or 15454-SA-HD) and the card reporting the alarm is not an E1000-2 or E100T-12, proceed to [Step 4](#).
  - If you have a newer 10-Gbps-compatible shelf assembly (15454-SA-ANSI or 15454-SA-HD) and the card reporting the alarm is an E1000-2 or E100T-12, then that version of the Ethernet card is incompatible and must be removed. Proceed to [Step 4](#).



**Note**

The E1000-2-G and E100T-G cards are compatible with the newer ANSI 10-Gbps-compatible shelf assembly and are the functional equivalent of the older, noncompatible E1000-2 and E100T-12 cards. E1000-2-G and E100T-G cards can be used as replacements for E1000-2 and E100T-12 cards in a 10-Gbps-compatible shelf assembly.

- If you have an older shelf assembly and the card reporting the alarm is not a card introduced in Release 3.1 or later, which includes the OC-192, E1000-2-G, E100T-G, or OC-48 any slot (AS), proceed to [Step 4](#).
- If you have an older shelf assembly and the card reporting the alarm is a card introduced in Release 3.1 or later, which includes the OC-192, E1000-2-G, E100T-G, or OC-48 any slot (AS), the reporting card is incompatible with the shelf assembly and must be removed. Proceed to [Step 4](#).

**Step 4** If you prefer the card type depicted by CTC, complete the [“Physically Replace a Traffic Card” procedure on page 2-281](#) for the reporting card.

**Step 5** If you prefer the card that physically occupies the slot but the card is not in service, does not have circuits mapped to it, and is not part of a protection group, place 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, does have circuits mapped to it, is paired in a working protection scheme, has DCC communications turned on, or is used as a timing reference, CTC does not allow you to delete the card.

**Step 6** If any ports on the card are in service, place them out of service (OOS,MT):



**Caution**

Before placing ports out of service, ensure that live traffic is not present.

- Double-click the reporting card to open the card view.
- Click the **Provisioning** tab.
- Click the admin state of any in-service ports.
- Choose **OOS,MT** to take the ports out of service.

**Step 7** If a circuit has been mapped to the card, complete the [“Delete a Circuit” procedure on page 2-283](#).



**Caution**

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

**Step 8** If the card is paired in a protection scheme, delete the protection group:

- Click the **Provisioning > Protection** tabs.
- Choose the protection group of the reporting card.
- Click **Delete**.

**Step 9** Right-click the card reporting the alarm.

**Step 10** Choose **Delete**.

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

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

## 2.7.280 MEA (FAN)

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

SONET Logical Object: FAN

The MEA alarm is reported against the fan-tray assembly when a newer fan-tray assembly (15454-FTA3) with a 5-A fuse is used with an older shelf assembly or when an older fan-tray assembly with a 2-A fuse is used with a newer 10-Gbps-compatible shelf assembly (15454-SA-ANSI or 15454-SA-HD) that contains cards introduced in Release 3.1 or later. If a 10-Gbps-compatible shelf assembly contains only cards introduced before Release 3.1, then an older fan-tray assembly (15454-FTA-2) can be used and does not report an MEA alarm.

### Clear the MEA (FAN) Alarm

- 
- Step 1** Determine whether the shelf assembly is a newer 10-Gbps-compatible shelf assembly (15454-SA-ANSI or 15454-SA-HD) or an earlier shelf assembly. In node view, click the **Inventory** tab.
- Under the HW Part # column, if the part number is 800-19857-XX or 800-19856-XX, then you have a 15454-SA-ANSI shelf. If the part number is 800-24848-XX, you have a 15454-SA-HD shelf.
- Under the HW Part # column, if the number is not one of those listed above, then you are using an earlier shelf assembly.
- Step 2** If you have a 10-Gbps-compatible shelf assembly (15454-SA-ANSI or 15454-SA-HD), the alarm indicates that an older incompatible fan-tray assembly is installed in the shelf assembly. Obtain a newer fan-tray assembly (15454-FTA3) with a 5-A fuse and complete the [“Replace the Fan-Tray Assembly” procedure on page 2-288](#).
- Step 3** If you are using an earlier shelf assembly, the alarm indicates that you are using a newer fan-tray assembly (15454-FTA3), which is incompatible with the earlier version of the shelf assembly. Obtain an earlier version of the fan-tray assembly (15454-FTA2) and complete the [“Replace the Fan-Tray Assembly” procedure on page 2-288](#).
- Step 4** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.
- 

## 2.7.281 MEA (PPM)

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

## 2.7.282 MEA (SHELF)

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

## 2.7.283 MEM-GONE

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

SONET Logical Object: EQPT

The Memory Gone alarm occurs when data generated by software operations exceeds the memory capacity of the TCC2/TCC2P. The TCC2/TCC2P cards which exceed the memory capacity reboot to avoid failure of card operations.



**Note**

The alarm does not require user intervention. The MEM-LOW alarm always precedes the MEM-GONE alarm.



**Note**

MEM-GONE alarm occurs on the ML-MR-10 card when the total available memory is less than 2MB and the largest chunk of memory available is 2MB.

## 2.7.284 MEM-LOW

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

SONET Logical Object: EQPT

The Free Memory of Card Almost Gone alarm occurs when data generated by software operations is close to exceeding the memory capacity of the TCC2/TCC2P. The alarm clears when additional memory becomes available. If additional memory is not made available and the memory capacity of the card is exceeded, CTC ceases to function.



**Note**

The ML-MR-10 card raises a MEM-LOW alarm (non service affecting) when the available free memory on the card goes below 15 percent of the total heap memory available.



**Note**

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

## 2.7.285 MFGMEM

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

SONET Logical Objects: AICI-AEP, AICI-AIE, AIP, BPLANE, FAN

DWDM Logical Object: PPM

The Manufacturing Data Memory Failure alarm occurs when the EEPROM fails on a card or component, or when the TCC2/TCC2P cannot read this memory. EEPROM stores manufacturing data that a system TCC2/TCC2P uses to determine system compatibility and shelf inventory status. Unavailability of this information can cause less-significant problems. The AIP EEPROM also stores the system MAC address. If the MFGMEM alarm indicates EEPROM failure on these panels, IP connectivity could be disrupted and the system icon is grayed out in CTC network view.

**Tip**

When you lose LAN connectivity with an ONS 15454 due to an MFGMEM alarm on the AIP, you can reestablish node management by disconnecting the Ethernet cable from the panel and connecting it to the active TCC2/TCC2P LAN port.

## Clear the MFGMEM Alarm

- 
- Step 1** Complete the [“Reset an Active TCC2/TCC2P Card and Activate the Standby Card” procedure on page 2-278](#).  
Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.
- Step 2** If the reset card has not rebooted successfully, or the alarm has not cleared, call Cisco TAC 1 800 553-2447. If the Cisco TAC technician tells you to reseat the card, complete the [“Remove and Reinsert \(Reseat\) the Standby TCC2/TCC2P Card” procedure on page 2-280](#). If the Cisco TAC technician tells you to remove the card and reinstall a new one, complete the [“Physically Replace a Traffic Card” procedure on page 2-281](#).
- Step 3** If the MFGMEM alarm continues to report after replacing the TCC2/TCC2Ps, the problem lies with the EEPROM.
- Step 4** If the MFGMEM is reported from the fan-tray assembly, obtain a fan-tray assembly and complete the [“Replace the Fan-Tray Assembly” procedure on page 2-288](#).
- Step 5** If the MFGMEM is reported from the AIP, the backplane, or the alarm persists after the fan-tray assembly is replaced, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 to report a Service-Affecting (SA) problem.
- 

## 2.7.286 MS-DEG

The MS-DEG condition is not used in this platform in this release. It is reserved for development.

## 2.7.287 MS-EXC

The MS-EXC condition is not used in this platform in this release. It is reserved for development.

## 2.7.288 MT-OCHNC

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

## 2.7.289 NO-CONFIG

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

SONET Logical Object: EQPT

The No Startup Configuration condition applies to ML-Series Ethernet cards and occurs when no startup configuration file has been downloaded to the TCC2/TCC2P, whether or not you preprovision the card slot. This alarm can be expected during provisioning. When the startup configuration file is copied to the active TCC2/TCC2P, the alarm clears.

**Note**

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

## Clear the NO-CONFIG Condition

- 
- Step 1** Create a startup configuration for the card in Cisco IOS.
- Follow the card provisioning instructions in the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.
- Step 2** Upload the configuration file to the TCC2/TCC2P:
- a. In node view, right-click the ML-Series card graphic.
  - b. Choose **IOS Startup Config** from the shortcut menu.
  - c. Click **Local > TCC** and navigate to the file location.
- Step 3** Complete the “[Reset a Traffic Card in CTC](#)” procedure on page 2-278.
- Step 4** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
- 

## 2.7.290 NON-CISCO-PPM

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

SONET Logical Object: PPM

The Non-Cisco PPM Inserted condition occurs when a PPM that is plugged into a card's port fails the security code check. The check fails when the PPM used is not a Cisco PPM.

## Clear the NON-CISCO-PPM Condition

- 
- Step 1** Obtain the correct Cisco PPM and replace the existing PPM with the new one.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
- 

## 2.7.291 NOT-AUTHENTICATED

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

SONET Logical Object: SYSTEM

The NOT-AUTHENTICATED alarm is raised by CTC (not by the NE) when CTC fails to log into a node. This alarm only appears in CTC where the login failure occurred. This alarm differs from the “INTRUSION-PSWD” alarm on page 2-135 because INTRUSION-PSWD occurs when a user exceeds the login failures threshold.

**Note**

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

## 2.7.292 OCHNC-INC

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

## 2.7.293 OCHTERM-INC

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

## 2.7.294 ODUK-1-AIS-PM

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

## 2.7.295 ODUK-2-AIS-PM

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

## 2.7.296 ODUK-3-AIS-PM

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

## 2.7.297 ODUK-4-AIS-PM

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

## 2.7.298 ODUK-AIS-PM

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

## 2.7.299 ODUK-BDI-PM

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

## 2.7.300 ODUK-LCK-PM

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

## 2.7.301 ODUK-OCI-PM

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

## 2.7.302 ODUK-SD-PM

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

## 2.7.303 ODUK-SF-PM

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

## 2.7.304 ODUK-TIM-PM

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

## 2.7.305 OOU-TPT

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

SONET Logical Objects: STSTRM, VT-TERM

The Out of Use Transport Failure alarm is a VCAT member alarm. (VCAT member circuits are independent circuits that are concatenated from different time slots into a higher-rate signal.) This condition is raised when a member circuit in a VCAT is unused, such as when it is removed by SW-LCAS. It occurs in conjunction with the [“VCG-DEG” condition on page 2-262](#).

### Clear the OOT-TPT Condition

- 
- Step 1** Complete the [“Clear the VCG-DEG Condition” procedure on page 2-262](#). Clearing that condition clears this condition as well.

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

## 2.7.306 OPEN-SLOT

Default Severity: Not Alarmed (NA)

Logical Object: EQPT

The Open Slot condition indicates that there is an open slot in the system shelf. Slot covers assist with airflow and cooling.

### Clear the OPEN-SLOT Condition

- Step 1** To install a slot cover and clear this condition, refer to the procedures located in the “Install Cards and Fiber-Optic Cable” chapter of the *Cisco ONS 15454 Procedure Guide*.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
- 

## 2.7.307 OPTNTWMIS

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

## 2.7.308 OPWR-HDEG

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

## 2.7.309 OPWR-HFAIL

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

## 2.7.310 OPWR-LDEG

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

## 2.7.311 OPWR-LFAIL

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

## 2.7.312 OSRION

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

## 2.7.313 OTUK-AIS

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

## 2.7.314 OTUK-BDI

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

## 2.7.315 OTUK-IAE

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

## 2.7.316 OTUK-LOF

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

## 2.7.317 OTUK-SD

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

## 2.7.318 OTUK-SF

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

## 2.7.319 OTUK-TIM

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

## 2.7.320 OUT-OF-SYNC

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

## 2.7.321 PARAM-MISM

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

## 2.7.322 PDI-P

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

SONET Logical Objects: STSMON, STSTRM

PDI-P is a set of application-specific codes indicating a signal label mismatch failure (SLMF) in the ONS 15454 STS path overhead. The condition indicates to downstream equipment that there is a defect in one or more of the directly mapped payloads contained in that STS synchronous payload envelope (SPE). For example, the mismatch could occur in the overhead to the path selector in a downstream node configured as part of a path protection. The PDI-P codes appear in the STS Signal Label (C2 byte).

An SLMF often occurs when the payload (for example, ATM) does not match what the signal label is reporting. The [“AIS” condition on page 2-38](#) often accompanies a PDI-P condition. If the PDI-P is the only condition reported with the AIS, clearing PDI-P clears the AIS. PDI-P can also occur during an upgrade, but usually clears itself and is not a valid condition.

A PDI-P condition reported on an OC-N port supporting a G1000-4 card circuit could result from the end-to-end Ethernet link integrity feature of the G1000-4 card. If the link integrity is the cause of the path defect, it is typically accompanied by the [“TPTFAIL \(G1000\)” alarm on page 2-254](#) or the [“CARLOSS \(G1000\)” alarm on page 2-64](#) reported against one or both Ethernet ports terminating the circuit. If this is the case, clear the TPTFAIL and CARLOSS alarms to resolve the PDI-P condition.

A PDI-P condition reported on an OC-N port supporting an ML-Series card circuit could result from the end-to-end Ethernet link integrity feature of the ML-Series card. If the link integrity is the cause, it is typically accompanied by the [“TPTFAIL \(ML100T, ML1000, MLFX\)” alarm on page 2-255](#) reported against one or both POS ports terminating the circuit. If TPTFAIL is reported against one or both of the POS ports, troubleshooting the accompanying alarm clears the PDI-P condition. Refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454*, *Cisco ONS 15454 SDH*, and *Cisco ONS 15327* for more information about ML-Series cards.



### Warning

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

**Warning**

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

**Warning**

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

**Note**

For more information about Ethernet cards, refer to the Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.

## Clear the PDI-P Condition

- Step 1** Verify that all circuits terminating in the reporting card are DISCOVERED:
- Click the **Circuits** tab.
  - Verify that the **Status** column lists the circuit as active.
  - If the Status column lists the circuit as PARTIAL, wait 10 minutes for the ONS 15454 to initialize fully. If the PARTIAL status does not change after full initialization, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC to report a Service-Affecting (SA) problem 1 800 553-2447.

- Step 2** After determining that the circuit is DISCOVERED, ensure that the signal source to the card reporting the alarm is working.

**Caution**

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

- Step 3** If traffic is affected, complete the [“Delete a Circuit” procedure on page 2-283](#).

**Caution**

Deleting a circuit can affect existing traffic.

- Step 4** Recreate the circuit with the correct circuit size. Refer to the “Create Circuits and VT Tunnels” chapter in the *Cisco ONS 15454 Procedure Guide* for detailed procedures to create circuits.
- Step 5** If circuit deletion and re-creation does not clear the condition, verify that there is no problem stemming from the far-end OC-N card providing STS payload to the reporting card.
- Step 6** If the condition does not clear, confirm the cross-connect between the OC-N card and the reporting card.
- Step 7** If the condition does not clear, clean the far-end optical fiber according to site practice. If no site practice exists, complete the procedure in the “Maintain the Node” chapter of the *Cisco ONS 15454 Procedure Guide*.
- Step 8** If the condition does not clear, complete the [“Physically Replace a Traffic Card” procedure on page 2-281](#) for the optical/electrical cards.

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

## 2.7.323 PEER-NORESPONSE

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

SONET Logical Object: MLMR

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

However, for ML-MR-10 cards, a peer card not responding alarm is raised if a CPP card that is active does not receive any heartbeat response from its peer card. This happens under the following conditions:

- Peer card is not present in the ONS 15454 chassis
- Peer card is not configured for protection
- Protection is disabled on the peer card
- Peer card has reset.

### Clear the PEER-NORESPONSE Alarm

- 
- Step 1** Complete the “[Reset a Traffic Card in CTC](#)” procedure on page 2-278 for the reporting card. For the LED behavior, see the “[2.8.2 Typical Traffic Card LED Activity During Reset](#)” section on page 2-267.
- Step 2** Verify that the reset is complete and error-free and that no new related alarms appear in CTC. Verify the LED appearance: A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
- Step 3** For ML-MR-10 card, ensure that the CPP peer card has not failed, the correct protection configuration is present on both CPP cards, and protection is not disabled on the CPP peer card.
- Step 4** If the alarm does not clear, log into the Cisco Technical Support Website at <http://www.cisco.com/techsupport> for more information or log into <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml> to obtain a directory of toll-free Technical Support numbers for your country.
- 

## 2.7.324 PLM-P

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

SONET Logical Objects: STSMON, STSTRM

A Payload Label Mismatch Path alarm indicates that signal does not match its label. The condition is indicated by a problematic C2 byte value in the SONET path overhead. The alarm is raised if all of the following conditions are met:

- The received C2 byte is not 0x00 (unequipped).

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

For example, on nodes equipped with CTC Software R4.1 and earlier, this alarm could occur when you have a DS3XM-6 card connected to a DS-3 card instead of a DS-1 card. The DS3XM-6 card expects a C2 label byte value of 01. A DS-1 card transmits this value, but a DS-3 card transmits a value of 04. The mismatch between the sent and expected values causes the PLM-P alarm.

**Warning**

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

**Warning**

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

**Warning**

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

## Clear the PLM-P Alarm

**Step 1**

Complete the [“Clear the PDI-P Condition” procedure on page 2-199](#).

**Caution**

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

**Step 2**

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

## 2.7.325 PLM-V

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

SONET Logical Object: VT-TERM, VT-MON

A Payload Label Mismatch VT Layer alarm indicates that the content of the V5 byte in the SONET overhead is inconsistent or invalid. PLM-V occurs when ONS 15454s interoperate with equipment that performs bit-synchronous mapping for DS-1 signal. The ONS 15454 uses asynchronous mapping.

## Clear the PLM-V Alarm

- 
- |               |                                                                                                                                                                                                                                                                   |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | 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.                                                                                                                   |
| <b>Step 2</b> | 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.                                                                |
| <b>Step 3</b> | If the alarm does not clear, log into the Technical Support Website at <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem. |
- 

## 2.7.326 PMI

For more information about the PMI condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*.

## 2.7.327 PORT-FAIL

For more information about the PORT-FAIL alarm, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*.

## 2.7.328 PORT-MISMATCH

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

SONET Logical Objects: CE-MR-10, ML-MR-10, FC\_MR-4

The Pluggable PORT-MISMATCH alarm applies to FC\_MR-4, ML-MR-10, and CE-MR-10 Ethernet cards.

For the ML-MR-10 and CE-MR-10 cards the alarm indicates either of the following:

- The provisioned payload, speed, or duplex configured on the port does not match that of the SFP plugged into the port.
- A non-supported SFP is plugged into the port.

For the FC\_MR-4 card the alarm indicates that a non-supported GBIC is plugged into the port.

## Clear the PORT-MISMATCH Alarm

To clear the alarm on the CE-MR-10 card, either plug-in a supported SFP into the CE-MR-10 port or follow these steps to provision the correct payload, speed, or duplex:

1. In node view (single-shelf mode) or shelf view (multishelf mode), double-click the CE-MR-10 card to open the card view.
2. Click the **Provisioning > Ether Ports** tabs.
3. Specify correct values in the Expected Speed and Expected Duplex fields to match the SFP configuration.

**4. Click **Apply**.**

To clear the alarm on the FC\_MR-4 card, plug-in a supported GBIC into the FC\_MR-4 port and follow these steps to provision the media type:

1. In node view (single-shelf mode) or shelf view (multishelf mode), double-click the FC\_MR-4 card graphic to open the card.
2. Click the **Provisioning > Port > General** tabs.
3. Specify proper payload value in the Media Type field.
4. Click **Apply**.

For the CE-MR-10 and FC\_MR-10 card, the alarm can also be cleared using TL1 commands. For detailed instructions, refer to the *Cisco ONS 15454*, *Cisco ONS 15600*, and *Cisco ONS 15310-MA SONET TL1 Command Guide*.

For the ML-MR-10 card, the alarm can be cleared through Cisco IOS commands. For detailed instructions, refer to the *Cisco ONS 15454* and *Cisco ONS 15454 SDH Ethernet Card Software Feature and Configuration Guide*.

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

## 2.7.329 PRC-DUPID

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

SONET Logical Object: OCN

The Procedural Error Duplicate Node ID alarm indicates that two identical node IDs exist in the same ring. The ONS 15454 requires each node in the ring to have a unique node ID.

### Clear the PRC-DUPID Alarm

- 
- |               |                                                                                                                                                                                                                                                                   |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Log into a node on the ring.                                                                                                                                                                                                                                      |
| <b>Step 2</b> | Find the node ID by completing the “ <a href="#">Identify a BLSR Ring Name or Node ID Number</a> ” procedure on <a href="#">page 2-268</a> .                                                                                                                      |
| <b>Step 3</b> | Repeat <a href="#">Step 2</a> for all the nodes on the ring.                                                                                                                                                                                                      |
| <b>Step 4</b> | If two nodes have an identical node ID number, complete the “ <a href="#">Change a BLSR Node ID Number</a> ” procedure on <a href="#">page 2-269</a> so that each node ID is unique.                                                                              |
| <b>Step 5</b> | If the alarm does not clear, log into the Technical Support Website at <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem. |
- 

## 2.7.330 PROTNA

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

SONET Logical Object: EQPT

The Protection Unit Not Available alarm is caused by an OOS protection card when a TCC2/TCC2P or XC10G card that has been provisioned as part of a protection group is not available. Unavailable protection can occur when a card is reset, but the alarm clears as soon as the card is back in service. The alarm clears if the device or facility is brought back in service.

## Clear the PROTNA Alarm

- 
- |               |                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | If the PROTNA alarm occurs and does not clear, and if it is raised against a controller or cross-connect card, ensure that there is a redundant TCC2/TCC2P installed and provisioned in the chassis.                                                                                                                                                                                                                                                       |
| <b>Step 2</b> | <p>If the alarm is raised against a line card, verify that the ports have been taken out of service (OOS,MT):</p> <ol style="list-style-type: none"> <li>a. In CTC, double-click the reporting card to open the card view (if the card is not an XC10G card).</li> <li>b. Click the <b>Provisioning</b> tab.</li> <li>c. Click the admin state of any in-service (IS) ports.</li> <li>d. Choose <b>OOS,MT</b> to take the ports out of service.</li> </ol> |
| <b>Step 3</b> | Complete the <a href="#">“Reset a Traffic Card in CTC” procedure on page 2-278</a> for the reporting card. For the LED behavior, see the <a href="#">“2.8.2 Typical Traffic Card LED Activity During Reset” section on page 2-267</a> .                                                                                                                                                                                                                    |
| <b>Step 4</b> | Verify that the reset is complete and error-free and that no new related alarms appear in CTC. Verify the LED appearance: A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.                                                                                                                                                                                                                                     |
| <b>Step 5</b> | If the alarm does not clear, complete the <a href="#">“Remove and Reinsert (Reseat) Any Card” procedure on page 2-280</a> for the reporting card.                                                                                                                                                                                                                                                                                                          |
| <b>Step 6</b> | If the alarm does not clear, log into the Technical Support Website at <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> for more information or call Cisco TAC 1 800 553-2447.                                                                                                                                                                                                                                              |
- 

## 2.7.331 PROV-MISMATCH

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

## 2.7.332 PTIM

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

## 2.7.333 PWR-FAIL-A

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

SONETLogical Object: EQPT

The Equipment Power Failure at Connector A alarm occurs when there is no power supply from the main power connector to the equipment. This alarm occurs on the electrical interface assemblies (EIA), 15454\_MRC-12 Multirate card, MRC-2.5G-4 Multirate card, OC192SR1/STM64IO Short Reach and OC192/STM64 Any Reach cards (also known as OC192-XFP in CTC), OC12 IR/STM4 SH 1310-4 card, OC3 IR/STM1 SH 1310-8 card or TCC2/TCC2P.

**Warning**

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

## Clear the PWR-FAIL-A Alarm

- Step 1** If a single card has reported the alarm, take the following actions depending on the reporting card:
- If the reporting card is an active traffic line port in a 1+1 protection group or part of a path protection, ensure that an APS traffic switch has occurred to move traffic to the protect port.
-  **Note** Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the [“2.9.2 Protection Switching, Lock Initiation, and Clearing”](#) section on page 2-269 for commonly used traffic-switching procedures.
- If the alarm is reported against a TCC2/TCC2P, complete the [“Reset an Active TCC2/TCC2P Card and Activate the Standby Card”](#) procedure on page 2-278.
  - If the alarm is reported against an OC-N card, complete the [“Reset a Traffic Card in CTC”](#) procedure on page 2-278.
  - If the alarm is reported against a cross-connect card, complete the [“Reset a Traffic Card in CTC”](#) procedure on page 2-278 for the cross-connect card. (The process is similar.)
- Step 2** If the alarm does not clear, complete the [“Remove and Reinsert \(Reseat\) Any Card”](#) procedure on page 2-280.
- Step 3** If the alarm does not clear, complete the [“Physically Replace a Traffic Card”](#) procedure on page 2-281 for the reporting card.
- Step 4** If the single card replacement does not clear the alarm, or if multiple cards report the alarm, verify the office power. Refer to the [“Install the Shelf and Backplane Cable”](#) chapter in the *Cisco ONS 15454 Procedure Guide* for procedures. See the [“1.13 Power Supply Problems”](#) section on page 1-149 as necessary.
- Step 5** If the alarm does not clear, reseal the power cable connection to the connector.
- Step 6** If the alarm does not clear, physically replace the power cable connection to the connector.
- Step 7** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

## 2.7.334 PWR-FAIL-B

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

SONET Logical Object: EQPT

The Equipment Power Failure at Connector B alarm occurs when there is no power supply from the main power connector to the equipment. This alarm occurs on the electrical interface assemblies (EIA), 15454\_MRC-12 Multirate card, MRC-2.5G-4 Multirate card, OC192SR1/STM64IO Short Reach and OC192/STM64 Any Reach cards (also known as OC192-XFP in CTC), OC12 IR/STM4 SH 1310-4 card, OC3 IR/STM1 SH 1310-8 card or TCC2/TCC2P.



### Warning

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

### Clear the PWR-FAIL-B Alarm

- 
- Step 1** Complete the [“Clear the PWR-FAIL-A Alarm” procedure on page 2-205](#).
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
- 

## 2.7.335 PWR-FAIL-RET-A

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

SONET Logical Object: EQPT

The Equipment Power Failure at Connector A alarm occurs when there is no power supplied to the backup power connector on the shelf. This alarm occurs on the electrical interface assemblies (EIA), 15454\_MRC-12 Multirate card, MRC-2.5G-4 Multirate card, OC192SR1/STM64IO Short Reach and OC192/STM64 Any Reach cards (also known as OC192-XFP in CTC), OC12 IR/STM4 SH 1310-4 card, OC3 IR/STM1 SH 1310-8 card or TCC2/TCC2P.

### Clear the PWR-FAIL-RET-A Alarm

- 
- Step 1** Complete the [“Clear the PWR-FAIL-A Alarm” procedure on page 2-205](#).
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
- 

## 2.7.336 PWR-FAIL-RET-B

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

SONET Logical Object: EQPT

The Equipment Power Failure at Connector B alarm occurs when there is no power supplied to the backup power connector on the shelf. This alarm occurs on the electrical interface assemblies (EIA), 15454\_MRC-12 Multirate card, MRC-2.5G-4 Multirate card, OC192SR1/STM64IO Short Reach and OC192/STM64 Any Reach cards (also known as OC192-XFP in CTC), OC12 IR/STM4 SH 1310-4 card, OC3 IR/STM1 SH 1310-8 card or TCC2/TCC2P.

## Clear the PWR-FAIL-RET-A Alarm

- 
- Step 1** Complete the “[Clear the PWR-FAIL-A Alarm](#)” procedure on page 2-205.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
- 

## 2.7.337 PWR-PROT-ON

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

SONET Logical Objects: OTS

The Raman Power Protection On alarm occurs only on the OPT-RAMP-C card when the Raman amplifier is used on fiber span that is too short for Raman power.

## Clear the PWR-PROT-ON Alarm

- 
- Step 1** To clear the alarm, check if the Raman amplifier is connected to the wrong span. If it is, check patch cords setup and fix it.
- Step 2** Alternatively, review the network configuration to see Raman amplifier has been wrongly used. If is, remove it.
- Step 3** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
- 

## 2.7.338 RAI

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

SONET Logical Objects: DS1, DS3, E1

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

## Clear the RAI Condition

- 
- Step 1** Complete the “[Clear the AIS Condition](#)” procedure on page 2-38.
-

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

## 2.7.339 RAMAN-SPAN-NOT-TUNED

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

SONET Logical Objects: OTS

The RAMAN-SPAN-NOT-TUNED condition indicates that the Raman span has not been tuned.

### Clear the RAMAN-SPAN-NOT-TUNED Condition

- Step 1** The condition clears when the span has been tuned through the previous procedure.
- Step 2** If the condition does not clear, log into the Cisco Technical Support Website at <http://www.cisco.com/techsupport> for more information or log into <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml> to obtain a directory of toll-free Technical Support numbers for your country.

## 2.7.340 RCVR-MISS

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

SONET Logical Objects: DS1, E1

A Facility Termination Equipment Receiver Missing alarm occurs when the facility termination equipment detects an incorrect amount of impedance on its backplane connector. Incorrect impedance usually occurs when a receive cable is missing from a DS-1 port, or a possible mismatch of backplane equipment occurs. For example, an SMB connector or a BNC connector could be misconnected to a DS-1 card.



#### Note

DS-1s are four-wire circuits and need a positive (tip) and negative (ring) connection for both transmit and receive.

### Clear the RCVR-MISS Alarm

- Step 1** Ensure that the device attached to the DS-1 port is operational.



#### Caution

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

- Step 2** If the attachment is good, verify that the cabling is securely connected.
- Step 3** If the cabling is good, verify that the pinouts are correct.

- Step 4** If the pinouts are correct, replace the receive cable.
- Step 5** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a service-affecting (SA) problem.
- 

## 2.7.341 RSV-RT-EXCD-RINGLETO

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

SONET Logical Object: RPRIF

The Reserved Bandwidth Exceeds Link Rate on Ringlet Zero alarm is raised by an ML-1000 card if the sum of reserved bandwidth configured on each station of ringlet 0 is greater than the link rate (circuit bandwidth). The alarm clears when the sum of the reserved bandwidth on each station falls below the link rate. In the case of SW-LCAS or LCAS circuits, the link rate is the working link rate, which will change when members are removed.

RSV-RT-EXCD-RINGLETO does not suppress any alarms, but it is suppressed by the [“RPR-PASSTHR” alarm on page 2-215](#).

### Clear the RSV-RT-EXCD-RINGLETO Alarm

- Step 1** At the CLI command prompt in privileged executive mode, enter the following command:
- ```
router# show rpr-ieee topology detail
```
- This command's output shows the configured reserved bandwidth rate from each station.
- Step 2** Reduce the reserved bandwidth on the alarmed station until the error clears. Enter the following CLI command in IEEE 802.17b-based RPR interface configuration mode:
- ```
router (config-if)# rpr-ieee tx-traffic rate-limit reserved
```
- Step 3** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a service-affecting (SA) problem.
- 

## 2.7.342 RSV-RT-EXCD-RINGLET1

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

SONET Logical Object: RPRIF

The Reserved Bandwidth Exceeds Link Rate on Ringlet One alarm is raised by an ML-1000 card if the sum of reserved bandwidth configured on each station of ringlet 1 is greater than the link rate (circuit bandwidth). The alarm clears when the sum of the reserved bandwidth on each station falls below the link rate. In the case of SW-LCAS or LCAS circuits, the link rate is the working link rate, which will change when members are removed.

RSV-RT-EXCD-RINGLET1 does not suppress any alarms, but it is suppressed by the [“RPR-PASSTHR” alarm on page 2-215](#).

## Clear the RSV-RT-EXCD-RINGLET1 Alarm

- 
- Step 1** At the CLI command prompt in privileged executive mode, enter the following command:
- ```
router# show rpr-ieee topology detail
```
- This command's output shows the configured reserved bandwidth rate from each station.
- Step 2** Reduce the reserved bandwidth on the alarmed station until the error clears. Enter the following CLI command in IEEE 802.17b-based RPR interface configuration mode:
- ```
router (config-if)# rpr-ieee tx-traffic rate-limit reserved
```
- Step 3** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a service-affecting (SA) problem.
- 

## 2.7.343 RFI

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

## 2.7.344 RFI-L

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

SONET Logical Objects: EC1, OCN

DWDM Logical Object: TRUNK

A RFI Line condition occurs when the ONS 15454 detects an RFI in OC-N card SONET overhead because of a fault in another node. Resolving the fault in the adjoining node clears the RFI-L condition in the reporting node. RFI-L indicates that the condition is occurring at the line level.

## Clear the RFI-L Condition

- 
- Step 1** Log into the node at the far-end node of the reporting ONS 15454.
- Step 2** Identify and clear any alarms, particularly the “[LOS \(OCN\)](#)” alarm on [page 2-168](#).
- Step 3** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
- 

## 2.7.345 RFI-P

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

SONET Logical Objects: STSMON, STSTRM

The RFI Path condition occurs when the ONS 15454 detects an RFI in the an STS-1 signal SONET overhead because of a fault in another node. Resolving the fault in the adjoining node clears the RFI-P condition in the reporting node. RFI-P occurs in the terminating node in that path segment.

## Clear the RFI-P Condition

- Step 1** Verify that the ports are enabled and in service (IS-NR) on the reporting ONS 15454:
- Confirm that the LED is correctly illuminated on the physical card.  
A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
  - To determine whether the OC-N port is in service, double-click the card in CTC to open the card view.
  - Click the **Provisioning > Line** tabs.
  - Verify that the Admin State column lists the port as IS.
  - If the Admin State column lists the port as OOS,MT or OOS,DSBLD, click the column and choose **IS**. Click **Apply**.



**Note** If ports managed into IS admin state are not receiving signals, the LOS alarm is either raised or remains, and the port service state transitions to OOS-AU,FLT.

- Step 2** To find the path and node failure, verify the integrity of the SONET STS circuit path at each of the intermediate SONET nodes.
- Step 3** Clear alarms in the node with the failure, especially the “[UNEQ-P](#)” alarm on page 2-258 or the “[UNEQ-V](#)” alarm on page 2-260.
- Step 4** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

## 2.7.346 RFI-V

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

SONET Logical Objects: VTMON, VT-TERM

An RFI VT Layer condition occurs when the ONS 15454 detects an RFI in the SONET overhead because of a fault in another node. Resolving the fault in the adjoining node clears the RFI-V condition in the reporting node. RFI-V indicates that an upstream failure has occurred at the VT layer.

## Clear the RFI-V Condition

- Step 1** Verify that the connectors are securely fastened and connected to the correct slot. For more information, refer to the “Install Cards and Fiber-Optic Cable” chapter in the *Cisco ONS 15454 Procedure Guide*.



### Caution

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

- Step 2** If connectors are correctly connected, verify that the DS-N
- Step 3** port is active and in service (IS-NR):
- Confirm that the LED is correctly illuminated on the physical card. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
  - To determine whether the OC-N port is in service, double-click the card in CTC to open the card view.
  - Click the **Provisioning > Line** tabs.
  - Verify that the Admin State column lists the port as IS. If the Admin State column lists the port as OOS,MT or OOS,DSBLD, click the column and choose **IS**. Click **Apply**.
-  **Note** If ports managed into IS admin state are not receiving signals, the LOS alarm is either raised or remains, and the port service state transitions to OOS-AU,FLT.
- Step 4** If the ports are active and in service, use an optical test set to verify that the signal source does not have errors. For specific procedures to use the test set equipment, consult the manufacturer.
- Step 5** If the signal is valid, log into the node at the far-end of the reporting ONS 15454.
- Step 6** Clear alarms in the far-end node, especially the “[UNEQ-P](#)” alarm on page 2-258 or the “[UNEQ-V](#)” alarm on page 2-260.
- Step 7** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

## 2.7.347 RING-ID-MIS

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

SONET Logical Object: OCN

DWDM Logical Object: OSC-RING

The Ring ID Mismatch condition refers to the ring ID in APC. It occurs when a ring name does not match other detectable node ring names, and can cause problems with applications that require data exchange with APC. This alarm is similar to the “[RING-MISMATCH](#)” alarm on page 2-213, but rather than apply to BLSDR ring protection, RING-ID-MIS applies to DWDM node discovery within the same network.



**Note**

For more information about APC, refer to the *Cisco ONS 15454 DWDM Procedure Guide*.

### Clear the RING-ID-MIS Alarm

- Step 1** Complete the “[Clear the RING-MISMATCH Alarm](#)” procedure on page 2-213.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

## 2.7.348 RING-MISMATCH

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

SONET Logical Object: OCN

A Procedural Error Mismatch Ring alarm occurs when the ring name of the ONS 15454 node that is reporting the alarm does not match the ring name of another node in the BLSR. Nodes connected in a BLSR must have identical ring names to function. This alarm can occur during BLSR provisioning.

RING-MISMATCH is somewhat similar to RING-ID-MIS, but it applies to BLSR protection discovery instead of DWDM node discovery.



**Note**

For more information about DWDM cards, refer to the *Cisco ONS 15454 DWDM Reference Manual*.

### Clear the RING-MISMATCH Alarm

- Step 1** In node view, click the **Provisioning > BLSR** tabs.
- Step 2** Note the name in the Ring Name field.
- Step 3** Log into the next ONS 15454 node in the BLSR.
- Step 4** Complete the [“Identify a BLSR Ring Name or Node ID Number” procedure on page 2-268](#).
- Step 5** If the ring name matches the ring name in the reporting node, repeat [Step 4](#) for the next ONS 15454 in the BLSR.
- Step 6** Complete the [“Change a BLSR Ring Name” procedure on page 2-268](#).
- Step 7** Verify that the ring map is correct.
- Step 8** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.

## 2.7.349 RING-SW-EAST

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

SONET Logical Object: OCN

The Ring Switch Is Active East Side condition occurs when a ring switch occurs at the east side of a BLSR using a Force Ring command. The condition clears when the switch is cleared. RING-SW-EAST is visible on the network view Alarms, Conditions, and History tabs. The port where the Force Ring was applied shows an “F” on the network view detailed circuit map.



**Note**

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

## 2.7.350 RING-SW-WEST

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

SONET Logical Object: OCN

The Ring Switch Is Active West Side condition occurs when a ring switch occurs at the west side of a BLSR using a Force Ring command. The condition clears when the switch is cleared. RING-SW-WEST is visible on the network view Alarms, Conditions, and History tabs. The port where the Force Ring was applied shows an “F” on the network view detailed circuit map.



**Note**

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

## 2.7.351 RLS

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

SONET Logical Objects: OTS

The Raman Laser Shutdown (RLS) alarm indicates that the Raman laser has shutdown.

Reflection causes the Tx light of the Raman amplifier to be reflected back to the light source. Because the power of the light source is high it can cause damage to the port. To prevent damage to the port, the laser shuts down. This alarm can be raised when the Raman pumps are turned on or when the first circuit is activated.

### Clear the RLS Condition

- 
- Step 1** Replace the cable connecting the transmitting device to the port or clean the optical connectors. To do this, refer to the "Install Hardware" chapter in the *Cisco ONS 15454 SDH Procedure Guide*.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
- 

## 2.7.352 ROLL

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

SONET Logical Objects: STSMON, STSTRM, VT-TERM, VT-MON

The ROLL condition indicates that circuits are being rolled. This is typically carried out to move traffic for a maintenance operation or to perform bandwidth grooming. The condition indicates that a good signal has been received on the roll destination leg, but the roll origination leg has not yet been dropped. The condition clears when the roll origination leg is dropped.



**Note**

ROLL is an informational condition and does not require troubleshooting.

## 2.7.353 ROLL-PEND

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

SONET Logical Objects: STSMON, STSTRM, VT-TERM, VT-MON

ROLL-PEND indicates that a roll process has been started, but a good signal has not been received yet by the roll destination leg. This condition can be raised individually by each path in a bulk circuit roll. The condition clears when a good signal has been received on the roll destination leg.

**Note**

ROLL-PEND is an informational condition and does not require troubleshooting.

## 2.7.354 ROUTE-OVERFLOW

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

SONET Logical Objects: NE

DWDM Logical Object: NE regardless of MSTP or MSPP

The ROUTE-OVERFLOW indicates the condition when the OSPF routing table exceeds 700 routes. The symptoms for this condition are loss of visibility to a node or network, inability to access a node using CTC, CTM, Telnet, Ping, and so on.

### Clear the ROUTE-OVERFLOW Condition

**Step 1** Reconfigure the OSPF network to less than 700 routes.

## 2.7.355 RPR-PASSTHR

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

SONET Logical Object: RPRIF

The IEEE 802.17 b-based RPR Interface in Pass-Through Mode condition indicates that an ML card's IEEE 802.17 b-based RPR interface is not participating in a ring. Instead, the card is behaving like a passive device that allows the signal to transit but does not manipulate it. Pass-through mode itself is hitless.

You can manually place an ML card into (or out of) pass-through mode using the Cisco IOS CLI command SHUTDOWN (SHUT) for such reasons as adding, removing, or servicing the node. To do so is hitless.

The ML-1000 automatically enters pass-through mode if either of the following conditions is true:

- Redundant interconnect (RI) is configured and the ML card is in primary mode (that is, single traffic queue mode), standby state.
- RI is configured and the RI interface goes down during a “WTR” alarm on page 2-266, while the ML card is in secondary mode (that is, dual traffic queue mode) on a Cisco proprietary RPR ring.

**Note**

For GFP and HDLC mode, the ML card shutdown (SHUT) command causes an “AIS-P” alarm on page 2-39 to be sent to the peer. But in IEEE 802.17b-based RPR mode, AIS-P is not inserted toward the peer.

The RPR-PASSTHR condition suppresses the following alarms:

- [FORCED-REQ](#), page 115
- [LINK-KEEPALIVE](#), page 145
- [MAN-REQ](#), page 183
- [MAX-STATIONS](#), page 185
- [RSV-RT-EXCD-RINGLET0](#), page 209
- [RSV-RT-EXCD-RINGLET1](#), page 209
- [RPR-PROT-ACTIVE](#), page 218
- [RPR-PROT-CONFIG-MISM](#), page 218
- [RPR-SD](#), page 219
- [RPR-SF](#), page 220
- [RPR-SPAN-MISMATCH](#), page 221
- [WTR](#), page 266

If RPR-PASSTHR is raised—meaning that this RPR-IEEE interface is not available—one or more of its peer nodes might raise the “[RPR-PEER-MISS](#)” alarm on page 2-216. RPR-PASSTHR does not suppress the “[RPR-PEER-MISS](#)” alarm on page 2-216, or the “[RPR-RI-FAIL](#)” alarm on page 2-219.

## Clear the RPR-PASSTHR Condition

- 
- Step 1** If the ML card was manually configured shut down using the CLI command SHUTDOWN (SHUT), enter the following command at the command prompt:
- ```
router# no shut
```
- Step 2** If the card is in pass-through mode due to being in an RI primary mode standby state, either the IEEE 802.17b-based RPR interface is down or the interconnect interface is down. You must clear the root cause of either problem to clear the pass-through. To trace the root cause problem in the RPR-IEEE interface setup, enter the following CLI command in privileged executive mode:
- ```
router# show interface rpr-ieee 0
```
- Step 3** View the command output and locate the RI information line. It displays the name of the monitored interfaces as “monitoring ring interface,” or “monitoring interconnect interface.”
- Step 4** Locate and clear any trouble on the monitored interface. Trouble might be indicated on that interface through previous alarms that occurred before RPR-PASSTHR was raised.
- Step 5** If the card is in pass-through mode while in RI secondary mode when the interconnect fails, pass-through mode should clear automatically in 60 seconds.
- Step 6** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
- 

## 2.7.356 RPR-PEER-MISS

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

SONET Logical Object: RPRIF

The IEEE 802.17-based RPR Peer Node Is Missing condition is raised by an ML card when RI is configured on the card, but this station does not detect its peer station in the topology. The condition clears when the peers detect each other.

## Clear the RPR-PEER-MISS Condition

**Step 1** Determine whether the peer MAC address is properly configured by completing the following steps:

- a. Enter the following CLI command in privileged executive mode:

```
router# show interface rpr-ieee 0
```

This command's output will include information, similar to the following, about the RPR-IEEE interface raising the condition:

```
Hardware is RPR-IEEE Channelized SONET, address is 000e.8312.bcf0 (bia
000e.87312.bfc0)
```

- b. Verify that the alarmed interface's configured peer MAC address is the correct MAC address for the peer card. A card in primary mode need to list the peer MAC address of the card operating in secondary mode; the secondary card needs to list the peer MAC address of the primary card. Peer MAC address information is contained in the same "show interface rpr-ieee 0" command output. In the following line example, the RPR-IEEE interface raising the alarm is primary; it is in active mode, and its configured peer, the secondary card, is MAC address 000e.8312.b870:

```
RI: primary,active peer mac 000e.8312.b870
```



**Note** The primary and secondary cards do not have to be neighbors on the ring.



**Note** If RI is configured, then RI information is displayed in the "show interface rpr 0" output.

To correct the MAC address configuration, refer to the *Cisco ONS 15454 and Cisco ONS 15454 SDH Ethernet Card Software Feature and Configuration Guide* for procedures.

**Step 2** If the condition does not clear, enter the following command in privileged executive mode:

```
router# show rpr-ieee protection
```

**Step 3** The command output, similar to the following lines, shows whether any protection switches are active:

```
West Span Failures: none
East Span Failures: none
```

A protection switch can cause an RPR-PEER-MISS condition. You may also see the ["RPR-PROT-ACTIVE" alarm on page 2-218](#) raised for a span. Clear any protection issues.

**Step 4** If the condition does not clear, correct any issues on the peer node that would cause it to go into pass-through mode, which can cause the peer to raise RPR-PEER-MISS.

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

## 2.7.357 RPR-PROT-ACTIVE

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

SONET Logical Object: RPRIF

The IEEE 802.17b-based RPR Protection is Active condition, raised by the ML card, indicates that ring protection is active and that steering protection as defined in IEEE 802.17b is active.

IEEE 802.17b-based RPR provides hitless protection switching for all protected traffic on a ring. Its steering protection mechanism ensures that each station receives span change information (such as fail or restoration) in time to make protection switching decisions within the 50-millisecond time frame.

The condition clears when steering protection is no longer active. For more information about steering, refer to the *Cisco ONS 15454 and Cisco ONS 15454 SDH Ethernet Card Software Feature and Configuration Guide*.

This condition is suppressed by the “RPR-PASSTHR” alarm on page 2-215.

### Clear the RPR-PROT-ACTIVE Condition

- 
- |               |                                                                                                                                                                                                                   |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Locate and clear any service-affecting SONET error that might have caused a protection switch, in turn triggering the RPR-PROT-ACTIVE condition. Clearing the SONET condition will clear RPR-PROT-ACTIVE.         |
| <b>Step 2</b> | If the condition does not clear, log into the Technical Support Website at <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> for more information or call Cisco TAC 1 800 553-2447. |
- 

## 2.7.358 RPR-PROT-CONFIG-MISM

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

SONET Logical Object: RPRIF

The IEEE 802.17b-based RPR Protection Configuration Mismatched alarm is raised by an ML card when it detects that its steering protection scheme is mismatched with other vendors' equipment configured for wrapping protection. The ONS 15454 does not support IEEE 802.17b's optional wrapping scheme.

The alarm clears when the other vendor's equipment configuration is changed to utilize steering protection.

RPR-PROT-CONFIG-MISM is suppressed by the “RPR-PASSTHR” alarm on page 2-215.

### Clear the RPR-PROT-CONFIG-MISM Alarm

- 
- |               |                                                                                                                                                                                                                                                                                       |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | You cannot clear this alarm from the ONS 15454; rather, it is caused by incompatible vendor equipment configuration. See that equipment's support information to correct the configuration for steering instead of wrapping. This, in turn, will cause RPR-PROT-CONFIG-MISM to clear. |
| <b>Step 2</b> | If the alarm does not clear, log into the Technical Support Website at <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> for more information or call Cisco TAC (1 800 553-2447) to report a Service-Affecting (SA) problem.                            |
-

## 2.7.359 RPR-RI-FAIL

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

SONET Logical Object: RPRIF

The IEEE 802.17b-based RPR RI Fail condition is raised by an ML card in primary or secondary mode. If a card is in primary mode, a Gigabit Ethernet interface can cause an interconnect interface (IC) failure. (The IC includes the Gigabit Ethernet interface and possibly a port channel interface.) In primary mode, RPR-RI-FAIL can also be raised in response to a downed ring interface. In secondary mode, the only possible cause of this condition is IC failure.

The alarm clears when the IEEE 802.17b-based RPR interface returns to Init modes and faults, if present, are cleared. RPR-RI-FAIL is suppressed by the “RPR-PASSTHR” alarm on page 2-215.

### Clear the RPR-RI-FAIL Condition

- 
- Step 1** If the card is in primary mode, enter the following command at the CLI in privileged executive mode:
- ```
router# show interface rpr-ieee 0
```
- Step 2** The RI information line displays the name of the monitored interfaces and says either “monitoring ring interface,” or “monitoring interconnect interface.”
- Step 3** Determine why the monitored interface is down. It can occur because the ring interface has been shut down using the “shutdown” CLI command, or because both SONET circuits are down or OOS.
- Step 4** If correcting the previous problem on a primary interface does not clear the condition, or if the condition is raised on a card in secondary mode, the IC failure root cause must be corrected. This can be due to a fiber pull, having link protocol down, or shut down interfaces.
- Link state is indicated in the “show interface rpr-ieee 0” output on the following line:
RPR-IEEE0 is up, line protocol is up
 - A shutdown is indicated if a node is in pass-through mode. The same command output indicates whether or not this is the case:
MAC passthrough not set
- Step 5** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.360 RPR-SD

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

SONET Logical Objects: ML100T, ML1000, MLFX

The IEEE 802.17b-based RPR Signal Degrade condition indicates that a minor signal degradation has occurred on an IEEE- RPR ring that, if not overridden, can deactivate the link. The RPR-SD condition is reported if the SONET “SD-P” alarm on page 2-226, is raised on the circuit which carries the span. The RPR-SD condition clears when the SONET signal degrade clears.

RPR-SD suppresses the “MAN-REQ” alarm on page 2-183 and the “WTR” alarm on page 2-266.

It is suppressed by the following alarms:

- [FORCED-REQ](#), page 115
- [RPR-PASSTHR](#), page 215
- [RPR-SF](#), page 220

Clear the RPR-SD Condition

-
- Step 1** Complete the “[Clear the SD-P Condition](#)” procedure on page 2-227 to clear this secondary condition.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) to report a Service-Affecting (SA) problem.
-

2.7.361 RPR-SF

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

SONET Logical Objects: ML100T, ML1000, MLFX

The IEEE 802.17b-based RPR Signal Fail condition indicates a signal loss or major signal degradation that deactivates the RPR-IEEE link. The failure that raises RPR-SF can be attributable to any of the following alarms:

- [AIS-P](#), page 39
- [GFP-LFD](#), page 122
- [LOP-P](#), page 158
- [PDI-P](#), page 198
- [PLM-P](#), page 200
- [RFI-P](#), page 210
- [TIM-P](#), page 251
- [UNEQ-P](#), page 258
- [VCG-DOWN](#), page 262

The RPR-SF condition can also occur if a SONET circuit’s state is UNASSIGNED (not provisioned).

This condition clears when these primary cause alarms are cleared. RPR-SF is suppressed by the “[RPR-PASSTHR](#)” alarm on page 2-215 or the “[FORCED-REQ](#)” alarm on page 2-115. RPR-SF itself suppresses the following alarms:

- [MAN-REQ](#), page 183
- [RPR-SD](#), page 219
- [WTR](#), page 266

Clear the RPR-SF Condition

-
- Step 1** Complete the trouble-clearing procedure in this chapter for any primary cause SONET failure condition as previously listed.

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

2.7.362 RPR-SPAN-MISMATCH

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

SONET Logical Objects: ML100T, ML1000, MLFX

The IEEE 802.17b-based RPR-SPAN-MISMATCH alarm is caused by span misprovisioning, span forced switching, physical miscabling, or a circuit loopback.

Miscabling problems between this node's east or west span and its neighboring span in the same direction can also cause this alarm, as will provisioning an XC loopback on a circuit that carries RPR-IEEE traffic.

If a traffic-affecting issue such as the “AIS-P” alarm on page 2-39, the “GFP-LFD” alarm on page 2-122, the “LOP-P” alarm on page 2-158, the “RFI-P” alarm on page 2-210, or the “UNEQ-P” alarm on page 2-258 occurs, it in turn suppresses RPR-SPAN-MISMATCH.



Note

Clearing a circuit XC loopback does not always cause the loopback to clear. If this is the case, a FORCE switch is used to clear the RPR-SPAN-MISMATCH alarm. The FORCE might cause a traffic hit.

RPR- SPAN-MISMATCH is suppressed by “RPR-PASSTHR” alarm on page 2-215.

Clear the RPR-SPAN-MISMATCH Alarm

- Step 1** Locate and clear any primary cause provisioning errors.
- Step 2** If the alarm does not clear, locate and correct any span cabling errors.
- Step 3** If the alarm does not clear, look for and clear XC loopbacks on the spans.
- Step 4** If the alarm does not clear, configure a FORCE switch on the 802.17b-based RPR span and then clear the switch. To do this, enter the following CLI command in RPR-IEEE interface provisioning mode:
- ```
router(config)# rpr-ieee protection request forced-switch {east | west}
```
- Clear the switch by entering the following command:
- ```
router(config)# no rpr-ieee protection request forced-switch {east | west}
```
- Step 5** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) to report a Service-Affecting (SA) problem.

2.7.363 RPRW

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

SONET Logical Objects: ML100T, ML1000, MLFX

The Cisco proprietary RPR Wrapped condition applies to CE100T-8 and ML-Series cards and occurs when the Cisco proprietary RPR protocol initiates a ring wrap due to a fiber cut, node failure, node restoration, new node insertion, or other traffic problem. It can also be raised if the POS port has an Admin down condition. (In this case, you will not see any SONET-level alarms or the “[TPTFAIL \(ML100T, ML1000, MLFX\)](#)” alarm on page 2-255.)

When the wrap occurs, traffic is redirected to the original destination by sending it in the opposite direction around the ring after a link state change or after receiving any SONET path-level alarms.

**Note**

ML-Series card POS interfaces normally send the “[PDI-P](#)” alarm on page 2-198 to the far end when the POS link goes down or when Cisco proprietary RPR wraps. ML-Series card POS interfaces do not send a PDI-P alarm to the far end when this alarm is detected, when the alarm is being sent to the far end, or when the only defects being detected are the “[GFP-LFD](#)” alarm on page 2-122, the “[GFP-CSF](#)” alarm on page 2-120, the VCAT “[LOM](#)” alarm on page 2-158, or the VCAT “[SQM](#)” alarm on page 2-237.

**Note**

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

Clear the RPRW Condition

- Step 1** Look for and clear any service-affecting SONET path-level alarms on the affected circuit, such as the “[LOP-P](#)” alarm on page 2-158, the “[LOS-P \(TRUNK\)](#)” alarm on page 2-170, the “[PLM-P](#)” alarm on page 2-200, or the “[TIM-P](#)” alarm on page 2-251. Clearing such an alarm can also clear RPRW.
- Step 2** If the condition does not clear, look for and clear any service alarms for the ML-Series card itself, such as the “[CARLOSS \(CEMR, CE1000, CE100T\)](#)” alarm on page 2-60, the “[CARLOSS \(ML1000, ML100T, MLFX\)](#)” alarm on page 2-67, the “[TPTFAIL \(CEMR, CE100T, CE1000\)](#)” alarm on page 2-253, or the “[TPTFAIL \(ML100T, ML1000, MLFX\)](#)” alarm on page 2-255.
- Step 3** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.7.364 RUNCFG-SAVENEED

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

SONET Logical Object: EQPT

The Run Configuration Save Needed condition occurs when you change the running configuration file for ML-Series cards. It is a reminder that you must save the change to the startup configuration file for it to be permanent.

The condition clears after you save the running configuration to the startup configuration, such as by entering the following command in privileged executive mode in the CLI:

```
router# copy run start
```

If you do not save the change, the change is lost after the card reboots. If the command “copy run start” is executed in configuration mode and not privileged executive mode, the running configuration will be saved, but the alarm will not clear.

**Note**

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

2.7.365 SD (DS1, DS3)

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

SONET Logical Objects: DS1, DS3

A Signal Degrade (SD) condition for DS-1 or DS-3 occurs when the quality of an electrical signal on a DS3XM-6, DS3XM-12, or DS3/EC1-48 card has exceeded the BER 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, but SD is triggered at a lower bit error rate than SF.

The BER threshold is user-provisionable and has a range for SD from 1E-9 dBm to 1E-5 dBm.

SD can be reported on electrical card ports that are In-Service and Normal (IS-NR); Out-of-Service and Autonomous, Automatic In-Service (OOS-AU,AIS); or Out-of-Service and Management, Maintenance (OOS-MA,MT), but not in the Out-of-Service and Management, Disabled (OOS-MA,DSBLD) service state. The BER count increase associated with this alarm does not take an IS-NR port out of service, but if it occurs on an AINS port, the alarm prevents the port from going into service.

The SD condition clears when the BER level falls to one-tenth of the threshold level that triggered the condition. A BER increase is sometimes caused by a physical fiber problem such as a faulty fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice. SD can also be caused by repeated XC10G card switches that in turn can cause switching on the lines or paths.

**Warning**

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

**Warning**

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

**Note**

Some levels of BER errors (such as 1E-9 dBm) take a long period to raise or clear, about 9,000 seconds, or 150 minutes. If the SD threshold is provisioned at 1E-9 dBm rate, the SD alarm needs at least one and one-half hours to raise and then another period at least as long to clear.

**Note**

The recommended test set for use on all SONET ONS electrical cards is the Omniber 718. For specific procedures to use the test set equipment, consult the manufacturer.

Clear the SD (DS1, DS3) Condition

- Step 1** If the condition applies for a DS-3 line on a DS3XM-6, DS3XM-12, DS3E-12, or DS3/EC1-48 card, complete the [“Clear a DS3XM-6, DS3XM-12, or DS3E-12 Card Loopback Circuit” procedure on page 2-284](#). If the condition applies to any other DS-N card (DS3i-N-14, DS3-12, DS3i-N-14, or DS1/E1-56) complete the [“Clear Other Electrical Card or Ethernet Card Loopbacks” procedure on page 2-284](#).



Caution

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

- Step 2** Ensure that the fiber connector for the card is completely plugged in. For more information about fiber connections and card insertion, refer to the “Install Cards and Fiber-Optic Cable” chapter in the *Cisco ONS 15454 Procedure Guide*.
- Step 3** If the BER threshold is correct and at the expected level, use an optical test set to measure the power level of the line to ensure it is within guidelines. For specific procedures to use the test set equipment, consult the manufacturer.
- Step 4** If the optical power level is good, verify that optical receive levels are within the acceptable range.
- Step 5** If receive levels are good, clean the fibers at both ends according to site practice. If no site practice exists, complete the procedure in the “Maintain the Node” chapter in the *Cisco ONS 15454 Procedure Guide*.
- Step 6** If the condition does not clear, verify that single-mode fiber is used.
- Step 7** If the fiber is of the correct type, verify that a single-mode laser is used at the far-end node.
- Step 8** Clean the fiber connectors at both ends for a signal degrade according to site practice.
- Step 9** Verify that a single-mode laser is used at the far end.
- Step 10** If the problem does not clear, the transmitter at the other end of the optical line could be failing and require replacement. Refer to the [“2.9.4 Physical Card Reseating, Resetting, and Replacement” section on page 2-279](#).
- Step 11** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

2.7.366 SD (E1)

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

SONET Logical Object: E1

An SD condition for an E1 occurs on a DS1/E1-56 card in E1 only mode when the quality of an electrical signal has exceeded the BER signal degrade threshold.

SD is triggered at a lower bit error rate than SF. The SD BER threshold is user-provisionable and ranges from 1E-9 dBm to 1E-5 dBm.

SD can be reported on electrical card ports that are In-Service and Normal (IS-NR); Out-of-Service and Autonomous, Automatic In-Service (OOS-AU,AIS); or Out-of-Service and Management, Maintenance (OOS-MA,MT) but not in the Out-of-Service and Management, Disabled (OOS-MA,DSBLD) service state. The BER count increase associated with this alarm does not take an IS-NR port out of service, but if it occurs on an AINS port, the alarm prevents the port from going into service.

The SD condition clears when the BER level falls to one-tenth of the threshold level that triggered the condition. A BER increase is sometimes caused by a physical fiber problem such as a faulty fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice. SD can also be caused by repeated XC10G card switches that in turn can cause switching on the lines or paths.

**Warning**

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

**Warning**

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

**Note**

Some levels of BER errors (such as 1E-9 dBm) take a long period to raise or clear, about 9,000 seconds, or 150 minutes. If the SD threshold is provisioned at 1E-9 dBm rate, the SD alarm needs at least one and a half hours to raise and then another period at least as long to clear.

**Note**

The recommended test set for use on all SONET ONS electrical cards is the Omniber 718. For specific procedures to use the test set equipment, consult the manufacturer.

Clear the SD (E1) Condition

- Step 1** Complete the [“Clear Other Electrical Card or Ethernet Card Loopbacks” procedure on page 2-284](#).

**Caution**

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

- Step 2** Ensure that the fiber connector for the card is completely plugged in. For more information about fiber connections and card insertion, refer to the “Install Cards and Fiber-Optic Cable” chapter in the *Cisco ONS 15454 Procedure Guide*.
- Step 3** If the BER threshold is correct and at the expected level, use an optical test set to measure the power level of the line to ensure it is within guidelines. For specific procedures to use the test set equipment, consult the manufacturer.
- Step 4** If the optical power level is good, verify that optical receive levels are within the acceptable range.
- Step 5** If receive levels are good, clean the fibers at both ends according to site practice. If no site practice exists, complete the procedure in the “Maintain the Node” chapter of the *Cisco ONS 15454 Procedure Guide*.
- Step 6** If the condition does not clear, verify that single-mode fiber is used.
- Step 7** If the fiber is of the correct type, verify that a single-mode laser is used at the far-end node.
- Step 8** Clean the fiber connectors at both ends for a signal degrade according to site practice.
- Step 9** If the problem does not clear, the transmitter at the other end of the optical line could be failing and require replacement. Refer to the [“2.9.4 Physical Card Reseating, Resetting, and Replacement” section on page 2-279](#).

- Step 10** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.367 SD (TRUNK)

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.368 SD-L

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

SONET Logical Objects: EC1, OCN

An SD Line condition is similar to the “[SD \(DS1, DS3\) condition on page 2-223](#)”. It applies to the line level of the SONET signal and travels on the B2 byte of the SONET overhead.

An SD-L on an Ethernet or OC-N card does not cause a protection switch. If the alarm is reported on a card that has also undergone a protection switch, the SD BER count continues to accumulate. The condition is superseded by higher-priority alarms such as the “[LOF \(EC1\) alarm on page 2-154](#)”, the “[LOF \(OCN\) alarm on page 2-155](#)”, the “[LOS \(EC1\) alarm on page 2-166](#)”, and the “[LOS \(OCN\) alarm on page 2-168](#)”.



Note

For more information about Ethernet cards, refer to the Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.

Clear the SD-L Condition

- Step 1** Complete the “[Clear the SD \(DS1, DS3\) Condition procedure on page 2-224](#)”.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.369 SD-L (TRUNK)

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.370 SD-P

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

SONET Logical Objects: STSMON, STSTRM

An SD Path condition is similar to the “SD (DS1, DS3)” condition on page 2-223, but it applies to the path (STS) layer of the SONET overhead. A path or STS-level SD alarm travels on the B3 byte of the SONET overhead.

For path protection protected circuits, the BER threshold is user-provisionable and has a range for SD from 1E-9 dBm to 1E-5 dBm. For BLSR 1+1 and unprotected circuits, the BER threshold value is not user-provisionable and the error rate is hard-coded to 1E-6 dBm.

On path protection configurations, an SD-P condition causes a switch from the working card to the protect card at the path (STS) level. On BLSR, 1+1, and on unprotected circuits, an SD-P condition does not cause switching.

The BER increase that causes the condition 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.

The SD clears when the BER level falls to one-tenth of the threshold level that triggered the alarm.

Clear the SD-P Condition

-
- Step 1** Complete the “Clear the SD (DS1, DS3) Condition” procedure on page 2-224.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.371 SD-V

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

SONET Logical Objects: VT-MON, VT-TERM

An SD-V condition is similar to the “SD (DS1, DS3)” condition on page 2-223, but it applies to the VT layer of the SONET overhead.

For path protection protected circuits, the BER threshold is user-provisionable and has a range for SD from 1E-9 dBm to 1E-5 dBm. For BLSR 1+1 and unprotected circuits, the BER threshold value is not user-provisionable and the error rate is hard-coded to 1E-6 dBm.

On path protection configurations, an SD-V condition does not cause a switch from the working card to the protect card at the path (STS) level. On BLSR, 1+1, and on unprotected circuits, an SD-V condition does not cause switching.

The BER increase that causes the alarm is sometimes caused by a physical fiber problem such as a poor fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice.

The SD alarm clears when the BER level falls to one-tenth of the threshold level that triggered the alarm.

Clear the SD-V Condition

-
- Step 1** Complete the “Clear the SD (DS1, DS3) Condition” procedure on page 2-224.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.372 SF (DS1, DS3)

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

SONET Logical Objects: DS1, DS3

A Signal Fail (SF) condition occurs when the quality of the signal has exceeded the BER signal failure threshold. Signal failure is defined by Telcordia as a “hard failure” condition. The SD and SF conditions both monitor the incoming BER error rate and are similar conditions, but SF is triggered at a higher BER than SD.

The BER threshold is user-provisionable and has a range for SF from 1E–5 dBm to 1E–3 dBm.



Warning

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



Warning

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

Clear the SF (DS1, DS3) Condition

Step 1 Complete the “[Clear the SD \(DS1, DS3\) Condition](#)” procedure on page 2-224.



Caution

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

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

2.7.373 SF (E1)

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

SONET Logical Object: E1

An SF condition for an E1 occurs on a DS1/IE1-56 card in E1 only mode when the quality of the signal has exceeded the BER signal failure threshold.

SF monitors the incoming BER error rate just as SD does, but SF is triggered at a higher BER than SD. The SF BER threshold is user-provisionable and has a range for SF from 1E–5 dBm to 1E–3 dBm.



Warning

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

**Warning**

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

Clear the SF (E1) Condition

Step 1 Complete the [“Clear the SD \(E1\) Condition” procedure on page 2-225](#).

**Caution**

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

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

2.7.374 SF (TRUNK)

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.375 SF-L

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

SONET Logical Objects: EC1, OCN

An SF Line condition is similar to the [“SF \(DS1, DS3\)” condition on page 2-228](#), but it applies to the line layer B2 overhead byte of the SONET signal. It can trigger a protection switch.

The SF-L condition clears when the BER level falls to one-tenth of the threshold level that triggered the condition. A BER increase is sometimes caused by a physical fiber problem, including a poor fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice.

The condition is superseded by higher-priority alarms such as the [“LOF \(EC1\)” alarm on page 2-154](#), the [“LOS \(EC1\)” alarm on page 2-166](#), and the [“LOS \(OCN\)” alarm on page 2-168](#).

Clear the SF-L Condition

Step 1 Complete the [“Clear the SD \(DS1, DS3\) Condition” procedure on page 2-224](#).

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

2.7.376 SF-L (TRUNK)

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.377 SF-P

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

SONET Logical Objects: STSMON, STSTRM

An SF Path condition is similar to the “[SF \(DS1, DS3\)” condition on page 2-228](#), but it applies to the path (STS) layer B3 byte of the SONET overhead. It can trigger a protection switch.

The SF-P condition clears when the BER level falls to one-tenth of the threshold level that triggered the condition. A BER increase is sometimes caused by a physical fiber problem, including a poor fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice.

Clear the SF-P Condition

-
- Step 1** Complete the “[Clear the SD \(DS1, DS3\) Condition” procedure on page 2-224](#).
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.378 SFTWDOWN

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

SONET Logical Object: EQPT

A Software Download in Progress alarm occurs when the TCC2/TCC2P is downloading or transferring software.

If the active and standby TCC2/TCC2Ps have the same versions of software, it takes approximately three minutes for software to be updated on a standby TCC2/TCC2P.

If the active and standby TCC2/TCC2Ps have different software versions, the transfer can take up to 30 minutes. Software transfers occur when different software versions exist on the two cards. After the transfer completes, the active TCC2/TCC2P reboots and goes into standby mode after approximately three minutes.

No action is necessary. Wait for the transfer or the software download to complete. If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.



Caution

Updating software on a standby TCC2/TCC2P can take up to 30 minutes. Wait the full time period before removing the card. Premature removal can cause flash corruption.

**Note**

When you upgrade a TCC2 to card to a TCC2P, the SFTWDOWN alarm can be raised and cleared more than once before the software download is complete. For example, when you remove the standby TCC2 card in Slot 11 and replace it with a TCC2P card, the SFTWDOWN alarm occurs within moments of this replacement. It can briefly clear and then raise again before it is finally cleared at the end of the upgrade process.

**Note**

SFTWDOWN is an informational alarm.

2.7.379 SF-V

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

SONET Logical Objects: VT-MON, VT-TERM

An SF-V condition is similar to the “[SF \(DS1, DS3\)](#)” condition on page 2-228, but it applies to the VT layer of the SONET overhead.

Clear the SF-V Condition

-
- Step 1** Complete the “[Clear the SD \(DS1, DS3\) Condition](#)” procedure on page 2-224.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.380 SHELF-COMM-FAIL

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.381 SH-IL-VAR-DEG-HIGH

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.382 SH-IL-VAR-DEG-LOW

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.383 SHUTTER-OPEN

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.384 SIGLOSS

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

SONET Logical Object: FCMR

DWDM Logical Objects: ESCON, FC, GE, ISC, TRUNK

The Signal Loss on Data Interface alarm is raised on FC_MR-4 card receive client ports and MXP card FC and ISC client data ports when there is a loss of signal. (Loss of Gigabit Ethernet client signal results in a “CARLOSS (GE)” alarm on page 2-67, not SIGLOSS.) SIGLOSS can also be raised on the MXP trunk port.

If the “SYNCLOSS” alarm on page 2-246, was previously raised on the port, the SIGLOSS alarm will demote it.

Clear the SIGLOSS Alarm

-
- Step 1** Ensure that the data port connection at the near-end card’s port of the SONET link is operational.
 - Step 2** Verify fiber continuity to the port. To verify fiber continuity, follow site practices.
 - Step 3** Check the physical port LED on the card. The port LED looks clear (that is, not lit green) if the link is not connected.
 - Step 4** If the alarm does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.
-

2.7.385 SNTP-HOST

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

SONET Logical Object: NE

The Simple Network Timing Protocol (SNTP) Host Failure alarm indicates that an ONS 15454 serving as an IP proxy for the other ONS 15454 nodes in the ring is not forwarding SNTP information to the other nodes in the network. The forwarding failure can result from two causes: either the IP network attached to the ONS 15454 proxy node is experiencing problems, or the ONS 15454 proxy node itself is not functioning properly.

Clear the SNTP-HOST Alarm

-
- Step 1** Ping the SNTP host from a workstation in the same subnet to ensure that communication is possible within the subnet by completing the “[1.9.8 Verify PC Connection to the ONS 15454 \(ping\)](#)” procedure on page 1-120.

- Step 2** If the ping fails, contact the network administrator who manages the IP network that supplies the SNTP information to the proxy and determine whether the network is experiencing problems, which could affect the SNTP server/router connecting to the proxy ONS 15454 system.
- Step 3** If no network problems exist, ensure that the ONS system proxy is provisioned correctly:
- In node view for the ONS 15454 serving as the proxy, click the **Provisioning > General** tabs.
 - Ensure that the Use NTP/SNTP Server check box is checked.
 - If the Use NTP/SNTP Server check box is not checked, click it.
 - Ensure that the Use NTP/SNTP Server field contains a valid IP address for the server.
- Step 4** If proxy is correctly provisioned, refer to the “Timing” chapter in the *Cisco ONS 15454 Reference Manual* for more information on SNTP Host.
- Step 5** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.386 SPANLEN-OUT-OF-RANGE

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.387 SPAN-SW-EAST

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

SONET Logical Object: OCN

The Span Switch Is Active East Side condition occurs when a span switch occurs at the east side of a four-fiber BLSR span using a Manual Switch, APS switch, or Force Span command. The condition clears when the switch is cleared. SPAN-SW-EAST is visible on the network view Alarms, Conditions, and History tabs. The port where the Force Span was applied shows an “F” on the network view detailed circuit map.



Note

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

2.7.388 SPAN-SW-WEST

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

SONET Logical Object: OCN

The Span Switch Is Active West Side condition occurs when a span switch occurs at the west side of a four-fiber BLSR span using a Manual Switch, APS switch, or Force Span command. The condition clears when the switch is cleared. SPAN-SW-WEST is visible on the network view Alarms, Conditions, and History tabs. The port where the Force Span was applied shows an “F” on the network view detailed circuit map.

**Note**

SPAN-SW-WEST is an informational condition and does not require troubleshooting.

2.7.389 SQUELCH

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

SONET Logical Object: OCN

The Ring Squelching Traffic condition occurs in a BLSR when a node that originates or terminates STS circuits fails or is isolated by multiple fiber cuts or maintenance Force Ring commands. The isolation or failure of the node disables circuits that originate or terminate on the failed node. SQUELCH conditions appear on one or both of the nodes on either side of the isolated or failed node. The [“AIS-P” condition on page 2-39](#) also appears on all nodes in the ring except the isolated node.

**Warning**

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

**Warning**

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

**Warning**

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

Clear the SQUELCH Condition

**Caution**

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

Step 1

Determine the isolated node:

- a. From the View menu, choose **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. To verify cable continuity, follow site practices.

Step 3

If fiber continuity is good, verify that the proper ports are in service:

- a. Confirm that the LED is correctly illuminated on the physical card.
A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
- b. To determine whether the OC-N port is in service, double-click the card in CTC to open the card view.
- c. Click the **Provisioning > Line** tabs.

- d. Verify that the Admin State column lists the port as IS.
- e. If the Admin State column lists the port as OOS,MT or OOS,DSBLD, click the column and choose **IS**. Click **Apply**.

**Note**

If ports managed into IS admin state are not receiving signals, the LOS alarm is either raised or remains, and the port service state transitions to OOS-AU,FLT.

- Step 4** If the correct ports are in service, use an optical test set to verify that a valid signal exists on the line. For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving card as possible.
- Step 5** If the signal is valid, verify that the power level of the optical signal is within the optical card receiver specifications. Refer to the *Cisco ONS 15454 Reference Manual* for card specifications.
- Step 6** If the receiver levels are good, ensure that the optical transmit and receive fibers are connected properly.
- Step 7** If the connectors are good, complete the [“Physically Replace a Traffic Card” procedure on page 2-281](#) for the OC-N card.
- Step 8** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

2.7.390 SQUELCHED

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

SONET Logical Object: OCN

DWDM Logical Objects: 2R, ESCON, FC, GE, ISC, TRUNK

The Client Signal Squelched condition is raised by a TXP_MR_10G, TXP_MR_10E, TXP_MR_2.5G, TXPP_MR_2.5G, MXP_2.5G_10G, MXP_2.5G_10E, MXP_MR_2.5G, or MXPP_MR_2.5G card.

The condition can be raised in the following situations:

- An MXP or TXP client facility detects that an upstream receive facility has experienced a loss of signal (such as an Ethernet CARLOSS, DWDM SIGLOSS, or optical LOS). In response, the facility's transmit is turned off (SQUELCHED). The upstream receive facilities are the trunk receive on the same card as the client, as well as the client receive on the card at the other end of the trunk span.
- The client will squelch if the upstream trunk receive (on the same card) experiences the [“SIGLOSS” alarm on page 2-232](#), the [“CARLOSS \(FC\)” alarm on page 2-64](#), the [“CARLOSS \(GE\)” alarm on page 2-67](#), the [“CARLOSS \(ISC\)” alarm on page 2-67](#), the [“LOS \(2R\)” alarm on page 2-161](#), the [“LOS \(ESCON\)” alarm on page 2-167](#), the [“LOS \(ISC\)” alarm on page 2-168](#), or the [“LOS \(TRUNK\)” alarm on page 2-170](#). In some transparent modes, the client is squelched if the trunk detects the [“AIS” alarm on page 2-38](#) or the [“TIM” alarm on page 2-250](#).
- The client will squelch if the upstream client receive (on the card at the other end of the DWDM span) experiences the [“SIGLOSS” alarm on page 2-232](#), the [“CARLOSS \(FC\)” alarm on page 2-64](#), the [“CARLOSS \(GE\)” alarm on page 2-67](#), the [“CARLOSS \(ISC\)” alarm on page 2-67](#), the [“LOS \(2R\)” alarm on page 2-161](#), the [“LOS \(ESCON\)” alarm on page 2-167](#), the [“LOS \(ISC\)” alarm on page 2-168](#), or the [“LOS \(TRUNK\)” alarm on page 2-170](#).

In an example situation, an upstream MXP_2.5G_10G client port receive experiences a “loss of light,” and this port raises CARLOSS, SIGLOSS, or LOS (determined by the payload type) locally. The port also sends client signal fail to its downstream card. The downstream card raises a “GFP-CSF” alarm on page 2-120, turns off the client transmit laser, and raises the SQUELCHED condition.

The local client raises SQUELCHED if it also raises one of the following alarms for the client, all of which are signalled by the upstream node:

- 2.7.155 GFP-CSF, page 2-120
- 2.7.158 GFP-LFD, page 2-122
- 2.7.159 GFP-NO-BUFFERS, page 2-123
- 2.7.156 GFP-DE-MISMATCH, page 2-121
- 2.7.157 GFP-EX-MISMATCH, page 2-122
- 2.7.294 ODUK-1-AIS-PM, page 2-194
- 2.7.295 ODUK-2-AIS-PM, page 2-194
- 2.7.296 ODUK-3-AIS-PM, page 2-194
- 2.7.297 ODUK-4-AIS-PM, page 2-194

On the MXP_MR_10G, the local client raises a SQUELCHED condition if the upstream client detects one of the following alarms. Note that no corresponding local alarm is raised to indicate which of these conditions is present upstream.

- LOS for the clients including the “LOS (2R)” alarm on page 2-161, the “LOS (ESCON)” alarm on page 2-167, and the “LOS (ISC)” alarm on page 2-168
- CARLOSS for the clients including the “CARLOSS (FC)” alarm on page 2-64, the “CARLOSS (GE)” alarm on page 2-67, and the “CARLOSS (ISC)” alarm on page 2-67.

The local client raises a SQUELCHED condition if the local trunk raises one of the following alarms:

- 2.7.313 OTUK-AIS, page 2-197
- 2.7.316 OTUK-LOF, page 2-197
- 2.7.232 LOS (TRUNK), page 2-170
- 2.7.319 OTUK-TIM, page 2-198 (squelching enabled)
- 2.7.298 ODUK-AIS-PM, page 2-194
- 2.7.300 ODUK-LCK-PM, page 2-195
- 2.7.304 ODUK-TIM-PM, page 2-195 (squelching enabled)
- 2.7.422 TIM, page 2-250 (for the OC-N, squelching enabled)
- 2.7.209 LOF (OCN), page 2-155
- 2.7.230 LOS (OCN), page 2-168
- 2.7.58 CARLOSS (TRUNK), page 2-68
- 2.7.456 WVL-MISMATCH, page 2-267 (client or trunk)

When troubleshooting the SQUELCHED condition locally, look for failures progressing upstream in the following order. (If you are troubleshooting this alarm remotely, reverse the order of progress.)

- Local client alarms, as above
- Local trunk alarms, as above
- Remote (upstream) client receive alarms, as above

**Note**

If you see a SQUELCHED condition on the trunk, this can only be caused by a transponder (TXP) card.

**Note**

For more information about MXP or TXP cards, refer to the *Cisco ONS 15454 DWDM Reference Manual*.

Clear the SQUELCHED Condition

- Step 1** If the object is reported against any object besides ESCON, determine whether the remote node and local node reports and LOF or the LOS alarm (for the client trunk, as listed above). If it does, turn to the relevant section in this chapter and complete the troubleshooting procedure.
- Step 2** If no LOF or LOS is reported, determine whether any other listed remote node or local node conditions as listed above has occurred. If so, turn to the relevant section of this chapter and complete the troubleshooting procedure.
- Step 3** If none of these alarms is reported, determine whether the local port reporting the SQUELCHED condition is in loopback. (You will see LPBKFACILITY or LPBKTERMINAL condition for this particular client type in the Condition window.) If it is in loopback, complete the following steps:
- Double-click the client card to open the card view.
 - Click the **Maintenance > Loopback > Port** tabs.
 - If the port Admin State column says OOS,MT or OOS,DSBLD, click the cell to highlight it and choose **IS** from the drop-down list. Changing the state to IS also clears any loopback provisioned on the port.

**Note**

If ports managed into IS admin state are not receiving signals, the LOS alarm is either raised or remains, and the port service state transitions to OOS-AU,FLT.

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

2.7.391 SQM

Default Severity: Critical (CR), Service-Affecting (SA) for STSTRM; Major (MJ), Service-Affecting (SA) for VT-TERM

SONET Logical Objects: STSTRM, VT-TERM

The Sequence Mismatch alarm is a virtual concatenated (VCAT) member alarm. (VCAT member circuits are independent circuits that are concatenated from different time slots into a higher-rate signal.) The alarm occurs when the expected sequence numbers of VCAT members do not match the received sequence numbers.

Clear the SQM Alarm

-
- Step 1** For the errored circuit, complete the [“Delete a Circuit” procedure on page 2-283](#).
 - Step 2** Recreate the circuit using the “Create Circuits and VT Tunnels” chapter of the *Cisco ONS 15454 Procedure Guide*.
 - Step 3** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.
-

2.7.392 SSM-DUS

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

SONET Logical Objects: BITS, DS1, E1, OCN

DWDM Logical Object: TRUNK

The Synchronization Status (SSM) Message Quality Changed to Do Not Use (DUS) condition occurs when the synchronization status message (SSM) quality level degrades to DUS or is manually changed to DUS.

The signal is often manually changed to DUS to prevent timing loops from occurring. Sending a DUS prevents the timing from being reused in a loop. The DUS signal can also be sent for line maintenance testing.



Note

SSM-DUS is an informational condition and does not require troubleshooting.

2.7.393 SSM-FAIL

Single Failure Default Severity: Minor (MN), Non-Service-Affecting (NSA); Double Failure

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

SONET Logical Objects: BITS, DS1, E1, OCN

DWDM Logical Object: TRUNK

The SSM Failed alarm occurs when the synchronization status messaging received by the ONS 15454 fails. The problem is external to the ONS 15454. This alarm indicates that although the ONS 15454 is set up to receive SSM, the timing source is not delivering valid SSM messages.

Clear the SSM-FAIL Alarm

-
- Step 1** Verify that SSM is enabled on the external timing source.
 - Step 2** If timing is enabled, use an optical test set to determine that the external timing source is delivering SSM. For specific procedures to use the test set equipment, consult the manufacturer.
-

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

2.7.394 SSM-LNC

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

SONET Logical Objects: BITS, NE-SREF, OCN

DWDM Logical Object: TRUNK

The SSM Local Node Clock (LNC) Traceable condition occurs on MXP trunk ports when the SSM (S1) byte of the SONET overhead multiplexing section has been changed to signify that the line or BITS timing source is the LNC.



Note

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

2.7.395 SSM-OFF

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

SONET Logical Objects: BITS, DS1, E1, OCN

DWDM Logical Object: TRUNK

The SSM Off condition applies to references used for timing the node. It occurs when the SSM for the reference has been turned off. The node 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 2-238.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.396 SSM-PRC

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

SONET Logical Objects: BITS, NE-SREF, OCN

DWDM Logical Object: TRUNK

The SSM Primary Reference Clock (PRC) Traceable condition occurs when the SONET transmission level for an MXP trunk port is PRC.

**Note**

SSM-PRS is an informational condition and does not require troubleshooting.

2.7.397 SSM-PRS

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

SONET Logical Objects: BITS, DS1, E1, NE-SREF, OCN

DWDM Logical Object: TRUNK

The SSM Primary Reference Source (PRS) Traceable condition occurs when the SSM transmission level is changed to Stratum 1 Traceable.

**Note**

SSM-PRS is an informational condition and does not require troubleshooting.

2.7.398 SSM-RES

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

SONET Logical Objects: BITS, DS1, E1, NE-SREF, OCN

DWDM Logical Object: TRUNK

The SSM Reserved (RES) For Network Synchronization Use condition occurs when the synchronization message quality level is changed to RES.

**Note**

SSM-RES is an informational condition and does not require troubleshooting.

2.7.399 SSM-SDH-TN

The SSM-SDH-TN condition is not used in this platform in this release. It is reserved for development.

2.7.400 SSM-SETS

The SSM-SETS condition is not used in this platform in this release. It is reserved for development.

2.7.401 SSM-SMC

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

SONET Logical Objects: BITS, DS1, E1, NE-SREF, OCN

DWDM Logical Object: TRUNK

The SSM SONET Minimum Clock (SMC) Traceable condition occurs when the synchronization message quality level changes to SMC. The login node does not use the clock because the node cannot use any reference beneath its internal level, which is ST3.

**Note**

SSM-SMC is an informational condition and does not require troubleshooting.

2.7.402 SSM-ST2

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

SONET Logical Objects: BITS, DS1, E1, NE-SREF, OCN

DWDM Logical Object: TRUNK

The SSM Stratum 2 (ST2) Traceable condition occurs when the synchronization message quality level is changed to ST2.

**Note**

SSM-ST2 is an informational condition and does not require troubleshooting.

2.7.403 SSM-ST3

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

SONET Logical Objects: BITS, DS1, E1, NE-SREF, OCN

DWDM Logical Object: TRUNK

The SSM Stratum 3 (ST3) Traceable condition occurs when the synchronization message quality level is changed to ST3.

**Note**

SSM-ST3 is an informational condition and does not require troubleshooting.

2.7.404 SSM-ST3E

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

SONET Logical Objects: BITS, DS1, E1, NE-SREF, OCN

DWDM Logical Object: TRUNK

The SSM Stratum 3E (ST3E) Traceable condition indicates that the synchronization message quality level is changed to ST3E from a lower level of synchronization. SSM-ST3E is a Generation 2 SSM and is used for Generation 1.

**Note**

SSM-ST3E is an informational condition and does not require troubleshooting.

2.7.405 SSM-ST4

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

SONET Logical Objects: BITS, DS1, E1, NE-SREF, OCN

DWDM Logical Object: TRUNK

The SSM Stratum 4 (ST4) Traceable condition occurs when the synchronization message quality level is lowered to ST4. The message quality is not used because it is below ST3.



Note

SSM-ST4 is an informational condition and does not require troubleshooting.

2.7.406 SSM-STU

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

SONET Logical Objects: BITS, DS1, E1, NE-SREF, OCN

DWDM Logical Object: TRUNK

The SSM Synchronization Traceability Unknown (STU) condition occurs when the reporting node is timed to a reference that does not support SSM, but the ONS 15454 has SSM support enabled. SSM-STU can also occur if the timing source is sending out SSM messages but SSM is not enabled on the ONS 15454.

Clear the SSM-STU Condition

-
- Step 1** In node view, click the **Provisioning > Timing > BITS Facilities** tabs.
- Step 2** Complete one of the following depending upon the status of the Sync Messaging Enabled check box:
- If the **Sync. Messaging Enabled** check box for the BITS source is checked, uncheck the box.
 - If the **Sync. Messaging Enabled** check box for the BITS source is not checked, check the box.
- Step 3** Click **Apply**.
- Step 4** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.407 SSM-TNC

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

SONET Logical Objects: BITS, NE-SREF, OCN

DWDM Logical Object: TRUNK

The SSM Transit Node Clock (TNC) Traceable condition occurs when the synchronization message quality level is changed to TNC.



Note

SSM-TNC is an informational condition and does not require troubleshooting.

2.7.408 STS-SQUELCH-L

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

SONET Logical Object: OCN

The Ring is Squelching STS traffic condition is raised on an OC-N facility. If the node failure scenario includes the source or destination node, then switching the nodes will squelch all the STSs that originate from or destinate to the failure node. The condition resolves when the node is no longer failing.

This condition has an NA severity by default. However, the condition indicates that traffic is squelched due to node failure, that is, traffic outage. Traffic outage can be caused by different problems, such as multiple LOS alarms, AIS-L, or node power outage. STS-SQUELCH-L is symptomatic and indicates that the user must investigate which node in a ring is being isolated and what is causing the node isolation.

**Note**

STS-SQUELCH-L is an informational condition.

2.7.409 SW-MISMATCH

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

SONET Logical Object: EQPT

The Software Mismatch condition occurs during software upgrade when there is a mismatch between software versions. The card connecting to the TCC2/TCC2P is running an older version than the TCC2/TCC2P is.

Clear the SW-MISMATCH Condition

- Step 1** Complete the [“Reset a Traffic Card in CTC” procedure on page 2-278](#) for the errored card.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

2.7.410 SWMTXMOD-PROT

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

SONET Logical Object: EQPT

The Switching Matrix Module Failure on Protect Slot alarm is raised by the Slot 10 cross connect card if this card is active (ACT). Any kind of cross-connect card can raise this alarm. (Two exceptions are given in the following paragraph.) SWMTXMOD-PROT occurs when a logic component internal to the Slot 10 cross connect is out of frame (OOF) with a traffic card in the system. In this case, the alarm is raised against the traffic card slot.

The XC-VXC-10G card can raise this alarm (in Slot 10) whether it is ACT or standby (SBY). The XCVT card can raise SWMTXMOD-PROT against itself if the cross-connect card is OOF with a second logic component on the same cross connect card.

Clear the SWMTXMOD-PROT Alarm

- Step 1** Complete the [“Reset a Traffic Card in CTC” procedure on page 2-278](#) for the Slot 10 card. For the LED behavior, see the [“2.8.2 Typical Traffic Card LED Activity During Reset” section on page 2-267](#).

- Step 2** Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
- Step 3** If the alarm does not clear, complete the [“Remove and Reinsert \(Reseat\) Any Card” procedure on page 2-280](#) for the Slot 10 cross-connect card.
- Step 4** Complete the [“Side Switch the Active and Standby Cross-Connect Cards” procedure on page 2-278](#).



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

- Step 5** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.

2.7.411 SWMTXMOD-WORK

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

SONET Logical Object: EQPT

The Switching Matrix Module Failure on Working Slot alarm is raised by the Slot 8 cross connect card if this card is active (ACT). Any kind of cross-connect card can raise this alarm. (Two exceptions are given in the following paragraph.) SWMTXMOD-WORK occurs when a logic component internal to the Slot 8 cross connect is OOF with a traffic card in the system. In this case, the alarm is raised against the traffic card slot.

The XC-VXC-10G card can raise this alarm (in Slot 8) whether it is ACT or standby (SBY). The XCVT card can raise SWMTXMOD-WORK against itself if the cross-connect card is OOF with a second logic component on the same cross connect card.

Clear the SWMTXMOD-WORK Alarm

- Step 1** Complete the [“Reset a Traffic Card in CTC” procedure on page 2-278](#) for the Slot 8 card. For LED behavior, see the [“2.8.2 Typical Traffic Card LED Activity During Reset” section on page 2-267](#).
- Step 2** Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
- Step 3** If the alarm does not clear, complete the [“Remove and Reinsert \(Reseat\) Any Card” procedure on page 2-280](#) for the Slot 8 cross-connect card.
- Step 4** Complete the [“Side Switch the Active and Standby Cross-Connect Cards” procedure on page 2-278](#).



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

- Step 5** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.
-

2.7.412 SWTOPRI

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

SONET Logical Objects: EXT-SREF, NE-SREF

The Synchronization Switch to Primary Reference condition occurs when the ONS 15454 switches to the primary timing source (reference 1). The ONS 15454 uses three ranked timing references. The timing references are typically two BITS-level or line-level sources and an internal reference.



Note

SWTOPRI is an informational condition and does not require troubleshooting.

2.7.413 SWTOSEC

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

SONET Logical Objects: EXT-SREF, NE-SREF

The Synchronization Switch to Secondary Reference condition occurs when the ONS 15454 has switched to a secondary timing source (reference 2).

Clear the SWTOSEC Condition

- Step 1** To clear the condition, clear alarms related to failures of the primary source, such as the [“SYNCPRI” alarm on page 2-247](#).
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.414 SWTOTHIRD

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

SONET Logical Objects: EXT-SREF, NE-SREF

The Synchronization Switch to Third Reference condition occurs when the ONS 15454 has switched to a third timing source (reference 3).

Clear the SWTOTHIRD Condition

- Step 1** To clear the condition, clear alarms related to failures of the primary source, such as the [“SYNCPRI” alarm on page 2-247](#) or the [“SYNCSEC” alarm on page 2-248](#).

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

2.7.415 SYNC-FREQ

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

SONET Logical Objects: BITS, DS1, E1, OCN

DWDM Logical Object: TRUNK

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

Clear the SYNC-FREQ Condition

- Step 1** Use an optical test set to verify the timing frequency of the line or BITS timing source and ensure that it falls within the proper frequency. For specific procedures to use the test set equipment, consult the manufacturer.

For BITS, the proper timing frequency range is approximately –15 PPM to 15 PPM. For optical line timing, the proper frequency range is approximately –16 PPM to 16 PPM.

- Step 2** If the reference source frequency is not outside of bounds, complete the [“Physically Replace a Traffic Card” procedure on page 2-281](#) for the TCC2/TCC2P.



Note It takes up to 30 minutes for the TCC2/TCC2P to transfer the system software to the newly installed TCC2/TCC2P. Software transfer occurs in instances where different software versions exist on the two cards. When the transfer completes, the active TCC2/TCC2P reboots and goes into standby mode after approximately three minutes.

- Step 3** If the SYNC-FREQ condition continues to report after replacing the TCC2/TCC2P, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

2.7.416 SYNCLOSS

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

SONET Logical Object: FCMR

DWDM Logical Objects: FC, GE, ISC, TRUNK

The Loss of Synchronization on Data Interface alarm is raised on FC_MR-4 client ports and MXP cards client or trunk ports when there is a loss of signal synchronization on the port. This alarm is demoted by the SIGLOSS alarm.

Clear the SYNCLOSS Alarm

-
- Step 1** Ensure that the data port connection at the near-end card's port of the SONET link is operational.
- Step 2** Verify fiber continuity to the port. To do this follow site practices.
- Step 3** View the physical port LED to determine whether the alarm has cleared:
- If the LED is green, the alarm has cleared.
 - If the port LED is clear (that is, not illuminated green), the link is not connected and the alarm has not cleared.
 - If the LED is red, this indicates that the fiber is pulled.
- Step 4** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 to report a Service-Affecting (SA) problem.
-

2.7.417 SYNCPRI

Default Severity: Minor (MN), Non-Service-Affecting (NSA) for EXT-SREF;Major (MJ), Service-Affecting (SA) for NE-SREF

SONET Logical Objects: EXT-SREF, NE-SREF

A Loss of Timing on Primary Reference alarm occurs when the ONS 15454 loses the primary timing source (reference 1). The ONS 15454 uses three ranked timing references. The timing references are typically two BITS-level or line-level sources and an internal reference. If SYNCPRI occurs, the ONS 15454 should switch to its secondary timing source (reference 2). Switching to the secondary timing source also triggers the [“SWTOSEC” alarm on page 2-245](#).



Note

The SYNCPRI alarm will be escalated to Major (MJ), Service-Affecting if no other valid references (SYNCSEC, SYNCTHIRD) are available. If any other reference are available then SYNCPRI gets raised as Minor (MN), non service affecting.

Clear the SYNCPRI Alarm

-
- Step 1** In node view, click the **Provisioning > Timing > General** tabs.
- Step 2** Verify the current configuration for REF-1 of the NE Reference.
- Step 3** If the primary timing reference is a BITS input, complete the [“Clear the LOS \(BITS\) Alarm” procedure on page 2-161](#).
- Step 4** If the primary reference clock is an incoming port on the ONS 15454, complete the [“Clear the LOS \(OCN\) Alarm” procedure on page 2-169](#).
- Step 5** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.418 SYNCSEC

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

SONET Logical Objects: EXT-SREF, NE-SREF

A Loss of Timing on Secondary Reference alarm occurs when the ONS 15454 loses the secondary timing source (reference 2). If SYNCSEC occurs, the ONS 15454 should switch to a third timing source (reference 3) to obtain valid timing for the ONS 15454. Switching to a third timing source also triggers the [“SWTOTHIRD” alarm on page 2-245](#).



Note

The severity of SYNCSEC alarm is dependent on the alarm profile it is associated with. If the alarm profile it is associated with is Major (MJ), then this condition is raised as MJ, service affecting, even if alternate source of references are available.

Clear the SYNCSEC Alarm

-
- Step 1** In node view, click the **Provisioning > Timing > General** tabs.
 - Step 2** Verify the current configuration of 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 2-161](#).
 - Step 4** Verify that the BITS clock is operating properly.
 - Step 5** If the secondary timing source is an incoming port on the ONS 15454, complete the [“Clear the LOS \(OCN\) Alarm” procedure on page 2-169](#).
 - Step 6** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.419 SYNCTHIRD

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

SONET Logical Objects: EXT-SREF, NE-SREF

A Loss of Timing on Third Reference alarm occurs when the ONS 15454 loses the third timing source (reference 3). If SYNCTHIRD occurs and the ONS 15454 uses an internal reference for source three, the TCC2/TCC2P could have failed. The ONS 15454 often reports either the [“FRNGSYNC” condition on page 2-118](#) or the [“HLDVRSYNC” condition on page 2-130](#) after a SYNCTHIRD alarm.



Note

The severity of SYNCTHIRD alarm is dependent on the alarm profile it is associated with. If the alarm profile it is associated with is Major (MJ), then this condition is raised as MJ, service affecting, even if alternate source of references are available.

Clear the SYNCTHIRD Alarm

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

- Step 2** Verify that the current configuration of REF-3 for the NE Reference. For more information about references, refer to the “Timing” chapter in the *Cisco ONS 15454 Reference Manual*.
- Step 3** If the third timing source is a BITS input, complete the [“Clear the LOS \(BITS\) Alarm” procedure on page 2-161](#).
- Step 4** If the third timing source is an incoming port on the ONS 15454, complete the [“Clear the LOS \(OCN\) Alarm” procedure on page 2-169](#).

**Caution**

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

- Step 5** If the third timing source uses the internal ONS 15454 timing, complete the [“Reset an Active TCC2/TCC2P Card and Activate the Standby Card” procedure on page 2-278](#).
Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.
- Step 6** If the reset card has not rebooted successfully, or the alarm has not cleared, call Cisco TAC 1 800 553-2447. If the Cisco TAC technician tells you to reseal the card, complete the [“Remove and Reinsert \(Reseat\) the Standby TCC2/TCC2P Card” procedure on page 2-280](#). If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the [“Physically Replace a Traffic Card” procedure on page 2-281](#).

2.7.420 SYSBOOT

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

SONET Logical Object: NE

The System Reboot alarm indicates that new software is booting on the TCC2/TCC2P. No action is required. The alarm clears when all cards finish rebooting the new software. The reboot takes up to 30 minutes.

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

**Note**

SYSBOOT is an informational alarm. It only requires troubleshooting if it does not clear.

2.7.421 TEMP-MISM

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

SONET Logical Object: NE

Temperature Reading Mismatch Between Control Cards is raised when the temperature readings on the two TCC2/TCC2Ps are out of range of each other by more than some predefined difference (such as 5 degrees C). A message containing power monitoring and temperature information is exchanged between the two TCC2/TCC2Ps, allowing the values to be compared. The temperature of each TCC2/TCC2P is read from a system variable.

This condition can be caused by a clogged fan filter or by fan tray stoppage.

Clear the TEMP-MISM Condition

-
- Step 1** Complete the [“Inspect, Clean, and Replace the Reusable Air Filter” procedure on page 2-286](#).
 - Step 2** If the condition does not clear, complete the [“Remove and Reinsert a Fan-Tray Assembly” procedure on page 2-287](#).
 - Step 3** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.422 TIM

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

SONET Logical Object: OCN

DWDM Logical Object: TRUNK

The Section TIM alarm occurs when the expected J0 section trace string does not match the received section trace string. This occurs because the data being received is not correct, and the receiving port could not be connected to the correct transmitter port.

If the alarm occurs on a port that has been operating with no alarms, the circuit path has changed due to a fiber misconnection, a TL1 routing change, or to someone entering an incorrect value in the Current Transmit String field.

TIM occurs on a port that has previously been operating without alarms if someone switches optical fibers that connect the ports. TIM is usually accompanied by other alarms, such as the [“LOS \(OCN\)” alarm on page 2-168](#) or the [“UNEQ-P” alarm on page 2-258](#). If these alarms accompany a TIM alarm, reattach or replace the original cables/fibers to clear the alarms. If a Transmit or Expected String was changed, restore the original string.

Clear the TIM Alarm

-
- Step 1** Ensure that the physical fibers are correctly configured and attached. To do this, consult site documents. For more information about cabling the ONS 15454, refer to the *“Install Cards and Fiber-Optic Cable”* chapter in the *Cisco ONS 15454 Procedure Guide*.
 - Step 2** If the alarm does not clear, you can compare the J0 expected and transmitted strings and, if necessary, change them:
 - a. Log into the circuit source node and click the **Circuits** tab.
 - b. Select the circuit reporting the condition, then click **Edit**.
 - c. In the Edit Circuit window, check the **Show Detailed Circuit Map** check box and click **Apply**.
 - d. On the detailed circuit map, right-click the source circuit port and choose **Edit J0 Path Trace (port)** from the shortcut menu.
 - e. Compare the Current Transmit String and the Current Expected String entries in the Edit J0 Path Trace dialog box.
 - f. If the strings differ, correct the Transmit or Expected strings and click **Apply**.
 - g. Click **Close**.
-

- Step 3** If the alarm does not clear, ensure that the signal has not been incorrectly routed. (Although the ONS 15454 routes circuits automatically, the circuit route could have been changed using TL1.) If necessary, manually correct the routing using TL1. For instructions, refer to the *Cisco ONS SONET TL1 Reference Guide* and the *Cisco ONS SONET TL1 Command Guide*.
- Step 4** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem if necessary.

2.7.423 TIM-MON

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

SONET Logical Object: OCN

DWDM Logical Object: TRUNK

The TIM Section Monitor TIM alarm is similar to the “TIM-P” alarm on page 2-251, but it applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards when they are configured in transparent mode. (In transparent termination mode, all SONET overhead bytes are passed through from client ports to the trunk ports or from trunk ports to client ports.)



Note

For more information about MXP and TXP cards, refer to the *Cisco ONS 15454 DWDM Reference Manual*.

Clear the TIM-MON Alarm

- Step 1** Complete the “Clear the TIM-P Alarm” procedure on page 2-252.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

2.7.424 TIM-P

Default Severity: Critical (CR), Service-Affecting (SA) for STSTRM; Default Severity: Minor (MN), Non-Service-Affecting (NSA) for STSMON

SONET Logical Objects: STSMON, STSTRM

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

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

Clear the TIM-P Alarm

- Step 1** Complete the “[Clear the TIM Alarm](#)” procedure on page 2-250. (The option will say “Edit J1 Path Trace” rather than “Edit J0 Path Trace.”)
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447. If the alarm applies to the STSTRM object, it is Service-Affecting (SA).


Note

When you perform an upgrade from a previous release to Release 9.0, with one-way multiple drops circuit, J1-path traces needs to be re-configured for one-way multiple drops circuits. In Release 9.0, configuring of same J1-path trace mode or same expected string for all the drop points is supported.

The information given below is valid for all the STS one-way multiple drop points on all the cards.


Note

- In Release 9.0, configuring of same J1-path trace mode or same expected string for all the drop points is supported for one-way multiple drop points. When you change the J1-path trace mode or the same expected string for one drop, the same J1-path trace gets copied to all drop points, which support all the J1 path traces.
- In Release 9.0, all the one-way multiple drops circuit have same J1-path trace parameters. and when a new drop point is added, which supports J1-path trace, the first drop point J1-path trace parameters get copied to a new drop point.
- With a circuit between two nodes, if the J1-path trace mode or the expected string is changed for trunk port of source node, the same J1-path trace mode or expected string gets copied to the remaining drop points of the source node.
- However, when the J1-path trace mode or expected string is changed for trunk port of destination node, the same J1-path trace mode or expected string does not get copied to the drop points of the destination node.

2.7.425 TIM-S

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

SONET Logical Objects: EC1, OCN

The TIM for Section Overhead alarm occurs when there is a mismatch between the expected and received J0 section overhead strings in either Manual or Auto mode.

In manual mode at the DS3/EC1-48 card Section Trace window, the user enters 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-S 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 problem.

TIM-S also occurs on a port that has previously been operating without alarms if someone switches the cables or optical fibers that connect the ports. If TIM-S is enabled on the port, the “AIS-L” alarm on page 2-38 can be raised downstream and the “RFI-L” alarm on page 2-210 can be raised upstream.

**Note**

AIS-L and RFI-L are disabled or enabled in the **Provisioning > EC1 > Section Trace** tab **Disable AIS/RDI on TIM-S?** check box.

Clear the TIM-S Alarm

-
- Step 1** Double-click the DS3/EC1-48 card to open the card view.
 - Step 2** Click the **Provisioning > EC1 > Section Trace** tabs.
 - Step 3** Choose the port from the **Port** pull-down.
 - Step 4** In the Expected area, enter the correct string into the **Current Expected String** field.
 - Step 5** Click **Apply**.
 - Step 6** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447. If the alarm applies to the STSTRM object, it is Service-Affecting (SA).
-

2.7.426 TIM-V

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

SONET Logical Object: VT-TERM, VT-MON

The VT Path TIM alarm is raised on VT terminations when the J2 path trace is enabled and is mismatched with the expected trace string.

Clear the TIM-V Alarm

-
- Step 1** Complete the “[Clear the TIM Alarm](#)” procedure on page 2-250.
 - Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 to report a Service-Affecting (SA) problem.
-

2.7.427 TPTFAIL (CEMR, CE100T, CE1000)

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

SONET Logical Objects: CEMR, CE100T, CE1000

The Transport (TPT) Layer Failure alarm for the CE-Series card indicates a break in the end-to-end Ethernet link integrity feature of the card. TPTFAIL indicates a far-end condition and not a problem with the port reporting TPTFAIL.

**Note**

For more information about Ethernet cards, refer to the Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.

Clear the TPTFAIL (CEMR, CE100T, CE1000) Alarm

-
- Step 1** Complete the [“Clear the TPTFAIL \(G1000\) Alarm” procedure on page 2-255](#).
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 to report a Service-Affecting (SA) problem.
-

2.7.428 TPTFAIL (FCMR)

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

SONET Logical Object: FCMR

The Transport Fail alarm is raised against a local Fibre Channel (FC) port on an FC_MR-4 card when the port receives another SONET error such as the [“AIS-P” alarm on page 2-39](#), the [“LOP-P” alarm on page 2-158](#); [“UNEQ-P” alarm on page 2-258](#), the [“PLM-P” alarm on page 2-200](#), the [“TIM-P” alarm on page 2-251](#), the [“LOM” alarm on page 2-158](#) (for VCAT only), or the [“SQM” alarm on page 2-237](#) (for VCAT only).

This TPTFAIL can be raised against Fibre Channel cards if the remote FC card port is down from SIGLOSS or SYNCLOSS. In that case, the remote FC card port sends a PDI-P error code in the SONET C2 byte and signals the local FC port transmitter to turn off (thus causing the local FC port to raise the TPTFAIL alarm). A TPTFAIL can also be raised when a far-end receive fiber is pulled. This alarm can be demoted when a facility loopback is placed on the FC_MR-4 port.

Clear the TPTFAIL (FCMR) Alarm

-
- Step 1** Find and clear any path alarms applying to the port. Refer to the correct section of this chapter for trouble clearing instructions. Clearing the path alarm also clears the TPTFAIL.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.
-

2.7.429 TPTFAIL (G1000)

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

SONET Logical Object: G1000

The Transport Layer Failure alarm for the G-Series Ethernet card indicates a break in the end-to-end Ethernet link integrity feature of the ONS 15454 G1000-4 cards. TPTFAIL indicates a far-end condition and not a problem with the port reporting TPTFAIL.

The TPTFAIL alarm indicates a problem on either the SONET path or the remote Ethernet port that prevents the complete end-to-end Ethernet path from working. If any SONET path alarms such as the “AIS-P” alarm on page 2-39, the “LOP-P” alarm on page 2-158, the “PDI-P” alarm on page 2-198, or the “UNEQ-P” alarm on page 2-258 exist on the SONET path used by the Ethernet port, the affected port causes a TPTFAIL alarm. Also, if the far-end G1000-4 port Ethernet port is administratively disabled or it is reporting the “CARLOSS (G1000)” alarm on page 2-64, the C2 byte in the SONET path overhead indicates the “PDI-P” alarm on page 2-198, which in turn causes a TPTFAIL to be reported against the near-end port.

When a TPTFAIL alarm occurs, the near-end port is automatically disabled (transmit laser turned off). In turn, the laser shutoff can also cause the external Ethernet device attached at the near end to detect a link down and turn off its transmitter. This also causes a CARLOSS alarm to occur on the reporting port. In all cases, the source problem is either in the SONET path being used by the G1000-4 port or the far-end G1000-4 port to which it is mapped.

An occurrence of TPTFAIL on an ONS 15454 G1000-4 port indicates either a problem with the SONET path that the port is using or with the far-end G1000-4 port that is mapped to the port.

**Note**

For more information about Ethernet cards, refer to the Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.

Clear the TPTFAIL (G1000) Alarm

-
- Step 1** Clear any alarms being reported by the OC-N card on the G1000-4 circuit.
 - Step 2** If no alarms are reported by the OC-N card, or if the “PDI-P” condition on page 2-198 is reported, the problem could be on the far-end G1000-4 port. Clear any alarms, such as CARLOSS, reported against the far-end port or card.
 - Step 3** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.
-

2.7.430 TPTFAIL (ML100T, ML1000, MLFX)

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

SONET Logical Objects: ML100T, ML1000, MLFX

The TPT Layer Failure alarm for the ML-Series Ethernet card indicates a break in the end-to-end packet-over-SONET (POS) link integrity feature of the ML-Series POS cards. TPTFAIL indicates a far-end condition or misconfiguration of the POS port.

The TPTFAIL alarm indicates a problem on the SONET path, a problem on the remote POS port, or a misconfiguration of the POS port that prevents the complete end-to-end POS path from working. If any SONET path alarms such as the “AIS-P” condition on page 2-39, the “LOP-P” alarm on page 2-158, the “PDI-P” condition on page 2-198, or the “UNEQ-P” alarm on page 2-258 exist on the circuit used by the POS port, the affected port could report a TPTFAIL alarm. If the far-end ML POS port is administratively disabled, it inserts an “AIS-P” condition on page 2-39 that is detected by the near-end port. The near-end port could report TPTFAIL in this event. If the POS port is misconfigured at the Cisco IOS CLI level, the misconfiguration causes the port to go down and report TPTFAIL.

**Note**

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

Clear the TPTFAIL (ML100T, ML1000, MLFX) Alarm

-
- Step 1** If there are no SONET alarms reported against the POS port circuit, verify that both POS ports are properly configured. Refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327* for configuration information.
- Step 2** If the “PLM-P” alarm on page 2-200 is the only one reported against the POS port circuit, verify that both POS ports are properly configured. Refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327* for configuration information.
- Step 3** If the “PDI-P” condition on page 2-198 is the only one reported against the POS port circuit and the circuit is terminated by a G-Series card, determine whether a “CARLOSS (G1000)” alarm on page 2-64 is reported against the G-Series card, and if so, complete the “Clear the CARLOSS (G1000) Alarm” procedure on page 2-65.
- Step 4** If the “AIS-P” alarm on page 2-39, the “LOP-P” alarm on page 2-158, or the “UNEQ-P” alarm on page 2-258 is present, clear those alarms using the procedures in those sections.
- Step 5** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.
-

2.7.431 TRMT

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

SONET Logical Objects: DS1, E1

A Missing Transmitter alarm occurs when there is a transmit failure on the ONS 15454 DS-1 card because of an internal hardware failure. The card must be replaced.

Clear the TRMT Alarm

-
- Step 1** Complete the “Physically Replace a Traffic Card” procedure on page 2-281 for the reporting DS-1 card.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.
-

2.7.432 TRMT-MISS

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

SONET Logical Objects: DS1, E1

A Facility Termination Equipment Transmitter Missing alarm occurs when the facility termination equipment detects an incorrect amount of impedance on its backplane connector. Incorrect impedance is detected when a transmit cable is missing on the DS-1 port or the backplane does not match the inserted card. For example, an SMB connector or a BNC connector could be connected to a DS-1 card instead of a DS-3 card.



Note

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

Clear the TRMT-MISS Alarm

-
- Step 1** Verify that the device attached to the DS-1 port is operational.
 - Step 2** If the device is operational, verify that the cabling is securely connected.
 - Step 3** If the cabling is secure, verify that the pinouts are correct.
 - Step 4** If the pinouts are correct, replace the transmit cable.
 - Step 5** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.
-

2.7.433 TX-AIS

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

SONET Logical Objects: DS1, DS3, E1

The (TX) Transmit Direction AIS condition is raised by the ONS 15454 backplane when it receives a far-end DS-1 LOS.

Clear the TX-AIS Condition

-
- Step 1** Determine whether there are alarms on the downstream nodes and equipment, especially the “**LOS (OCN)**” alarm on page 2-168, or OOS ports.
 - Step 2** Clear the downstream alarms using the applicable procedures in this chapter.
 - Step 3** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.434 TX-LOF

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

SONET Logical Objects: DS1, E1

The Transmit Direction LOF condition is transmitted by the backplane when it receives a DS-1 TX-LOF.

This alarm is raised only at the transmit (egress) side.

Clear the TX-LOF Condition

-
- Step 1** Complete the [“Clear the LOF \(DS1\) Alarm” procedure on page 2-152](#).
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.435 TX-RAI

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

SONET Logical Objects: DS1, DS3, E1

The Transmit Direction RAI condition is transmitted by the backplane when it receives a DS-1 TX-AIS. This alarm is raised only at the transmit side, but RAI is raised at both ends.



Note

The DS1-56 card operating in retiming mode reports a Transmit Condition remote alarm indication (TX-RAI) alarm in the alarm log. However, the physical signal that is transmitted out does not have TX-RAI in the frame. Hence, TX-RAI is not transmitted in the DS1 signal. This causes the client equipment not to detect TX-RAI in the incoming signal.

Clear the TX-RAI Condition

-
- Step 1** Complete the [“Clear the TX-AIS Condition” procedure on page 2-257](#).
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.436 UNC-WORD

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.437 UNEQ-P

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

SONET Logical Objects: STSMON, STSTRM

An SLMF UNEQ Path alarm occurs when the path does not have a valid sender. The UNEQ-P indicator is carried in the C2 signal path byte in the SONET overhead. The source of the problem is the node that is transmitting the signal into the node reporting the UNEQ-P.

The alarm could result from a PARTIAL circuit or an empty VT tunnel. UNEQ-P occurs in the node that terminates a path.

**Note**

If a newly created circuit has no signal, a UNEQ-P alarm is reported on the OC-N cards and the “AIS-P” condition on page 2-39 is reported on the terminating cards. These alarms clear when the circuit carries a signal.

**Caution**

Deleting a circuit affects traffic.

Clear the UNEQ-P Alarm

- Step 1** In node view, choose **Go to Network View from the View menu**.
- Step 2** Right-click the alarm to display the Select Affected Circuits shortcut menu.
- Step 3** Click **Select Affected Circuits**.
- Step 4** When the affected circuits appear, look in the Type column for VTT, which indicates a VT tunnel circuit. A VT tunnel with no VTs assigned could be the cause of an UNEQ-P alarm.
- Step 5** If the Type column does not contain VTT, there are no VT tunnels connected with the alarm. Go to [Step 7](#).
- Step 6** If the Type column does contain VTT, attempt to delete these rows:

**Note**

The node does not allow you to delete a valid VT tunnel or one with a valid VT circuit inside.

- a. Click the VT tunnel circuit row to highlight it. Complete the “[Delete a Circuit](#)” procedure on page 2-283.
- b. If an error message dialog box appears, the VT tunnel is valid and not the cause of the alarm.
- c. If any other rows contain VTT, repeat [Step 6](#).
- Step 7** If all nodes in the ring appear in the CTC network view, determine whether the circuits are complete:
 - a. Click the **Circuits** tab.
 - b. Verify that PARTIAL is not listed in the Status column of any circuits.
- Step 8** If you find circuits listed as PARTIAL, use an optical test set to verify that these circuits are not working circuits that continue to pass traffic. For specific procedures to use the test set equipment, consult the manufacturer.
- Step 9** If the PARTIAL circuits are not needed or are not passing traffic, delete the PARTIAL circuits. Complete the “[Delete a Circuit](#)” procedure on page 2-283.
- Step 10** Recreate the circuit with the correct circuit size. Refer to the “Create Circuits and VT Tunnels” chapter in the *Cisco ONS 15454 Procedure Guide*.
- Step 11** Log back in and verify that all circuits terminating in the reporting card are active:
 - a. Click the **Circuits** tab.
 - b. Verify that the **Status** column lists all circuits as active.

- Step 12** If the alarm does not clear, clean the far-end optical fiber according to site practice. If no site practice exists, complete the procedure in the “Maintain the Node” chapter of the *Cisco ONS 15454 Procedure Guide*.

**Warning**

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

**Warning**

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

**Warning**

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

**Caution**

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

- Step 13** If the alarm does not clear, complete the [“Physically Replace a Traffic Card” procedure on page 2-281](#) for the OC-N and electrical cards.
- Step 14** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.

2.7.438 UNEQ-V

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

SONET Logical Objects: VT-MON, VT-TERM

An SLMF UNEQ VT alarm indicates that the node is receiving SONET path overhead with Bits 5, 6, and 7 of the V5 overhead byte all set to zeroes. The source of the problem is not the node raising the alarm, but the node transmitting the VT signal to it. The V in UNEQ-V indicates that the failure has occurred at the VT layer.

**Warning**

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

**Warning**

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

**Warning**

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

Clear the UNEQ-V Alarm

Step 1 Complete the “[Clear the UNEQ-P Alarm](#)” procedure on page 2-259.

**Caution**

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

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

2.7.439 UNQUAL-PPM

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

SONET Logical Objects: PPM

The Unqualified PPM Inserted condition occurs when a PPM with a nonqualified product ID is plugged into the card's port; that is, the PPM passes the security code check as a Cisco PPM but is not qualified for use on the particular card.

Clear the UNQUAL-PPM Condition

Step 1 Obtain the correct Cisco PPM and replace the existing PPM with the new one.

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

2.7.440 UT-COMM-FAIL

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.441 UT-FAIL

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.442 VCG-DEG

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

SONET Logical Object: VCG

The VCAT Group Degraded alarm is a VCAT group alarm. (VCATs are groups of independent circuits that are concatenated from different time slots into higher-rate signals.) The alarm occurs when one member circuit carried by the ML-Series Ethernet card is down. This alarm is accompanied by the “[OOU-TPT](#)” alarm on page 2-195. It only occurs when a Critical (CR) alarm, such as LOS, causes a signal loss.



Note

For more information about Ethernet cards, refer to the Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.

Clear the VCG-DEG Condition

- Step 1** Look for and clear any Critical (CR) alarms that apply to the errored card, such as the “[LOS \(2R\)](#)” alarm on page 2-161 or “[LOS \(OTS\)](#)” alarm on page 2-170.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

2.7.443 VCG-DOWN

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

SONET Logical Object: VCG

The VCAT Group Down alarm is a VCAT group alarm. (VCATs are groups of independent circuits that are concatenated from different time slots into higher-rate signals.) The alarm occurs when one or more member circuits carried by an ML-Series or CE-Series Ethernet card are down. This alarm occurs in conjunction with another Critical (CR) alarm, such as the “[LOS \(2R\)](#)” alarm on page 2-161.



Note

If LCAS (Link Capacity Adjustment Scheme) is not enabled, the VCAT group transitions to the down state with even a single member down. If SW-LCAS is enabled on the VCAT group for ML1 cards, or HW LCAS is enabled for CE cards, the VCAT group transitions to the VCG-DOWN state only when all the members are down. The presence of at least one working member causes the VCAT group to remain in VCG-DEG (VCG degraded) state.

**Note**

For more information about Ethernet cards, refer to the Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.

Clear the VCG-DOWN Condition

-
- Step 1** Complete the [“Clear the VCG-DEG Condition” procedure on page 2-262](#).
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.
-

2.7.444 VLAN-AIS

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

SONET Logical Object: ETH

The Virtual Lan Alarm Indication Signal alarm summarizes the presence of VLAN-X-AIS alarms on the facility. The card raises this alarm when the first VLAN-X-AIS (X = Vlan ID) condition is raised on the facility.

The VLAN-X-AIS indicates that the VLAN X is lost and the AIS defect is received.

Clear the VLAN-AIS Condition

Clear the last VLAN-X-AIS alarm on the port to clear this alarm.

2.7.445 VOA-DISABLED

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

SONET Logical Object: EQPT

The VOA Disabled alarm indicates that the VOA control loop is disabled due to excessive counter-propagation light.

Clear the VOA-DISABLED Condition

-
- Step 1** Complete the [“Physically Replace a Traffic Card” procedure on page 2-281](#) for the alarmed card.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.446 VOA-HDEG

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.447 VOA-HFAIL

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.448 VOA-LDEG

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.449 VOA-LFAIL

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.450 VOLT-MISM

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

SONET Logical Object: PWR

The Power Monitoring Mismatch Between Control Cards alarm is raised against the shelf when the power voltages of both TCC2/TCC2Ps are out of range of each other by more than 5 VDC.

Clear the VOLT-MISM Condition

-
- | | |
|---------------|---|
| Step 1 | Check the incoming voltage level to the shelf using a voltmeter. Follow site practices or refer to the “Install the Shelf and Backplane Cable” chapter in the <i>Cisco ONS 15454 Procedure Guide</i> for power installation procedures. |
| Step 2 | Correct any incoming voltage issues. |
| Step 3 | If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC 1 800 553-2447. |
-

2.7.451 VT-SQUELCH-L

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

SONET Logical Object: OCN

The Ring is Squelching VT Traffic condition is raised on an OC-N facility. If the node failure scenario includes the source node, the node dropping VT will squelch VT traffic. The condition resolves when the node failure is recovered.

This condition is raised as NA severity by default. However, it indicates that traffic is squelched due to node failure, that is, traffic outage. Traffic outage can be caused by different problems, such as multiple instances of the “LOS (OCN)” alarm on page 2-168, the “AIS-L” condition on page 2-38, or node power outage. VT-SQUELCH-L is symptomatic and indicates that the user must investigate which node in a ring is being isolated and what causes node isolation.



Note

VT-SQUELCH-L is an informational condition.

2.7.452 WIZARD-IS-RUNNING

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

SONET Logical Objects: OTS

The OPT-RAMP-C (Raman Pump) board installation requires the execution of a wizard, launched through CTC, to tune the Raman amplification power. The wizard tunes more than one span, all the involved nodes, and raises the WIZARD-IS-RUNNING condition. The condition signifies that the tuning procedure is currently in place.

Clear the WIZARD-IS-RUNNING Condition

-
- Step 1** The WIZARD-IS-RUNNING condition clears when the wizard stops.
- Step 2** If the condition does not clear, log into the Cisco Technical Support Website at <http://www.cisco.com/techsupport> for more information or log into <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml> to obtain a directory of toll-free Technical Support numbers for your country.
-

2.7.453 WKSWPR

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

SONET Logical Objects: EQPT, OCN, STSMON, VT-MON

DWDM Logical Objects: 2R, ESCON, FC, GE, ISC

The Working Switched To Protection condition occurs when a line experiences the “LOS (OCN)” alarm on page 2-168, the “SD (DS1, DS3)” condition on page 2-223, or the “SD (TRUNK)” condition on page 2-226.

This condition is also raised when you use the Manual Switch, APS Switch, FORCE SPAN, FORCE RING or MANUAL SPAN command at the network level. WKSWPR is visible on the network view Alarms, Conditions, and History tabs.

Clear the WKSWPR Condition

-
- Step 1** Complete the [“Clear the LOS \(OCN\) Alarm” procedure on page 2-169](#).
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

2.7.454 WORK-QUEUE-FULL

Default Severity: Not Alarmed (NA)

Logical Object: EQPT

The Work Queue Full condition occurs when the netTask Queue in VxWorks has filled up and task operations for the card is postponed.

2.7.455 WTR

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

SONET Logical Objects: EC1, EQPT, ML1000, ML100T, MLFX, OCN, STSMON, VT-MON

DWDM Logical Objects: 2R, ESCON, FC, GE, ISC, TRUNK

The Wait To Restore condition for SONET and DWDM objects occurs when the [“WKSWPR” condition on page 2-265](#) is raised, but the wait-to-restore time has not expired, meaning that the active protect path cannot revert to the working path. The condition clears when the timer expires and traffic switches back to the working path.

If the condition is raised on an IEEE 802.17b-based RPR span, it indicates that the wait-to-restore timer is active after a span failure has cleared.



Caution

DS-1 traffic loss can occur on a DS-1 with 1:N protection if a DS-1 card is reset with the protect card in the WTR state.



Note

Generally, WTR is an informational condition and does not require troubleshooting.

Clear the WTR Condition on an IEEE 802.17b-Based RPR Span

-
- Step 1** Determine the setting for the IEEE 802.17b-based RPR interface’s WTR timer setting. In privileged executive mode, enter the following command:
- ```
router#show interface rpr protection
```
- View the WTR timer setting.
- Step 2** If the timer is set to “never,” clear the WTR condition by requesting a forced switch on the span. Enter the following command at the RPR-IEEE interface configuration mode command prompt:
- ```
router(config-if)#rpr-ieee protection request force-switch {east | west}
```
- Step 3** If you configured a FORCE on the span, clear the switch with the following command:

```
router(config-if)#no rpr-ieee protection request force-switch {east | west}
```

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

2.7.456 WVL-MISMATCH

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8 Traffic Card LED Activity

ONS 15454 traffic card LED behavior patterns are listed in the following sections. These sections give behavior for card insertion, reset, and side-switch.

2.8.1 Typical Traffic Card LED Activity After Insertion

When a card is inserted, the following LED activities occur:

1. The red FAIL LED turns on and remains illuminated for 20 to 30 seconds.
2. The red FAIL LED blinks for 35 to 45 seconds.
3. All LEDs blink once and turn off for 5 to 10 seconds.
4. The ACT or ACT/SBY LED turns on. The SF LED can persist until all card ports connect to their far-end counterparts and a signal is present.

2.8.2 Typical Traffic Card LED Activity During Reset

While a card resets, the following LED activities occur:

1. The FAIL LED on the physical card blinks and turns off.
2. The white LED with the letters “LDG” appears on the reset card in CTC.
3. The green ACT LED appears in CTC.

2.8.3 Typical Card LED State After Successful Reset

When a card successfully resets, the following LED states are present:

- If you are looking at the physical ONS 15454, the ACT/SBY LED is illuminated.
- If you are looking at node view of the ONS 15454, the current standby card has an amber LED depiction with the initials “SBY,” and this has replaced the white “LDG” depiction on the card in CTC.
- If you are looking at node view of the ONS 15454, the current active card has a green LED depiction with the initials “ACT,” and this has replaced the white “LDG” depiction on the card in CTC.

2.8.4 Typical Cross-Connect LED Activity During Side Switch

When a XC10G card is switched in CTC from active (ACT) to standby (SBY) or from SBY to ACT, the following LED activities occur:

1. The FAIL LED on the physical card blinks and turns off.
2. The standby card yellow SBY LED becomes a green ACT LED, indicating it is now active.
3. The active card green ACT LED becomes a yellow SBY LED, indicating it is now standby.

2.9 Frequently Used Alarm Troubleshooting Procedures

This section gives common procedures that are frequently used when troubleshooting alarms. Most of these procedures are summarized versions of fuller procedures existing elsewhere in the ONS 15454 documentation. They are included in this chapter for the user's convenience. For further information, please refer to the *Cisco ONS 15454 Procedure Guide*.

2.9.1 Node and Ring Identification, Change, Visibility, and Termination

The following procedures relate how to identify or change BLSR names and node IDs, and how to verify visibility from other nodes.

Identify a BLSR Ring Name or Node ID Number

-
- | | |
|---------------|--|
| Step 1 | Log into a node on the network. |
| Step 2 | In node view, choose Go to Network View from the View menu . |
| Step 3 | Click the Provisioning > BLSR tabs. |
| Step 4 | From the Ring Name column, record the ring name, or in the Nodes column, record the Node IDs in the BLSR. The Node IDs are the numbers in parentheses next to the node name. |
-

Change a BLSR Ring Name

-
- | | |
|---------------|---|
| Step 1 | Log into a node on the network. |
| Step 2 | In node view, choose Go to Network View from the View menu . |
| Step 3 | Click the Provisioning > BLSR tabs. |
| Step 4 | Highlight the ring and click Edit . |
| Step 5 | In the BLSR window, enter the new name in the Ring Name field. |
| Step 6 | Click Apply . |
| Step 7 | Click Yes in the Changing Ring Name dialog box. |
-

Change a BLSR Node ID Number

-
- Step 1** Log into a node on the network.
 - Step 2** In node view, choose **Go to Network View from the View menu**.
 - Step 3** Click the **Provisioning > BLSR** tabs.
 - Step 4** Highlight the ring and click **Edit**.
 - Step 5** In the BLSR window, right-click the node on the ring map.
 - Step 6** Select **Set Node ID** from the shortcut menu.
 - Step 7** In the Edit Node ID dialog box, enter the new ID. The Node ID is the number in parentheses after the Node Name.
 - Step 8** Click **OK**.
-

Verify Node Visibility for Other Nodes

-
- Step 1** Log into a node on the network.
 - Step 2** In node view, click the **Provisioning > BLSR** tabs.
 - Step 3** Highlight a BLSR.
 - Step 4** Click **Ring Map**.
 - Step 5** In the BLSR Ring Map window, verify that each node in the ring appears on the ring map with a node ID and IP address.
 - Step 6** Click **Close**.
-

2.9.2 Protection Switching, Lock Initiation, and Clearing

The following sections give instructions for port, ring, and span switching and switch-clearing commands, as well as lock-ons and lockouts.

Initiate a 1+1 Force Switch Command

This procedure switches 1+1 protection group traffic from one port in the group to the other using a Force switch.



Caution

The Force command overrides normal protective switching mechanisms. Applying this command incorrectly can cause traffic outages.



Caution

Traffic is not protected during a Force protection switch.

**Note**

A Force command switches traffic on a working path even if the path has signal degrade (SD) or signal fail (SF) conditions. A Force switch does not switch traffic on a protect path. A Force switch preempts a Manual switch.

-
- Step 1** In node view, click the **Maintenance > Protection** tabs.
- Step 2** In the Protection Groups area, select the protection group with the port you want to switch.
- Step 3** In the Selected Groups area, select the port belonging to the card you are replacing. You can carry out this command for the working or protect port. For example, if you need to replace the card with the Protect/Standby port, click this port.
- Step 4** In the Switch Commands area, click **Force**.
- Step 5** Click **Yes** in the Confirm Force Operation dialog box.
- Step 6** If the switch is successful, the group says “Force to working” in the Selected Groups area.
-

Initiate a 1+1 Manual Switch Command

This procedure switches 1+1 protection group traffic from one port in the group to the other using a Manual switch.

**Note**

A Manual command switches traffic if the path has an error rate less than the signal degrade. A Manual switch is preempted by a Force switch.

-
- Step 1** In node view, click the **Maintenance > Protection** tabs.
- Step 2** In the Protection Groups area, select the protection group with the port you want to switch.
- Step 3** In the Selected Groups area, select the port belonging to the card you are replacing. You can carry out this command for the working or protect port. For example, if you need to replace the card with the protect/standby port, click this port.
- Step 4** In the Switch Commands area, click **Manual**.
- Step 5** Click **Yes** in the Confirm Force Operation dialog box.
- Step 6** If the switch is successful, the group now says “Manual to working” in the Selected Groups area.
-

Clear a 1+1 Force or Manual Switch Command

**Note**

If the 1+1 protection group is configured as revertive, clearing a Force switch to protect (or working) moves traffic back to the working port. In revertive operation, the traffic always switches back to working. There is no revert to the protect. If ports are not configured as revertive, clearing a Force switch to protect does not move traffic back.

**Note**

If the Force Switch was user-initiated, the reversion occurs immediately when the clear command is issued. The five-minute WTR period is not needed in this case. If the Force was system-initiated, allow the five-minute waiting period (during WTR) before the reversion occurs.

-
- Step 1** In node view, click the **Maintenance > Protection** tabs.
- Step 2** In the Protection Groups area, choose the protection group containing the port you want to clear.
- Step 3** In the Selected Group area, choose the port you want to clear.
- Step 4** In the Switching Commands area, click **Clear**.
- Step 5** Click **Yes** in the Confirmation Dialog box.
- The Force switch is cleared. Traffic immediately reverts to the working port if the group was configured for revertive switching.
-

Initiate a Lock-On Command

**Note**

For 1:1 and 1:N electrical protection groups, working or protect cards can be placed in the Lock On state. For a 1+1 optical protection group, only the working port can be placed in the Lock On state.

-
- Step 1** In node view, click the **Maintenance > Protection** tabs.
- Step 2** In the Protection Groups list, click the protection group where you want to apply a lock-on.
- Step 3** If you determine that the protect card is in standby mode and you want to apply the lock-on to the protect card, make the protect card active if necessary:
- a. In the Selected Group list, click the protect card.
 - b. In the Switch Commands area, click **Force**.
- Step 4** In the Selected Group list, click the active card where you want to lock traffic.
- Step 5** In the Inhibit Switching area, click **Lock On**.
- Step 6** Click **Yes** in the confirmation dialog box.
-

Initiate a Card or Port Lockout Command

**Note**

For 1:1 or 1:N electrical protection groups, working or protect cards can be placed in the Lock Out state. For a 1+1 optical protection group, only the protect port can be placed in the Lock Out state.

-
- Step 1** In node view, click the **Maintenance > Protection** tabs.
- Step 2** In the Protection Groups list, click the protection group that contains the card you want to lockout.
- Step 3** In the Selected Group list, click the card where you want to lock out traffic.

- Step 4** In the Inhibit Switching area, click **Lock Out**.
- Step 5** Click **Yes** in the confirmation dialog box.
- The lockout has been applied and traffic is switched to the opposite card.
-

Clear a Lock-On or Lockout Command

- Step 1** In node view, click the **Maintenance > Protection** tabs.
- Step 2** In the Protection Groups list, click the protection group that contains the card you want to clear.
- Step 3** In the Selected Group list, click the card you want to clear.
- Step 4** In the Inhibit Switching area, click **Unlock**.
- Step 5** Click **Yes** in the confirmation dialog box.
- The lock-on or lockout is cleared.
-

Initiate a 1:1 Card Switch Command



Note

The Switch command only works on the Active card, whether it is working or protect. It does not work on the Standby card.

- Step 1** In node view, click the **Maintenance > Protection** tabs.
- Step 2** Click the protection group that contains the card you want to switch.
- Step 3** Under Selected Group, click the active card.
- Step 4** Next to Switch Commands, click **Switch**.
- The working slot should change to Working/Active and the protect slot should change to Protect/Standby.
-

Initiate a Force Switch for All Circuits on a Path Protection Span

This procedure forces all circuits in a path protection configuration from the working span to the protect. It is used to remove traffic from a card that originates or terminates path protection circuits.



Caution

The Force command overrides normal protective switching mechanisms. Applying this command incorrectly can cause traffic outages.



Caution

Traffic is not protected during a Force protection switch.

-
- Step 1** Log into a node on the network.
- Step 2** In node view, choose **Go to Network View from the View menu**.
- Step 3** Right-click a network span and choose **Circuits**.
The Circuits on Span dialog box shows the path protection circuits, including circuit names, locations, and a color code showing which circuits are active on the span.
- Step 4** Click the **Perform Path Protection span switching** field.
- Step 5** Choose **Force Switch Away** from the drop-down list.
- Step 6** Click **Apply**.
- Step 7** In the Confirm Path Protection Switch dialog box, click **Yes**.
- Step 8** In the Protection Switch Result dialog box, click **OK**.
In the Circuits on Span dialog box, the switch state for all circuits is FORCE. Unprotected circuits do not switch.
-

Initiate a Manual Switch for All Circuits on a Path Protection Span

This procedure manually switches all circuits in a path protection configuration from the working span to the protect. It is used to remove traffic from a card that originates or terminates path protection circuits.



Caution

The Manual command does not override normal protective switching mechanisms.

-
- Step 1** Log into a node on the network.
- Step 2** Right-click a network span and choose **Circuits**.
The Circuits on Span dialog box shows the path protection circuits, including circuit names, locations, and a color code showing which circuits are active on the span.
- Step 3** Click the **Perform Path Protection span switching** field.
- Step 4** Choose **Manual** from the drop-down list.
- Step 5** Click **Apply**.
- Step 6** In the Confirm Path Protection Switch dialog box, click **Yes**.
- Step 7** In the Protection Switch Result dialog box, click **OK**.
In the Circuits on Span dialog box, the switch state for all circuits is Manual. Unprotected circuits do not switch.
-

Initiate a Lockout for All Circuits on a Protect Path Protection Span

This procedure prevents all circuits in a path protection working span from switching to the protect span. It is used to keep traffic off cards that originate or terminate path protection circuits.

**Caution**

The Lock Out of Protect command overrides normal protective switching mechanisms.

-
- Step 1** Log into a node on the network. If you are already logged in, continue with [Step 2](#).
- Step 2** Right-click a network span and choose **Circuits**.
The Circuits on Span dialog box shows the path protection circuits, including circuit names, locations, and a color code showing which circuits are active on the span.
- Step 3** Click the **Perform Path Protection span switching** field.
- Step 4** Choose **Lock Out of Protect** from the drop-down list.
- Step 5** Click **Apply**.
- Step 6** In the Confirm Path Protection Switch dialog box, click **Yes**.
- Step 7** In the Protection Switch Result dialog box, click **OK**.
In the Circuits on Span dialog box, the switch state for all circuits is LOCKOUT. Unprotected circuits do not switch.
-

Clear an External Switching Command on a Path Protection Span

**Note**

If the ports terminating a span are configured as revertive, clearing a Force or Manual switch to protect moves traffic back to the working port. If ports are not configured as nonrevertive, clearing a Force switch to protect does not move traffic back.

-
- Step 1** Log into a node on the network. If you are already logged in, continue with [Step 2](#).
- Step 2** Right-click a network span and choose **Circuits**.
The Circuits on Span dialog box shows the path protection circuits, including circuit names, locations, and a color code showing which circuits are active on the span.
- Step 3** Initiate a Force switch for all circuits on the span:
- Click the **Perform Path Protection span switching** field.
 - Choose **Clear** from the drop-down list.
 - Click **Apply**.
 - In the Confirm Path Protection Switch dialog box, click **Yes**.
 - In the Protection Switch Result dialog box, click **OK**.
In the Circuits on Span dialog box, the switch state for all circuits is Clear. Unprotected circuits do not switch.
-

Initiate a Force Ring Switch on a BLSR

-
- Step 1** Log into a node on the network. If you are already logged in, continue with [Step 2](#).

-
- Step 2** From the View menu choose **Go to Network View**.
 - Step 3** In network view, click the **Provisioning > BLSR** tabs.
 - Step 4** Click the row of the BLSR you are switching, then click **Edit**.
 - Step 5** Right-click a BLSR node west port and choose **Set West Protection Operation**.
 - Step 6** In the Set West Protection Operation dialog box, choose **Force Ring** from the drop-down list.
 - Step 7** Click **OK**.
 - Step 8** Click **Yes** in the two Confirm BLSR Operation dialog boxes that appear.
-

Initiate a Force Span Switch on a Four-Fiber BLSR

-
- Step 1** Log into a node on the network.
 - Step 2** From the View menu choose **Go to Network View**.
 - Step 3** In network view, click the **Provisioning > BLSR** tabs.
 - Step 4** Click the row of the BLSR you are switching, then click **Edit**.
 - Step 5** Right-click a BLSR node west port and choose **Set West Protection Operation**.
 - Step 6** In the Set West Protection Operation dialog box, choose **Force Span** from the drop-down list.
 - Step 7** Click **OK**.
 - Step 8** Click **Yes** in the two Confirm BLSR Operation dialog boxes that appear.
-

Initiate a Manual Span Switch on a BLSR

-
- Step 1** From the View menu, choose **Go to Network View**.
 - Step 2** Click the **Provisioning > BLSR** tabs.
 - Step 3** Choose the BLSR and click **Edit**.
 - Step 4** Right-click the BLSR node channel (port) and choose **Set West Protection Operation** (if you chose a west channel) or **Set East Protection Operation** (if you chose an east channel).
 - Step 5** In the Set West Protection Operation dialog box or the Set East Protection Operation dialog box, choose **Manual Span** from the drop-down list.
 - Step 6** Click **OK**.
 - Step 7** Click **Yes** in the two Confirm BLSR Operation dialog boxes.
-

Initiate a Manual Ring Switch on a BLSR

-
- Step 1** From the View menu, choose **Go to Network View**.
 - Step 2** Click the **Provisioning > BLSR** tabs.

- Step 3** Choose the BLSR and click **Edit**.
 - Step 4** Right-click the BLSR node channel (port) and choose **Set West Protection Operation** (if you chose a west channel) or **Set East Protection Operation** (if you chose an east channel).
 - Step 5** In the Set West Protection Operation dialog box or the Set East Protection Operation dialog box, choose **Manual Ring** from the drop-down list.
 - Step 6** Click **OK**.
 - Step 7** Click **Yes** in the two Confirm BLSR Operation dialog boxes.
-

Initiate a Lockout on a BLSR Protect Span

- Step 1** From the View menu choose **Go to Network View**.
 - Step 2** Click the **Provisioning > BLSR** tabs.
 - Step 3** Choose the BLSR and click **Edit**.
 - Step 4** Right-click the BLSR node channel (port) and choose **Set West Protection Operation** (if you chose a west channel) or **Set East Protection Operation** (if you chose an east channel).
 - Step 5** In the Set West Protection Operation dialog box or the Set East Protection Operation dialog box, choose **Lockout Protect Span** from the drop-down list.
 - Step 6** Click **OK**.
 - Step 7** Click **Yes** in the two Confirm BLSR Operation dialog boxes.
-

Initiate an Exercise Ring Switch on a BLSR

- Step 1** Log into a node on the network.
 - Step 2** Click **View > Go to Network View**.
 - Step 3** Click the **Provisioning > BLSR** tabs.
 - Step 4** Click the row of the BLSR you are exercising, then click **Edit**.
 - Step 5** Right-click the west port of a node and choose **Set West Protection Operation**.
 - Step 6** In the Set West Protection Operation dialog box, choose **Exercise Ring** from the drop-down list.
 - Step 7** Click **OK**.
 - Step 8** Click **Yes** in the Confirm BLSR Operation dialog box.
-

Initiate an Exercise Ring Switch on a Four Fiber BLSR

- Step 1** Log into a node on the network.
- Step 2** From the View menu, choose **Go to Network View**.
- Step 3** Click the **Provisioning > BLSR** tabs.

- Step 4** Click the row of the BLSR you are exercising, then click **Edit**.
 - Step 5** Right-click the west port of a node and choose **Set West Protection Operation**.
 - Step 6** In the Set West Protection Operation dialog box, choose **Exercise Span** from the drop-down list.
 - Step 7** Click **OK**.
 - Step 8** Click **Yes** in the Confirm BLSR Operation dialog box.
-

Clear a BLSR External Switching Command

- Step 1** Log into a node on the network.
 - Step 2** From the View menu, choose **Go to Network View**.
 - Step 3** Click the **Provisioning > BLSR** tabs.
 - Step 4** Click the BLSR you want to clear.
 - Step 5** Right-click the west port of the BLSR node where you invoked the switch and choose **Set West Protection Operation**.
 - Step 6** In the Set West Protection Operation dialog box, choose **Clear** from the drop-down list.
 - Step 7** Click **OK**.
 - Step 8** Click **Yes** in the Confirm BLSR Operation dialog box.
-

2.9.3 CTC Card Resetting and Switching

This section gives instructions for resetting traffic cards, TCC2/TCC2Ps, and cross-connect cards.



Caution

For TXP and MXP cards placed in a Y-cable protection group, do not perform a software reset on both cards simultaneously. Doing so will cause a traffic hit of more than one minute. For more information about Y-cable protection groups, refer to the *Cisco ONS 15454 DWDM Procedure Guide*.



Caution

Resetting the active card in a Y-cable group will cause a traffic outage if the standby card is down for any reason.



Note

When an AIC-I card is reset in CTC, any subsequent user client operations (such as CTC or TL1 activity) is paused for approximately 5-10 seconds. The reset does not cause any conditions to be raised.



Note

For more information about MXP and TXP cards, refer to the *Cisco ONS 15454 DWDM Reference Manual*.

Reset a Traffic Card in CTC

-
- Step 1** Log into a node on the network. If you are already logged in, continue with [Step 2](#).
- Step 2** In node view, position the cursor over the optical or electrical traffic card slot reporting the alarm.
- Step 3** Right-click the card. Choose **Reset Card** from the shortcut menu.
- Step 4** Click **Yes** in the Resetting Card dialog box.
-

Reset an Active TCC2/TCC2P Card and Activate the Standby Card



Caution

Resetting an active TCC2/TCC2P can be service-affecting.



Note

Before you reset the TCC2/TCC2P, you should wait at least 60 seconds after the last provisioning change you made to avoid losing any changes to the database.

-
- Step 1** Log into a node on the network. If you are already logged in, continue with [Step 2](#).
- Step 2** Identify the active TCC2/TCC2P:
- If you are looking at the physical ONS 15454 shelf, the ACT/SBY LED of the active card is green. The ACT/STBLY LED of the standby card is amber.
- Step 3** Right-click the active TCC2/TCC2P in CTC.
- Step 4** Choose **Reset Card** from the shortcut menu.
- Step 5** Click **Yes** in the Confirmation Dialog box.
- The card resets, the FAIL LED blinks on the physical card, and connection to the node is lost. CTC switches to network view.
- Step 6** Verify that the reset is complete and error-free and that no new related alarms appear in CTC. For LED appearance, see the [“2.8.3 Typical Card LED State After Successful Reset”](#) section on page 2-267.
- Step 7** Double-click the node and ensure that the reset TCC2/TCC2P is in standby mode and that the other TCC2/TCC2P is active. Verify the following:
- If you are looking at the physical ONS 15454 shelf, the ACT/SBY LED of the active card is green. The ACT/STBLY LED of the standby card is amber.
 - No new alarms appear in the Alarms window in CTC.
-

Side Switch the Active and Standby Cross-Connect Cards



Caution

The cross-connect card side switch is usually service-affecting.

Step 1 Log into a node on the network. For instructions regarding how to log into a node, refer *Cisco ONS 15454 Procedure Guide, Release 8.0*. If you are already logged in, continue with [Step 2](#).

Step 2 Display node view.

Step 3 Determine the active or standby XC10G card.

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



Note You can also position the cursor over the card graphic to display a popup identifying the card as active or standby.

Step 4 In node view, click the **Maintenance > Cross-Connect > Cards** tabs.

Step 5 Click **Switch**.

Step 6 Click **Yes** in the Confirm Switch dialog box. See the “[2.8.4 Typical Cross-Connect LED Activity During Side Switch](#)” section on page 2-268 for LED information.



Note During a maintenance side switch or soft reset of an active XC10G card, the 1+1 protection group might display a protection switch. To disallow the protection switch from being displayed, the protection group should be locked at the node where XC switch or soft reset of an active XC switch is in progress.



Caution Active cross connect (XC10G/XCVT) cards should not be physically removed.

The following rules must be followed for removing an Active Cross Connect Card (XC10G/XCVT):

If the active cross connect has to be removed, perform an XCVT/XC10G side switch to change the status of the card from active to standby and then remove the cross connect card once it goes back to standby.

OR

Perform a lockout on all circuits that originate from the node whose active cross connect card has to be removed (performing a lockout on all spans will also accomplish the same goal).

2.9.4 Physical Card Reseating, Resetting, and Replacement

This section gives instructions for physically reseating and replacing TCC2/TCC2P, cross-connect, and traffic cards.



Caution

Do not physically replace a card without first making provisions to switch or move traffic to a different card or circuit. General procedures for this are located in the “[2.9.2 Protection Switching, Lock Initiation, and Clearing](#)” section on page 2-269. In-depth traffic switching procedures and information can be found in the “Maintain the Node” chapter of the *Cisco ONS 15454 Procedure Guide*.

Remove and Reinsert (Reseat) the Standby TCC2/TCC2P Card


Caution

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


Caution

Do not perform this action without the supervision and direction of Cisco TAC 1 800 553-2447.


Caution

The TCC2/TCC2P reseat could be service-affecting. Refer to the [“2.9.2 Protection Switching, Lock Initiation, and Clearing” section on page 2-269](#) for traffic-switching procedures.


Note

Before you reset the TCC2/TCC2P, you should wait at least 60 seconds after the last provisioning change you made to avoid losing any changes to the database.


Note

When a standby TCC2/TCC2P card is removed and reinserted (reseated), all three fan lights could momentarily turn on, indicating that the fans have also reset.

Step 1

Log into a node on the network.

Ensure that the TCC2/TCC2P you want to reseat is in standby mode. A standby card has an amber ACT/SBY (Active/Standby) LED illuminated.

Step 2

When the TCC2/TCC2P is in standby mode, unlatch both the top and bottom ejectors on the TCC2/TCC2P.

Step 3

Physically pull the card at least partly out of the slot until the lighted LEDs turn off.

Step 4

Wait 30 seconds. Reinsert the card and close the ejectors.


Note

The TCC2/TCC2P requires several minutes to reboot and display the amber standby LED after rebooting. Refer to the *Cisco ONS 15454 Reference Manual* for more information about LED behavior during a card reboot.

Remove and Reinsert (Reseat) Any Card


Caution

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

Step 1

Open the card ejectors.

Step 2

Slide the card halfway out of the slot along the guide rails.

- Step 3** Slide the card all the way back into the slot along the guide rails.
- Step 4** Close the ejectors.
-

Physically Replace a Traffic Card

**Caution**

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

**Caution**

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Refer to the procedures in the [“2.9.2 Protection Switching, Lock Initiation, and Clearing” section on page 2-269](#). For more information, refer to the “Maintain the Node” chapter in the *Cisco ONS 15454 Procedure Guide*.

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

- Step 1** Open the card ejectors.
- Step 2** Slide the card out of the slot.
- Step 3** Open the ejectors on the replacement card.
- Step 4** Slide the replacement card into the slot along the guide rails.
- Step 5** Close the ejectors.
-

Physically Replace an In-Service Cross-Connect Card

**Caution**

The cross-connect reseal could be service-affecting. Refer to the [“2.9.2 Protection Switching, Lock Initiation, and Clearing” section on page 2-269](#) for traffic-switching procedures prior to completing this procedure.

**Note**

This procedure is placed in the chapter as a quick guide for the user’s convenience. A more detailed procedure is located in the “Maintain the Node” chapter of the *Cisco ONS 15454 Procedure Guide*.

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

- Step 1** Determine the active cross-connect card (XCVT/XC10G/XC-VXC-10G). The ACT/SBY LED of the active card is green. The ACT/SBY LED of the standby card is amber.

**Note**

You can also place the cursor over the card graphic to display a popup identifying the card as active or standby.

- Step 2** Switch the active cross-connect card to standby:
- In the node view, click the **Maintenance > Cross-Connect** tabs.
 - Under Cross Connect Cards, choose **Switch**.
 - Click **Yes** in the Confirm Switch dialog box.

**Note**

After the active cross-connect card becomes standby, the original standby slot becomes active. This causes the ACT/SBY LED to become green on the former standby card.

- Step 3** Physically remove the new standby cross-connect card from the ONS 15454.

**Note**

An improper removal (IMPROPRMVL) alarm is raised when a card reseal is performed, unless the card is first deleted in Cisco Transport Controller (CTC). The alarm clears after the card is replaced.

- Step 4** Insert the replacement cross-connect card into the empty slot.
- The replacement card boots up and becomes ready for service after approximately one minute.

2.9.5 Generic Signal and Circuit Procedures

This section gives instructions for verify BER thresholds, deleting circuits, provisioning SDCC terminations, and clearing loopbacks.

Verify the Signal BER Threshold Level

- Step 1** Log into a node on the network.
- Step 2** In node view, double-click the card reporting the alarm to open the card view.
- Step 3** Click the **Provisioning > Line** tabs.
- Step 4** Under the **SD BER** (or **SF BER**) column in the Provisioning window, verify that the cell entry is consistent with the originally provisioned threshold. The default setting is 1E-7.
- Step 5** If the entry is consistent with the original provisioning, go back to your original procedure.
- Step 6** If the entry is not consistent with what the system was originally provisioned for, click the cell to reveal the range of choices and click the original entry.
- Step 7** Click **Apply**.

Delete a Circuit

-
- Step 1** Log into a node on the network.
- Step 2** In node view, click the **Circuits** tab.
- Step 3** Click the circuit row to highlight it and click **Delete**.
- Step 4** Click **Yes** in the Delete Circuits dialog box.
-

Verify or Create Node Section DCC Terminations



Note Portions of this procedure are different for ONS 15454 DWDM nodes.

-
- Step 1** Log into a node on the network.
- Step 2** In node view, click the **Provisioning > Comm Channels > SDCC** tab.
- Step 3** View the Port column entries to see where terminations are present for a node. If terminations are missing, proceed to [Step 4](#).
- Step 4** If necessary, create a DCC termination:
- Click **Create**.
 - In the Create SDCC Terminations dialog box, click the ports where you want to create the DCC termination. To select more than one port, press the Shift key.
 - In the port state area, click the **Set to IS** radio button.
 - Verify that the Disable OSPF on Link check box is unchecked.
 - Click **OK**.
-

Clear an OC-N Card Facility or Terminal Loopback Circuit

-
- Step 1** Log into a node on the network.
- Step 2** Double-click the reporting card in CTC to open the card view.
- Step 3** Click the **Maintenance > Loopback > Port** tabs.
- Step 4** In the Loopback Type column, determine whether any port row shows a state other than None.
- Step 5** If a row contains another state besides None, click in the column cell to display the drop-down list and select None.
- Step 6** In the Admin State column, determine whether any port row shows a state other than IS.
- Step 7** If a row shows a state other than IS, click in the column cell to display the drop-down list and select **IS**.
- Step 8** Click **Apply**.

**Note**

If a port in the IS admin state does not receive a signal, the LOS alarm is raised and the port service state transitions to OOS-AU,FLT.

Clear an OC-N Card Cross-Connect (XC) Loopback Circuit

- Step 1** Log into a node on the network.
- Step 2** Double-click the reporting card in CTC to open the card view.
- Step 3** Click the **Maintenance > Loopback > SONET STS** tabs.
- Step 4** Uncheck the XC Loopback check box.
- Step 5** Click **Apply**.

Clear a DS3XM-6, DS3XM-12, or DS3E-12 Card Loopback Circuit

- Step 1** Log into a node on the network.
- Step 2** Double-click the reporting card in CTC to open the card view.
- Step 3** Click the **Maintenance > DS3** tabs or the **Maintenance > DS1** tabs.
- Step 4** In the Loopback Type column, determine whether any port row shows a state other than None.
- Step 5** If a row contains another state besides None, click in the column cell to display the drop-down list and select None.
- Step 6** In the Admin State column, determine whether any port row shows a state other than IS.
- Step 7** If a row shows a state other than IS, click in the column cell to display the drop-down list and select **IS**.
- Step 8** Click **Apply**.

**Note**

If a port in the IS admin state does not receive a signal, the LOS alarm is raised and the port service state transitions to OOS-AU,FLT.

Clear Other Electrical Card or Ethernet Card Loopbacks

**Note**

This procedure does not apply to DS3XM-6 or DS3XM-12 cards.

**Note**

For more information about Ethernet cards, refer to the Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.

-
- Step 1** Log into a node on the network.
- Step 2** Double-click the reporting card in CTC to open the card view.
- Step 3** Click the **Maintenance > Loopback** tabs.
- Step 4** In the Loopback Type column, determine whether any port row shows a state other than None.
- Step 5** If a row contains another state besides None, click in the column cell to display the drop-down list and select **None**.
- Step 6** In the Admin State column, determine whether any port row shows a state other than IS.
- Step 7** If a row shows a state other than IS, click in the column cell to display the drop-down list and select **IS**.
- Step 8** Click **Apply**.



Note If a port in the IS admin state does not receive a signal, the LOS alarm is raised and the port service state transitions to OOS-AU,FLT.

Clear an MXP, TXP, or FC_MR-4 Card Loopback Circuit

- Step 1** Log into a node on the network.
- Step 2** Double-click the reporting card in CTC to open the card view.
- Step 3** Click the **Maintenance > Loopback** tabs.
- Step 4** In the Loopback Type column, determine whether any port row shows a state other than None.
- Step 5** If a row contains another state besides None, click in the column cell to display the drop-down list and select None.
- Step 6** In the Admin State column, determine whether any port row shows an admin state other than IS, for example, OOS,MT.
- Step 7** If a row shows an admin state other than IS, click in the column cell to display the drop-down list and select **IS**.



Note If a port in the IS admin state does not receive a signal, the LOS alarm is raised and the port service state transitions to OOS-AU,FLT.

- Step 8** Click **Apply**.
-

2.9.6 Air Filter and Fan Procedures

This section gives instructions for cleaning or replacing the air filter and reseating or replacing the fan tray assembly.

Inspect, Clean, and Replace the Reusable Air Filter

To complete this task, you need a vacuum cleaner or detergent and water faucet, a spare filter, and a pinned hex key.



Warning

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

Although the filter works if it is installed with either side facing up, Cisco recommends that you install it with the metal bracing facing up to preserve the surface of the filter.



Caution

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

-
- Step 1** Verify that you are replacing a reusable air filter. The reusable filter is made of a gray, open-cell, polyurethane foam that is specially coated to provide fire and fungi resistance. NEBS 3E and later versions of the ONS 15454 use a reusable air filter.
- Step 2** If the air filter is installed in the external filter brackets, slide the filter out of the brackets while being careful not to dislodge any dust that could have collected on the filter. If the filter is installed beneath the fan tray and not in the external filter brackets, open and remove the front door assembly by completing the following steps:
- a. Open the front door of the shelf assembly by completing the following substeps. (If it is already open or if the shelf assembly does not have a front door, continue with [Step 3](#).)
 - Open the front door lock.
 - Press the door button to release the latch.
 - Swing the door open.
 - b. Remove the front door by completing the following substeps (optional):
 - Detach the ground strap from either the door or the chassis by removing one of the Kepnuts.
 - Place the Kepnut back on the stud after the ground strap is removed to avoid misplacement.
 - Secure the dangling end of the ground strap to the door or chassis with tape.
- Step 3** Push the outer side of the handles on the fan-tray assembly to expose the handles.
- Step 4** Pull the handles and slide the fan-tray assembly one inch (25.4 mm) out of the shelf assembly and wait until the fans stop.
- Step 5** When the fans have stopped, pull the fan-tray assembly completely out of the shelf assembly.
- Step 6** Gently remove the air filter from the shelf assembly. Be careful not to dislodge any dust that could have collected on the filter.
- Step 7** Visually inspect the air filter material for dirt and dust.
- Step 8** If the reusable air filter has a concentration of dirt and dust, either vacuum or wash the air filter. Prior to washing the air filter, replace the dirty air filter with a clean air filter and also reinsert the fan-tray assembly. Wash the dirty air filter under a faucet with a light detergent.
- Spare ONS 15454 filters should be kept in stock for this purpose.

**Note**

Cleaning should take place outside the operating environment to avoid releasing dirt and dust near the equipment.

Step 9 If you washed the filter, allow it to completely air dry for at least eight hours.

**Caution**

Do not put a damp filter back in the ONS 15454.

Step 10 If the air filter should be installed in the external filter brackets, slide the air filter all the way to the back of the brackets to complete the procedure.

Step 11 If the filter should be installed beneath the fan-tray assembly, remove the fan-tray assembly and slide the air filter into the recessed compartment at the bottom of the shelf assembly. Put the front edge of the air filter flush against the front edge of the recessed compartment. Push the fan tray back into the shelf assembly.

**Caution**

If the fan tray does not slide all the way to the back of the shelf assembly, pull the fan tray out and readjust the position of the reusable filter until the fan tray fits correctly.

**Note**

On a powered-up ONS 15454, the fans start immediately after the fan-tray assembly is correctly inserted.

Step 12 To verify that the tray is plugged into the backplane, ensure that the LCD on the front of the fan-tray assembly is activated and displays node information.

Step 13 Rotate the retractable handles back into their compartments.

Step 14 Replace the door and reattach the ground strap.

Remove and Reinsert a Fan-Tray Assembly

Step 1 Use the retractable handles embedded in the front of the fan-tray assembly to pull it forward several inches.

Step 2 Push the fan-tray assembly firmly back into the ONS 15454.

Step 3 Close the retractable handles.

Replace the Fan-Tray Assembly


Caution

The 15454-FTA3 fan-tray assembly can only be installed in ONS 15454 R3.1 and later shelf assemblies (15454-SA-ANSI, P/N: 800-19857; 15454-SA-HD, P/N: 800-24848). It includes a pin that does not allow it to be installed in ONS 15454 shelf assemblies released before ONS 15454 R3.1 (15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1, P/N: 800-07149). Equipment damage can result from attempting to install the 15454-FTA3 in a incompatible shelf assembly.


Caution

Do not force a fan-tray assembly into place. Doing so can damage the connectors on the fan tray and/or the connectors on the backplane.


Caution

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

To replace the fan-tray assembly, it is not necessary to move any of the cable management facilities.

-
- Step 1** Open the front door of the shelf assembly by completing the following steps. If the shelf assembly does not have a front door, continue with [Step 3](#).
- a. Open the front door lock.
 - b. Press the door button to release the latch.
 - c. Swing the door open.
- Step 2** Remove the front door (optional):
- a. Detach the ground strap from either the door or the chassis by removing one of the Kepnuts.
 - b. Place the Kepnut back on the stud after the ground strap is removed to avoid misplacement.
 - c. Secure the dangling end of the ground strap to the door or chassis with tape.
- Step 3** Push the outer side of the handles on the fan-tray assembly to expose the handles.
- Step 4** Fold out the retractable handles at the outside edges of the fan tray.
- Step 5** Pull the handles and slide the fan-tray assembly one inch (25.4 mm) out of the shelf assembly and wait until the fans stop.
- Step 6** When the fans have stopped, pull the fan-tray assembly completely out of the shelf assembly.
- Step 7** If you are replacing the fan-tray air filter and it is installed beneath the fan-tray assembly, slide the existing air filter out of the shelf assembly and replace it before replacing the fan-tray assembly.
- If you are replacing the fan-tray air filter and it is installed in the external bottom bracket, you can slide the existing air filter out of the bracket and replace it at anytime. For more information on the fan-tray air filter, see the [“Inspect, Clean, and Replace the Reusable Air Filter”](#) section on page 2-286.
- Step 8** Slide the new fan tray into the shelf assembly until the electrical plug at the rear of the tray plugs into the corresponding receptacle on the backplane.
- Step 9** To verify that the tray has plugged into the backplane, check that the LCD on the front of the fan tray is activated.

Step 10 If you replace the door, be sure to reattach the ground strap.

2.9.7 Interface Procedures

This section includes instructions for replacing an EIA and an AIP.

Replace the Electrical Interface Assembly



Note

You need a #2 Phillips screwdriver. If you use high-density BNC EIAs, you also need a BNC insertion and removal tool.

- Step 1** To remove the lower backplane cover, loosen the five screws that secure it to the ONS 15454 and pull it away from the shelf assembly.
- Step 2** Loosen the nine perimeter screws that hold the backplane sheet metal cover or EIA in place. Do not remove the interior screws.
- If you are removing an AMP Champ EIA, remove the fastening plate before proceeding. To remove the fastening plate, loosen the two thumbscrews.
- Step 3** If a backplane cover is attached to the ONS 15454, lift the panel by the bottom to remove it from the shelf assembly and store the panel for later use.
- Step 4** If an EIA is attached to the ONS 15454, lift the EIA handles and gently pull it away from the backplane.



Note

Attach backplane sheet metal covers whenever EIAs are not installed.

- Step 5** Line up the connectors on the new EIA with the mating connectors on the backplane.
- Step 6** Gently push the EIA until both sets of connectors fit together snugly.
- Step 7** Replace the nine perimeter screws that you removed while removing the backplane cover.
- Step 8** If you are installing an AMP Champ EIA, attach the fastening plate with the two thumbscrews.
- Step 9** Reattach the lower backplane cover.
-

Replace the Alarm Interface Panel



Caution

Do not use a 2A AIP with a 5A fan-tray assembly; doing so causes a blown fuse on the AIP.



Caution

If any nodes in an Ethernet circuit are not using Software R4.0 or later, there is a risk of Ethernet traffic disruptions. Contact Cisco TAC at 1 800 553-2447 when prompted to do so in the procedure.

**Note**

Perform this procedure during a maintenance window. Resetting the active TCC2/TCC2P can cause a service disruption of less than 50 ms to OC-N or DS-N traffic. Resetting the active TCC2/TCC2P can cause a service disruption of 3 to 5 minutes on all Ethernet traffic due to spanning tree reconvergence if any nodes in the Ethernet circuit are not using Software R4.0 or later.

**Caution**

Do not perform this procedure on a node with live traffic. Hot-swapping the AIP can affect traffic and result in a loss of data. For assistance with AIP replacement contact Cisco TAC 1 800 553-2447.

**Caution**

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

This procedure replaces an existing AIP with a new AIP on an in-service node without affecting traffic. Ethernet circuits that traverse nodes with a software release prior to R4.0 is affected.

You need a #2 Phillips screwdriver.

Step 1 Ensure that all nodes in the affected network are running the same software version before replacing the AIP and repairing circuits:

- a. In network view, click the **Maintenance > Software** tabs. The working software version for each node is listed in the Working Version column.
- b. If you need to upgrade the software on a node, refer to the release-specific software upgrade document for procedures. No hardware should be changed or circuit repair performed until after the software upgrade is complete. If you do not need to upgrade software or have completed the software upgrade, proceed to [Step 2](#).

Step 2 Record the MAC address of the old AIP:

- a. Log into the node where you are replacing the AIP. For login procedures, refer to the “Connect the PC and Log into the GUI” chapter in the *Cisco ONS 15454 Procedure Guide*.
- b. In node view, click the **Provisioning > Network > General** tabs.
- c. Record the MAC address.

Step 3 Call Cisco TAC 1 800 553-2447 for assistance in replacing the AIP and maintaining the original MAC address.

Step 4 Unscrew the five screws that hold the lower backplane cover in place.

Step 5 Grip the lower backplane cover and gently pull it away from the backplane.

Step 6 Unscrew the two screws that hold the AIP cover in place.

Step 7 Grip the cover and gently pull away from the backplane.

**Note**

On the 15454-SA-HD (P/N: 800-24848), 15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1 (P/N: 800-07149) shelves the AIP cover is clear plastic. On the 15454-SA-ANSI shelf (P/N: 800-19857), the AIP cover is metal.

Step 8 Grip the AIP and gently pull it away from the backplane.

Step 9 Disconnect the fan-tray assembly power cable from the AIP.

Step 10 Set the old AIP aside for return to Cisco.

**Caution**

The type of shelf the AIP resides in determines the version of AIP that should replace the failed AIP. The 15454-SA-ANSI shelf (P/N: 800-19857) and 15454-SA-HD (P/N: 800-24848) currently use the 5A AIP, (P/N: 73-7665-01). The 15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1 (P/N: 800-07149) shelves and earlier use the 2A AIP (P/N: 73-5262-01).

**Caution**

Do not put a 2A AIP (P/N: 73-5262-01) into a 15454-SA-ANSI (P/N: 800-19857) or 15454-SA-HD (P/N: 800-24848) shelf; doing so causes a blown fuse on the AIP.

Step 11 Attach the fan-tray assembly power cable to the new AIP.

Step 12 Place the new AIP on the backplane by plugging the panel into the backplane using the DIN connector.

Step 13 Replace the AIP cover over the AIP and secure the cover with the two screws.

Step 14 Replace the lower backplane cover and secure the cover with the five screws.

Step 15 In node view, click the **Provisioning > Network** tabs.

**Caution**

Cisco recommends TCC2/TCC2P resets be performed in a maintenance window to avoid any potential service disruptions.

Step 16 Reset the standby TCC2/TCC2P:

- a. Right-click the standby TCC2/TCC2P and choose **Reset Card**.
- b. Click **Yes** in the Resetting Card dialog box. As the card resets, a loading (Ldg) indication appears on the card in CTC. The reset takes approximately five minutes. Do not perform any other steps until the reset is complete.

Step 17 Reset the active TCC2/TCC2P:

- a. Right click the active TCC2/TCC2P and choose **Reset Card**.
- b. Click **Yes** in the Resetting Card dialog box. As the card resets, a Ldg indication appears on the card in CTC. The reset takes approximately five minutes and CTC loses its connection with the node.

Step 18 From the **File** drop-down list, choose **Exit** to exit the CTC session.

Step 19 Log back into the node. At the Login dialog box, choose (**None**) from the Additional Nodes drop-down list.

Step 20 Record the new MAC address:

- a. In node view, click the **Provisioning > Network > General** tabs.
- b. Record the MAC address.

Step 21 In node view, click the **Circuits** tab. Note that all circuits listed are PARTIAL.

Step 22 In node view, choose **Repair Circuits** from the **Tools** drop-down list. The Circuit Repair dialog box appears.

Step 23 Read the instructions in the Circuit Repair dialog box. If all the steps in the dialog box have been completed, click **Next**. Ensure that you have the old and new MAC addresses.

Step 24 The Node MAC Addresses dialog box appears. Complete the following steps:

- a. From the Node drop-down list, choose the name of the node where you replaced the AIP.

- b. In the Old MAC Address field, enter the old MAC address that was recorded in [Step 2](#).
- c. Click **Next**.

Step 25 The Repair Circuits dialog box appears. Read the information in the dialog box and click **Finish**.

The CTC session freezes until all circuits are repaired. Circuit repair can take up to five minutes or more depending on the number of circuits provisioned on it.

When the circuit repair is complete, the Circuits Repaired dialog box appears.

Step 26 Click **OK**.

Step 27 In the node view of the new node, click the **Circuits** tab. Note that all circuits listed are DISCOVERED. If all circuits listed do not have a DISCOVERED status, call the Cisco TAC 1 800 553-2447 to open a Return Material Authorization (RMA).
