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 15600 alarm and condition. Tables 2-1 through 2-5 provide lists of ONS 15600 alarms organized by severity. Table 2-6 on page 2-5 provides a list of alarms organized alphabetically. Table 2-7 gives definitions of all ONS 15600 alarm logical objects, which are the basis of the alarm profile list in Table 2-8 on page 2-8. For a comprehensive list of all conditions, refer to the *Cisco SONET TL1 Command Guide*.

An alarm troubleshooting procedure applies to both the Cisco Transport Controller (CTC) and Transaction Language One (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 (TAC) (1-800-553-2447).

More information about alarm profile information modification and downloads is located in the “Manage Alarms” chapter in the *Cisco ONS 15600 Procedure Guide*.

2.1 Alarm Indexes by Default Severity

The following tables group alarms and conditions by their default severities in the ONS 15600 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 which 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 15600 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-CORE.

2.1.1 Critical Alarms (CR)

Table 2-1 alphabetically lists ONS 15600 Critical (CR) alarms.

Table 2-1 ONS 15600 Critical Alarm List

BKUPMEMP (EQPT)	IMPROPRMVL (EQPT)	MEA (EQPT)
CTNEQPT-PB-A (EQPT)	IMPROPRMVL (FAN)	MEA (PIM)
CTNEQPT-PB-B (EQPT)	IMPROPRMVL (PIM)	MEA (PPM)
ENCAP-MISMATCH-P (POS)	IMPROPRMVL (PPM)	MFGMEM (EQPT)
EQPT (EQPT)	LASER-BIAS (EQPT)	MFGMEM (FAN)
EQPT (PIM)	LASER-BIAS (PPM)	MFGMEM (PIM)
EQPT (PPM)	LASER-OVER-TEMP (EQPT)	MFGMEM (PPM)
EQPT-BOOT (EQPT)	LASER-OVER-TEMP (PPM)	PLM-P (STSMON)
EQPT-CC-PIM (PIM)	LOF (OCN)	SYNCCLK (NE)
EQPT-PIM-PPM (PPM)	LOP-P (STSMON)	UNEQ-P (STSMON)
FAN-FAIL (FAN)	LOS (OCN)	XCMTX (NE)

2.1.2 Major Alarms (MJ)

Table 2-2 alphabetically lists ONS 15600 Major (MJ) alarms.

Table 2-2 ONS 15600 Major Alarm List

APSCM (OCN)	DBOSYNC (NE)	MEM-GONE (EQPT)
APSCNMIS (OCN)	E-W-MISMATCH (OCN)	PRC-DUPID (OCN)
BLSROSYNC (OCN)	EXTRA-TRAF-PREEMPT (OCN)	PWR (PPM)
BLSR-SW-VER-MISM (OCN)	FAN-FAIL-PARTIAL (FAN)	RING-MISMATCH (OCN)
CARLOSS (GIGE)	GFP-LFD (POS)	SYNCPRI (NE-SREF)
CLKFAIL (EQPT)	GFP-UP-MISMATCH (POS)	SYSBOOT (NE)
CXCHALT (EQPT)	INVMACADR (BPlane)	TPTFAIL (POS)

2.1.3 Minor Alarms (MN)

Table 2-3 alphabetically lists ONS 15600 Minor (MN) alarms.

Table 2-3 ONS 15600 Minor Alarm List

APSB (OCN)	EXT (ENVALRM)	OPEN-SLOT (EQPT)
APSCDFLTK (OCN)	FAN-DEGRADE (FAN)	PROV-MISMATCH (PPM)
APSC-IMP (OCN)	FAN-PWR (FAN)	PWR-FA (BPlane)
APSCINCON (OCN)	FE-SDPRLF (OCN)	PWR-FAIL-A (CAP)

Table 2-3 ONS 15600 Minor Alarm List (continued)

APSIMP (OCN)	FREQ-MISMATCH (EQPT)	PWR-FAIL-A (EQPT)
APSMM (OCN)	HELLO (OCN)	PWR-FAIL-B (CAP)
AUTORESET (EQPT)	HI-LASERBIAS (PPM)	PWR-FAIL-B (EQPT)
CIDMISMATCH-A (EQPT)	HI-RXPOWER (OCN)	PWR-FAIL-RET-A (EQPT)
CIDMISMATCH-B (EQPT)	HI-TXPOWER (PPM)	PWR-FAIL-RET-B (EQPT)
CONTBUS-CLK-A (EQPT)	IMPROPRMVL (CAP)	SFTWDOWN (EQPT)
CONTBUS-CLK-B (EQPT)	IMPR-XC (NE)	SNTP-HOST (NE)
CONTBUS-IO-A (EQPT)	ISIS-ADJ-FAIL (OCN)	SSM-FAIL (BITS)
CONTBUS-IO-B (EQPT)	KBYTE-APS-CHANNEL-FAILURE (OCN)	SSM-FAIL (OCN)
CONTCOM (EQPT)	LOF (BITS)	SYNCPRI (EXT-SREF)
DATAFLT (NE)	LO-LASERBIAS (PPM)	SYNCSEC (EXT-SREF)
DUP-IPADDR (NE)	LO-RXPOWER (OCN)	SYNCSEC (NE-SREF)
DUP-NODENAME (NE)	LOS (BITS)	SYNCTHIRD (EXT-SREF)
EOC (OCN)	LO-TXPOWER (PPM)	TIM-P (STSMON)
EOC-L (OCN)	MATECLK (EQPT)	UNPROT-SYNCCLK (NE)
EQPT (CAP)	MEM-LOW (EQPT)	UNPROT-XCMTX (NE)
EQPT-HITEMP (EQPT)	MFGMEM (CAP)	UNROUTEABLE-IP (NE)

2.1.4 Not Alarmed (NA) Conditions

Table 2-4 alphabetically lists ONS 15600 Not Alarmed conditions.

Table 2-4 ONS 15600 NA Conditions List

AUD-LOG-LOSS (NE)	LKOUTPR-S (OCN)	SSM-PRS (NE-SREF)
AUD-LOG-LOW (NE)	LOCKOUT-REQ (OCN)	SSM-PRS (OCN)
AUTOSW-LOP (STSMON)	LOCKOUT-REQ (STSMON)	SSM-RES (BITS)
AUTOSW-PDI (STSMON)	LOCKOUT-REQ-RING (OCN)	SSM-RES (NE-SREF)
AUTOSW-SDBER (STSMON)	LPBKCRS (STSMON)	SSM-RES (OCN)
AUTOSW-SFBER (STSMON)	LPBKFACILITY (GIGE)	SSM-SMC (BITS)
AUTOSW-UNEQ (STSMON)	LPBKFACILITY (OCN)	SSM-SMC (NE-SREF)
CHANLOSS (OCN)	LPBKPAYLOAD (OCN)	SSM-SMC (OCN)
EXERCISE-RING-FAIL (OCN)	LPBKTERMINAL (GIGE)	SSM-ST2 (BITS)
EXERCISE-SPAN-FAIL (OCN)	LPBKTERMINAL (OCN)	SSM-ST2 (NE-SREF)
EXERCISING-RING (OCN)	MAN-REQ (STSMON)	SSM-ST2 (OCN)
EXERCISING-SPAN (OCN)	MANRESET (EQPT)	SSM-ST3 (BITS)
FAILTOSW (OCN)	MANRESET (PIM)	SSM-ST3 (NE-SREF)
FAILTOSW-PATH (STSMON)	MANRESET (PPM)	SSM-ST3 (OCN)

Table 2-4 ONS 15600 NA Conditions List (continued)

FAILTOSWR (OCN)	MANSWTOINT (NE-SREF)	SSM-ST3E (BITS)
FAILTOSWS (OCN)	MANSWTOPRI (EXT-SREF)	SSM-ST3E (NE-SREF)
FE-EXERCISING-RING (OCN)	MANSWTOPRI (NE-SREF)	SSM-ST3E (OCN)
FE-FRCDWKSWPR-RING (OCN)	MANSWTOSEC (EXT-SREF)	SSM-ST4 (BITS)
FE-FRCDWKSWPR-SPAN (OCN)	MANSWTOSEC (NE-SREF)	SSM-ST4 (NE-SREF)
FE-LOCKOUTOFPR-ALL (OCN)	MANSWTOTHIRD (EXT-SREF)	SSM-ST4 (OCN)
FE-LOCKOUTOFPR-SPAN (OCN)	MANSWTOTHIRD (NE-SREF)	SSM-STU (BITS)
FE-MANWKSWPR-RING (OCN)	MANUAL-REQ-RING (OCN)	SSM-STU (NE-SREF)
FE-MANWKSWPR-SPAN (OCN)	MANUAL-REQ-SPAN (OCN)	SSM-STU (OCN)
FE-SF-RING (OCN)	PDI-P (STSMON)	SSM-TNC (BITS)
FE-SF-SPAN (OCN)	PWRRESTART (EQPT)	SSM-TNC (NE-SREF)
FORCED-REQ (STSMON)	RING-SW-EAST (OCN)	SSM-TNC (OCN)
FORCED-REQ-RING (OCN)	RING-SW-WEST (OCN)	SWTOPRI (EXT-SREF)
FORCED-REQ-SPAN (OCN)	ROLL (STSMON)	SWTOPRI (NE-SREF)
FRCDSWTOINT (NE-SREF)	ROLL-PEND (STSMON)	SWTOSEC (EXT-SREF)
FRCDSWTOPRI (EXT-SREF)	SD-L (OCN)	SWTOSEC (NE-SREF)
FRCDSWTOPRI (NE-SREF)	SD-P (STSMON)	SWTOTHIRD (EXT-SREF)
FRCDSWTOSEC (EXT-SREF)	SF-L (OCN)	SWTOTHIRD (NE-SREF)
FRCDSWTOSEC (NE-SREF)	SF-P (STSMON)	SW-VER (EQPT)
FRCDSWTOTHIRD (EXT-SREF)	SPAN-SW-EAST (OCN)	SYNC-FREQ (BITS)
FRCDSWTOTHIRD (NE-SREF)	SPAN-SW-WEST (OCN)	SYNC-FREQ (OCN)
FRNGSYNC (NE-SREF)	SQUELCH (OCN)	UPGRADE (NE)
FSTSYNC (EQPT)	SSM-DUS (BITS)	WKSWPR (OCN)
FULLPASSTHR-BI (OCN)	SSM-DUS (OCN)	WKSWPR (STSMON)
HLDOVRSYNC (NE-SREF)	SSM-OFF (BITS)	WTR (OCN)
INTRUSION-PSWD (NE)	SSM-OFF (OCN)	WTR (STSMON)
KB-PASSTHR (OCN)	SSM-PRS (BITS)	—

2.1.5 Not Reported (NR) Conditions

Table 2-5 alphabetically lists ONS 15600 Not Reported conditions.

Table 2-5 ONS 15600 NR Conditions List

AIS (BITS)	AIS-P (STSMON)	RFI-L (OCN)
AIS-L (OCN)	AUTOSW-AIS (STSMON)	RFI-P (STSMON)

2.2 Alarms and Conditions Listed by Alphabetical Entry

Table 2-6 alphabetically lists all ONS 15600 alarms and conditions.

Table 2-6 ONS 15600 Alarm and Condition Alphabetical List

AIS (BITS)	FRCDSWTOSEC (EXT-SREF)	PWR-FAIL-B (CAP)
AIS-L (OCN)	FRCDSWTOSEC (NE-SREF)	PWR-FAIL-B (EQPT)
AIS-P (STSMON)	FRCDSWTOTHIRD (EXT-SREF)	PWR-FAIL-RET-A (EQPT)
APSB (OCN)	FRCDSWTOTHIRD (NE-SREF)	PWR-FAIL-RET-B (EQPT)
APSCDFLTK (OCN)	FREQ-MISMATCH (EQPT)	PWRRESTART (EQPT)
APSC-IMP (OCN)	FRNGSYNC (NE-SREF)	RFI-L (OCN)
APSCINCON (OCN)	FSTSYNC (EQPT)	RFI-P (STSMON)
APSCM (OCN)	FULLPASSTHR-BI (OCN)	RING-MISMATCH (OCN)
APSCNMIS (OCN)	GFP-LFD (POS)	RING-SW-EAST (OCN)
APSIMP (OCN)	GFP-UP-MISMATCH (POS)	RING-SW-WEST (OCN)
APSMM (OCN)	HELLO (OCN)	ROLL (STSMON)
AUD-LOG-LOSS (NE)	HI-LASERBIAS (PPM)	ROLL-PEND (STSMON)
AUD-LOG-LOW (NE)	HI-RXPOWER (OCN)	SD-L (OCN)
AUTORESET (EQPT)	HI-TXPOWER (PPM)	SD-P (STSMON)
AUTOSW-AIS (STSMON)	HLDOVRSYNC (NE-SREF)	SF-L (OCN)
AUTOSW-LOP (STSMON)	IMPROPRMVL (CAP)	SF-P (STSMON)
AUTOSW-PDI (STSMON)	IMPROPRMVL (EQPT)	SFTWDOWN (EQPT)
AUTOSW-SDBER (STSMON)	IMPROPRMVL (FAN)	SNTP-HOST (NE)
AUTOSW-SFBER (STSMON)	IMPROPRMVL (PIM)	SPAN-SW-EAST (OCN)
AUTOSW-UNEQ (STSMON)	IMPROPRMVL (PPM)	SPAN-SW-WEST (OCN)
BKUPMEMP (EQPT)	IMPR-XC (NE)	SQUELCH (OCN)
BLSROSYNC (OCN)	INTRUSION-PSWD (NE)	SSM-DUS (BITS)
BLSR-SW-VER-MISM (OCN)	INVMACADR (BPlane)	SSM-DUS (OCN)
CARLOSS (GIGE)	ISIS-ADJ-FAIL (OCN)	SSM-FAIL (BITS)
CHANLOSS (OCN)	KB-PASSTHR (OCN)	SSM-FAIL (OCN)
CIDMISMATCH-A (EQPT)	KBYTE-APS-CHANNEL-FAILURE (OCN)	SSM-OFF (BITS)
CIDMISMATCH-B (EQPT)	LASER-BIAS (EQPT)	SSM-OFF (OCN)
CLKFAIL (EQPT)	LASER-BIAS (PPM)	SSM-PRS (BITS)
CONTBUS-CLK-A (EQPT)	LASER-OVER-TEMP (EQPT)	SSM-PRS (NE-SREF)
CONTBUS-CLK-B (EQPT)	LASER-OVER-TEMP (PPM)	SSM-PRS (OCN)
CONTBUS-IO-A (EQPT)	LKOUTPR-S (OCN)	SSM-RES (NE-SREF)
CONTBUS-IO-B (EQPT)	LOCKOUT-REQ (OCN)	SSM-RES (OCN)
CONTCOM (EQPT)	LOCKOUT-REQ (STSMON)	SSM-RES)(BITS)

Table 2-6 ONS 15600 Alarm and Condition Alphabetical List (continued)

CTNEQPT-PB-A (EQPT)	LOCKOUT-REQ-RING (OCN)	SSM-SMC (BITS)
CTNEQPT-PB-B (EQPT)	LOF (BITS)	SSM-SMC (NE-SREF)
CXCHALT (EQPT)	LOF (OCN)	SSM-SMC (OCN)
DATAFLT (NE)	LO-LASERBIAS (PPM)	SSM-ST2 (BITS)
DBOSYNC (NE)	LOP-P (STSMON)	SSM-ST2 (NE-SREF)
DUP-IPADDR (NE)	LO-RXPOWER (OCN)	SSM-ST2 (OCN)
DUP-NODENAME (NE)	LOS (BITS)	SSM-ST3 (BITS)
FRCDSWTOPRI (EXT-SREF)	LOS (OCN)	SSM-ST3 (NE-SREF)
ENCAP-MISMATCH-P (POS)	LO-TXPOWER (PPM)	SSM-ST3 (OCN)
EOC (OCN)	LPBKCRS (STSMON)	SSM-ST3E (BITS)
EOC-L (OCN)	LPBKFACILITY (GIGE)	SSM-ST3E (NE-SREF)
EQPT (CAP)	LPBKFACILITY (OCN)	SSM-ST3E (OCN)
EQPT (EQPT)	LPBKPAYLOAD (OCN)	SSM-ST4 (BITS)
EQPT (PIM)	LPBKTERMINAL (GIGE)	SSM-ST4 (NE-SREF)
EQPT (PPM)	LPBKTERMINAL (OCN)	SSM-ST4 (OCN)
EQPT-BOOT (EQPT)	MAN-REQ (STSMON)	SSM-STU (BITS)
EQPT-CC-PIM (PIM)	MANRESET (EQPT)	SSM-STU (NE-SREF)
EQPT-HITEMP (EQPT)	MANRESET (PIM)	SSM-STU (OCN)
EQPT-PIM-PPM (PPM)	MANRESET (PPM)	SSM-TNC (BITS)
E-W-MISMATCH (OCN)	MANSWTOINT (NE-SREF)	SSM-TNC (NE-SREF)
EXERCISE-RING-FAIL (OCN)	MANSWTOPRI (EXT-SREF)	SSM-TNC (OCN)
EXERCISE-SPAN-FAIL (OCN)	MANSWTOPRI (NE-SREF)	SWTOPRI (EXT-SREF)
EXERCISING-RING (OCN)	MANSWTOSEC (EXT-SREF)	SWTOPRI (NE-SREF)
EXERCISING-SPAN (OCN)	MANSWTOSEC (NE-SREF)	SWTOSEC (EXT-SREF)
EXT (ENVALRM)	MANSWTOTHIRD (EXT-SREF)	SWTOSEC (NE-SREF)
EXTRA-TRAF-PREEMPT (OCN)	MANSWTOTHIRD (NE-SREF)	SWTOTHIRD (EXT-SREF)
FAILTOSW (OCN)	MANUAL-REQ-RING (OCN)	SWTOTHIRD (NE-SREF)
FAILTOSW-PATH (STSMON)	MANUAL-REQ-SPAN (OCN)	SW-VER (EQPT)
FAILTOSWR (OCN)	MATECLK (EQPT)	SYNCCLK (NE)
FAILTOSWS (OCN)	MEA (EQPT)	SYNC-FREQ (BITS)
FAN-FAIL (FAN)	MEA (PIM)	SYNC-FREQ (OCN)
FAN-FAIL-PARTIAL (FAN)	MEA (PPM)	SYNCPRI (EXT-SREF)
FAN-PWR (FAN)	MEM-GONE (EQPT)	SYNCPRI (NE-SREF)
FE-EXERCISING-RING (OCN)	MEM-LOW (EQPT)	SYNCSEC (EXT-SREF)
FE-FRCDWKSWPR-RING (OCN)	MFGMEM (CAP)	SYNCSEC (NE-SREF)
FE-FRCDWKSWPR-SPAN (OCN)	MFGMEM (EQPT)	SYNCTHIRD (EXT-SREF)
FE-LOCKOUTOFPR-ALL (OCN)	MFGMEM (FAN)	SYSBOOT (NE)

Table 2-6 ONS 15600 Alarm and Condition Alphabetical List (continued)

FE-LOCKOUTOFPR-SPAN (OCN)	MFGMEM (PIM)	TIM-P (STSMON)
FE-MANWKSWPR-RING (OCN)	MFGMEM (PPM)	TPTFAIL (POS)
FE-MANWKSWPR-SPAN (OCN)	NOT-AUTHENTICATED	UNEQ-P (STSMON)
FE-SDPRLF (OCN)	OPEN-SLOT (EQPT)	UNPROT-SYNCCLK (NE)
FE-SF-RING (OCN)	PDI-P (STSMON)	UNPROT-XCMTX (NE)
FE-SF-SPAN (OCN)	PLM-P (STSMON)	UNROUTEABLE-IP (NE)
FORCED-REQ (STSMON)	PRC-DUPID (OCN)	UPGRADE (NE)
FORCED-REQ-RING (OCN)	PROV-MISMATCH (PPM)	WKSWPR (OCN)
FORCED-REQ-SPAN (OCN)	PWR (PWR)	WKSWPR (STSMON)
FRCDSWTOINT (NE-SREF)	PWR-FA (BPlane)	WTR (OCN)
FRCDSWTOPRI (EXT-SREF)	PWR-FAIL-A (CAP)	WTR (STSMON)
FRCDSWTOPRI (NE-SREF)	PWR-FAIL-A (EQPT)	XCMTX (NE)

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 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 building integrated timing supply (BITS) clock as well as other objects. Therefore, both OCN: LOS and BITS: 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

Type	Description
BITS	Building integration timing supply incoming references (BITS-1, BITS-2).
BPLANE	The backplane.
CAP	Customer Access Panel (CAP)
ENVALRM	An environmental alarm port.
EQPT	A card, its physical objects, and 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).
EXT-SREF	BITS outgoing references (SYNC-BITS1, SYNC-BITS2).

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

FAN	Fan-tray assembly.
GIGE	Gigabit Ethernet.
NE	The entire network element.
NE-SREF	The timing status of the NE.
OCN	An OC-N line on an OC-N card.
PIM	Pluggable input-output module (or 4PIO) for the Any Service, Any Port (ASAP) card.
POS	Packet over SONET (virtual entity).
PPM	Pluggable port module (PPM), or small form-factor pluggable (SFP), for the ASAP card.
PS-STS	Protection-switched ONS 15600 STS.
PWR	The node's power supply.
STSMON	STS alarm detection at the monitor point (upstream from the cross-connect).
STSRNG	The STS ring.
STSTERM	STS alarm detection at termination (downstream from the cross-connect).

2.4 Alarm List by Logical Object Type

Table 2-8 lists all ONS 15600 Release 6.0 alarms and logical objects as they are given in the system alarm profile. The list entries are organized logical object name and then by alarm or condition name. Each entry refers to an alarm description in this chapter. Where appropriate, the alarm entries also contain troubleshooting procedures.

Note In a mixed network containing different types of nodes (such as an 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 ONS 15600 Alarm List by Logical Object in Alarm Profile

BITS: AIS	NE-SREF: FRCDSWTOSEC	OCN: LOCKOUT-REQ-RING
BITS: LOF	NE-SREF: FRCDSWTOTHIRD	OCN: LOF
BITS: LOS	NE-SREF: FRNGSYNC	OCN: LOS
BITS: SSM-DUS	NE-SREF: HLDOVRSYNC	OCN: LPBKFACILITY
BITS: SSM-FAIL	NE-SREF: MANSWTOINT	OCN: LPBKPAYLOAD
BITS: SSM-OFF	NE-SREF: MANSWTOPRI	OCN: LPBKTERMINAL
BITS: SSM-PRS	NE-SREF: MANSWTOSEC	OCN: MANUAL-REQ-RING

Table 2-8 ONS 15600 Alarm List by Logical Object in Alarm Profile (continued)

BITS: SSM-RES	NE-SREF: MANSWTOTHIRD	OCN: MANUAL-REQ-SPAN
BITS: SSM-SMC	NE-SREF: SSM-PRS	OCN: PRC-DUPID
BITS: SSM-ST2	NE-SREF: SSM-RES	OCN: RFI-L
BITS: SSM-ST3	NE-SREF: SSM-SMC	OCN: RING-MISMATCH
BITS: SSM-ST3E	NE-SREF: SSM-ST2	OCN: RING-SW-EAST
BITS: SSM-ST4	NE-SREF: SSM-ST3	OCN: RING-SW-WEST
BITS: SSM-STU	NE-SREF: SSM-ST3E	OCN: SD-L
BITS: SSM-TNC	NE-SREF: SSM-ST4	OCN: SF-L
BITS: SYNC-FREQ	NE-SREF: SSM-STU	OCN: SPAN-SW-EAST
BPlane: INVMACADR	NE-SREF: SSM-TNC	OCN: SPAN-SW-WEST
BPlane: PWR-FA	NE-SREF: SWTOPRI	OCN: SQUELCH
CAP: EQPT	NE-SREF: SWTOSEC	OCN: SSM-DUS
CAP: IMPROPRMVL	NE-SREF: SWTOTHIRD	OCN: SSM-FAIL
CAP: MFGMEM	NE-SREF: SYNCPRI	OCN: SSM-OFF
CAP: PWR-FAIL-A	NE-SREF: SYNCSEC	OCN: SSM-PRS
CAP: PWR-FAIL-B	NE: AUD-LOG-LOSS	OCN: SSM-RES
ENVALRM: EXT	NE: AUD-LOG-LOW	OCN: SSM-SMC
EQPT: AUTORESET	NE: DATAFLT	OCN: SSM-ST2
EQPT: BKUPMEMP	NE: DBOSYNC	OCN: SSM-ST3
EQPT: CIDMISMATCH-A	NE: DUP-IPADDR	OCN: SSM-ST3E
EQPT: CIDMISMATCH-B	NE: DUP-NODENAME	OCN: SSM-ST4
EQPT: CLKFAIL	NE: IMPR-XC	OCN: SSM-STU
EQPT: CONTBUS-CLK-A	NE: INTRUSION-PSWD	OCN: SSM-TNC
EQPT: CONTBUS-CLK-B	NE: SNTP-HOST	OCN: SYNC-FREQ
EQPT: CONTBUS-IO-A	NE: SYNCCLK	OCN: WKSWPR
EQPT: CONTBUS-IO-B	NE: SYSBOOT	OCN: WTR
EQPT: CONTCOM	NE: UNPROT-SYNCCLK	PIM: EQPT
EQPT: CTNEQPT-PB-A	NE: UNPROT-XCMTX	PIM: EQPT-CC-PIM
EQPT: CTNEQPT-PB-B	NE: UNROUTEABLE-IP	PIM: IMPROPRMVL
EQPT: CXCHALT	NE: UPGRADE	PIM: MANRESET
EQPT: EQPT	NE: XCMTX	PIM: MEA
EQPT: EQPT-BOOT	OCN: AIS-L	PIM: MFGMEM
EQPT: EQPT-HITEMP	OCN: APSB	POS: ENCAP-MISMATCH-P
EQPT: FREQ-MISMATCH	OCN: APSC-IMP	POS: GFP-LFD
EQPT: FSTSYNC	OCN: APSCDFLTK	POS: GFP-UP-MISMATCH
EQPT: IMPROPRMVL	OCN: APSCINCON	POS: TPTFAIL
EQPT: LASER-BIAS	OCN: APSCM	PPM: EQPT

Table 2-8 ONS 15600 Alarm List by Logical Object in Alarm Profile (continued)

EQPT: LASER-OVER-TEMP	OCN: APSCNMIS	PPM: EQPT-PIM-PPM
EQPT: MANRESET	OCN: APSIMP	PPM: HI-LASERBIAS
EQPT: MATECLK	OCN: APSMM	PPM: HI-TXPOWER
EQPT: MEA	OCN: BLSR-SW-VER-MISM	PPM: IMPROPRMVL
EQPT: MEM-GONE	OCN: BLSROSYNC	PPM: LASER-BIAS
EQPT: MEM-LOW	OCN: CHANLOSS	PPM: LASER-OVER-TEMP
EQPT: MFGMEM	OCN: E-W-MISMATCH	PPM: LO-LASERBIAS
EQPT: OPEN-SLOT	OCN: EOC	PPM: LO-TXPOWER
EQPT: PWR-FAIL-A	OCN: EOC-L	PPM: MANRESET
EQPT: PWR-FAIL-B	OCN: EXERCISE-RING-FAIL	PPM: MEA
EQPT: PWR-FAIL-RET-A	OCN: EXERCISE-SPAN-FAIL	PPM: MFGMEM
EQPT: PWR-FAIL-RET-B	OCN: EXERCISING-RING	PPM: PROV-MISMATCH
EQPT: PWRRESTART	OCN: EXERCISING-SPAN	PWR: PWR
EQPT: SFTWDOWN	OCN: EXTRA-TRAF-PREEMPT	STSMON: AIS-P
EQPT: SW-VER	OCN: FAILTOSW	STSMON: AUTOSW-AIS
EXT-SREF: FRCDSWTOPRI	OCN: FAILTOSWR	STSMON: AUTOSW-LOP
EXT-SREF: FRCDSWTOSEC	OCN: FAILTOSWS	STSMON: AUTOSW-PDI
EXT-SREF: FRCDSWTOTHIRD	OCN: FE-EXERCISING-RING	STSMON: AUTOSW-SDBER
EXT-SREF: MANSWTOPRI	OCN: FE-FRCDWKSWPR-RING	STSMON: AUTOSW-SFBER
EXT-SREF: MANSWTOSEC	OCN: FE-FRCDWKSWPR-SPAN	STSMON: AUTOSW-UNEQ
EXT-SREF: MANSWTOTHIRD	OCN: FE-LOCKOUTOFPR-ALL	STSMON: FAILTOSW-PATH
EXT-SREF: SWTOPRI	OCN: FE-LOCKOUTOFPR-SPAN	STSMON: FORCED-REQ
EXT-SREF: SWTOSEC	OCN: FE-MANWKSWPR-RING	STSMON: LOCKOUT-REQ
EXT-SREF: SWTOTHIRD	OCN: FE-MANWKSWPR-SPAN	STSMON: LOP-P
EXT-SREF: SYNCPRI	OCN: FE-SDPRLF	STSMON: LPBKCRS
EXT-SREF: SYNCSEC	OCN: FE-SF-RING	STSMON: MAN-REQ
EXT-SREF: SYNCTHIRD	OCN: FE-SF-SPAN	STSMON: PDI-P
FAN: FAN-DEGRADE	OCN: FORCED-REQ-RING	STSMON: PLM-P
FAN: FAN-FAIL	OCN: FORCED-REQ-SPAN	STSMON: RFI-P
FAN: FAN-FAIL-PARTIAL	OCN: FULLPASSTHR-BI	STSMON: ROLL
FAN: FAN-PWR	OCN: HELLO	STSMON: ROLL-PEND
FAN: IMPROPRMVL	OCN: HI-RXPOWER	STSMON: SD-P
FAN: MFGMEM	OCN: ISIS-ADJ-FAIL	STSMON: SF-P
GIGE: CARLOSS	OCN: KB-PASSTHR	STSMON: TIM-P
GIGE: LPBKFACILITY	OCN: KBYTE-APS-CHANNEL-FAILURE	STSMON: UNEQ-P
GIGE: LPBKTERMINAL	OCN: LKOUTPR-S	STSMON: WKSWPR

Table 2-8 ONS 15600 Alarm List by Logical Object in Alarm Profile (continued)

NE-SREF: FRCDSWTOINT	OCN: LO-RXPOWER	STSMON: WTR
NE-SREF: FRCDSWTOPRI	OCN: LOCKOUT-REQ	—

2.5 Trouble Notifications

The ONS 15600 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 15600 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 15600 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 15600 shelf. They might 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 SONET TL1 Command Guide*.

2.5.3 Severities

The ONS 15600 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 the free-running synchronization (FRNGSYNC) state or forced-switch to primary timing source (FRCSWTOPRI) event. They might or might not require troubleshooting, as indicated in the entries.
- Not Reported (NR) conditions occur as a secondary result of another event. For example, the alarm indication signal (AIS), with severity NR, is inserted by a downstream node when an LOS (CR or MJ) alarm occurs upstream. These conditions do not in themselves require troubleshooting, but are to be expected in the presence of primary alarms.

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. Procedures for customizing alarm severities are located in the "Manage Alarms" chapter in the *Cisco ONS 15600 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 hierarchy of path alarms in the ONS 15600 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 hierarchy of facility alarms in the ONS 15600 system is shown in Table 2-10.

Table 2-10 Facility Alarm Hierarchy

Priority	Condition Type
Highest	LOS
—	LOF
—	AIS-L
—	SF-L
—	SD-L
—	RFI-L
—	TIM-S[1]

Table 2-10 Facility Alarm Hierarchy (continued)

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

1. This alarm is not used in this platform in this release.

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, etc.), 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[3]
—	PLM-V
Lowest	DS-N AIS (if reported for outgoing DS-N signals, which are not supported for the ONS 15600)

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.
3. This alarm is not used in this platform in this release.

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—might be Critical (CR) or Major (MJ) severity alarms. Service-Affecting (SA) alarms indicate service is affected.
Non-Service-Affecting (NSA) alarms always have a Minor (MN), Not Alarmed (NA), or Not Reported (NR) 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."

2.5.7 Safety Summary

This section covers safety considerations to ensure safe operation of the ONS 15600 system. Personnel should not perform any procedures in this manual 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 might be present on the backplane when the system is operating. Use caution when removing or installing cards.

Some troubleshooting procedures require installation or removal of optical cards. In these instances, users should pay close attention to the following warnings:

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

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

Warning **Class 1 laser product.** Statement 1008

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

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

2.6 Alarm Procedures

This section lists alarms alphabetically and includes some conditions commonly encountered when troubleshooting alarms. The severities, descriptions, and troubleshooting procedures accompany alarms and conditions.

2.6.1 AIS

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

Logical Object: BITS

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 the node sees the AIS instead of a real signal. In most cases when this condition is raised, an upstream node is raising an alarm to indicate a signal failure; all nodes downstream from it only raise some type of AIS. This condition clears when you resolved the problem on the upstream node.

Clear the AIS Condition

Step 1 Determine whether there are alarms on the upstream nodes and equipment, especially the "LOS (OCN)" alarm on page 2-87 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).

2.6.2 AIS-L

Default Severity: Nor Reported (NR), Non-Service-Affecting (NSA)

Logical Object: OCN

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

Clear the AIS-L Condition

Step 1 Complete the "Clear the AIS Condition" procedure on page 2-15.

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).

2.6.3 AIS-P

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

Logical Object: STSMON

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 2-15.

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).

2.6.4 APSB

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

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 nodes not manufactured by Cisco send invalid APS codes if they are configured in a 1+1 protection scheme with newer SONET nodes, such as the ONS 15600. These invalid codes cause an APSB alarm on an ONS 15600.

Note APS switches are hitless on the ONS 15600.

Clear the APSB Alarm

Step 1 Use an optical test set to examine the incoming SONET overhead to confirm inconsistent or invalid K bytes. For specific procedures to use the test set equipment, consult the manufacturer. If corrupted K bytes are confirmed and the upstream equipment is functioning properly, the upstream equipment might not interoperate effectively with the ONS 15600.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15600. 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 and the overhead shows inconsistent or invalid K bytes, you might need to replace the upstream cards for protection switching to operate properly. Complete the "Replace an OC-48 Card or OC-192 Card" procedure on page 2-140.

Caution For the ONS 15600, 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 "2.8.5 Verify or Create Node DCC Terminations" section on page 2-145 for commonly used alarm troubleshooting procedures.

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

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

2.6.5 APSCDFLTK

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

Logical Object: OCN

The APS Default K Byte Received alarm occurs when a bidirectional line switched ring (BLSR) is not properly configured—for example, when a four-node BLSR has one node configured as a path protection. 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 2-28.

Clear the APSCDFLTK Alarm

Step 1 Complete the "Identify a BLSR Ring ID or Node ID Number" procedure on page 2-127 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 2-128 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 2-48.) 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 15600 Procedure Guide* contains procedures for fibering a BLSR.

Step 5 If the alarm does not clear and if the network is a four-fiber BLSR, ensure that each protect fiber is connected to another protect fiber and each working fiber is connected to another working fiber. The software does not report any alarm if a working fiber is incorrectly attached to a protect fiber.

Step 6 If the alarm does not clear, complete the "Verify Node Visibility for Other Nodes" procedure on page 2-128.

Step 7 If nodes are not visible, complete the "2.8.5 Verify or Create Node DCC Terminations" procedure on page 2-145 to ensure that SONET data communication channel (DCC) 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).

2.6.6 APSC-IMP

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

Logical Object: OCN

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

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

Note This alarm can occur on a VT tunnel when it does not have VT circuits provisioned 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 may result in hazardous radiation exposure.** Statement 1057

Clear the APSC-IMP Alarm

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

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15600. 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 15600. Troubleshoot the upstream equipment using the procedures in this chapter, as applicable. If the upstream nodes are not ONS 15600s, 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 ID or Node ID Number" procedure on page 2-127.

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 ID Number" procedure on page 2-127.

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).

2.6.7 APSCINCON

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

Logical Object: OCN

An APS Inconsistent alarm means that an inconsistent APS byte is present. The SONET overhead contains K1/K2 APS bytes that notify receiving equipment, such as the ONS 15600, 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 2-87, the "LOF (OCN)" alarm on page 2-83, or the "AIS" condition on page 2-15. 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).

2.6.8 APSCM

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

Logical Object: OCN

The APS Channel Mismatch alarm occurs when the ONS system 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 system when bidirectional protection is used on OC-N cards in a 1+1 configuration.

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

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

Note APS switches are hitless in the ONS 15600.

Clear the APSCM Alarm

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

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15600. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 2 If the fibers are correctly connected, verify that the protection-card channel fibers are physically connected directly to the adjoining node'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) to report a Service-Affecting (SA) problem.

2.6.9 APSCNMIS

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

Logical Object: OCN

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

Clear the APSCNMIS Alarm

Step 1 Complete the "Identify a BLSR Ring ID or Node ID Number" procedure on page 2-127 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 2-128 to change one node ID number so that each node ID is unique.

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

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

Step 5 If the alarm does not clear, use the "Initiate a Lock Out on a BLSR Protect Span" procedure on page 2-135 to lock out the span.

Step 6 Complete the "Clear a BLSR External Switching Command" procedure on page 2-136 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) to report a Service-Affecting (SA) problem.

2.6.10 APSIMP

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

Logical Object: OCN

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

The condition is superseded by an 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 Condition

Step 1 Check the configuration of the other node in the 1+1 protection group. If the far end is not configured for 1+1 protection, create the group. For instructions, refer to the "Turn Up Node" chapter in the *Cisco ONS 15600 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).

2.6.11 APSMM

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

Logical Object: OCN

An APS Mode Mismatch failure alarm occurs on traffic (OC-N) facilities 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. The alarm can also occur if a vendor's equipment (other than Cisco) is provisioned as 1:N and the ONS 15600 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 15600 node that is provisioned for 1+1 protection switching.

Clear the APSMM Alarm

Step 1 For the reporting ONS system, display node view and verify the protection scheme provisioning by completing the following steps:

- **a.** Click the **Provisioning > Protection** tabs.
- **b.** Click the 1+1 protection group configured for the OC-N cards.

  The chosen protection group is the protection group optically connected (with DCC connectivity) to the far end.
- **c.** Click **Edit**.
- **d.** 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).

2.6.12 AUD-LOG-LOSS

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

Logical Object: NE

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

Clear the AUD-LOG-LOSS Condition

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

Step 2 Click **Retrieve**.

Step 3 Click **Archive**.

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

Step 5 Enter a name in the File Name field.

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

Step 6 Click **Save**.

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

Step 7 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.13 AUD-LOG-LOW

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

Logical Object: NE

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

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

2.6.14 AUTORESET

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

Logical Object: EQPT

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

Note If an optical card associated with an active port in a 1+1 protection group resets, all DCC traffic terminated or tunneled on the active port is lost while the card resets. No DCC traffic is lost during a reset of an optical card associated with a standby port.

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 "Replace an OC-48 Card or OC-192 Card" procedure on page 2-140. If the lack of communication continues, the AUTORESET alarm is cleared and the 2.6.48 EQPT-BOOT alarm occurs. In this case, no AUTORESET troubleshooting is required. If the alarm does not clear, complete the following procedure.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15600. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Caution For the ONS 15600, 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 "2.8.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-128 for commonly used traffic-switching procedures.

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

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

2.6.15 AUTOSW-AIS

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

Logical Object: STSMON

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.

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 resolve the problem on the upstream node.

Clear the AUTOSW-AIS Condition

Step 1 Complete the "Clear the AIS Condition" procedure on page 2-15.

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).

2.6.16 AUTOSW-LOP (STSMON)

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

Logical Object: STSMON

The Automatic path protection Switch Caused by LOP condition for the STS monitor (STSMON) indicates that automatic path protection switching occurred because of the "LOP-P" alarm on page 2-84. If the path protection is configured for revertive switching, it reverts to the working path after the fault clears.

Clear the AUTOSW-LOP (STSMON) Condition

Step 1 Complete the "Clear the LOP-P Alarm" procedure on page 2-85.

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).

2.6.17 AUTOSW-PDI

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

Logical Object: STSMON

The Automatic path protection Switch Caused by Payload Defect Indication (PDI) condition indicates that automatic path protection switching occurred because of a "PDI-P" alarm on page 2-99. If the path protection is configured for revertive switching, it reverts to the working path after the fault clears.

Clear the AUTOSW-PDI Condition

Step 1 Complete the "Clear the PDI-P Condition" procedure on page 2-100.

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).

2.6.18 AUTOSW-SDBER

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

Logical Object: STSMON

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

Clear the AUTOSW-SDBER Condition

Step 1 Complete the "Clear the SD-L Condition" procedure on page 2-109. (It is also used for this 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).

2.6.19 AUTOSW-SFBER

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

Logical Object: STSMON

The Automatic USPR Switch Caused by Signal Fail Bit Error Rate (SFBER) condition indicates that a "SF-L" condition on page 2-110 caused automatic path protection switching to occur. If the path protection is configured for revertive switching, it reverts to the working path when the SF is resolved.

Clear the AUTOSW-SFBER Condition

Step 1 Complete the "Clear the SD-L Condition" procedure on page 2-109 (It is also used for a signal fail 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).

2.6.20 AUTOSW-UNEQ (STSMON)

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

Logical Object: STSMON

The Automatic path protection Switch Caused by Unequipped Circuit condition indicates that an UNEQ alarm 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.

Clear the AUTOSW-UNEQ (STSMON) Condition

Step 1 Complete the "Clear the UNEQ-P Alarm" procedure on page 2-121.

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).

2.6.21 BKUPMEMP

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

Logical Object: EQPT

The Primary Non-Volatile Backup Memory Failure alarm refers to a problem with the Timing and Shelf Controller (TSC) card flash memory. The alarm occurs when the controller card 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 TSC card).

The BKUPMEMP alarm can also cause the "EQPT (EQPT)" alarm on page 2-44. If the EQPT alarm is caused by BKUPMEMP, complete the following procedure to clear the BKUPMEMP and the EQPT alarm.

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

Clear the BKUPMEMP Alarm

Step 1 Verify that both TSC cards are powered and enabled by confirming lighted SRV LEDs on the TSC cards.

Step 2 Determine whether the active or standby TSC card that has the alarm.

Step 3 If both TSC cards are powered and enabled, reset the TSC card against which the alarm is raised. Complete the "Soft-Reset a Card Using CTC" procedure on page 2-136.

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

Step 4 If the TSC card you reset does not reboot successfully, or the alarm has not cleared, call Cisco TAC (1-800-553-2447). If the Cisco TAC technician tells you to reseat the card, complete the "Reset a Card with a Card Pull (Reseat)" procedure on page 2-138. If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the "Replace a TSC Card" procedure on page 2-142.

2.6.22 BLSROSYNC

This alarm is not supported on this platform in this release.

2.6.23 BLSR-SW-VER-MISM

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

Logical Object: OCN

The BLSR Software Version Mismatch alarm is raised by the TSC card 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 TSC card 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) condition.

2.6.24 CARLOSS (GIGE)

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

Logical Object: GIGE

The Carrier Loss for Gigabit Ethernet (GE) alarm occurs on ASAP ports supporting Gigabit Ethernet traffic. The loss can be due to a misconfiguration, fiber cut, or client equipment problem.

Clear the CARLOSS (GIGE) Alarm

Step 1 Ensure that the GIGE client is correctly configured by completing the following steps:

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

b. Click the **Provisioning > Pluggable Port Modules** tabs.

c. View the Pluggable Port Modules area port listing in the **Actual Equipment Type** column and compare this with the client equipment. If no small form-factor pluggable (SFP, or also referred to as a PPM) is provisioned, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15600 Procedure Guide* for provisioning instructions.

d. If an SFP (PPM) has been created, view the contents of the Selected PPM area **Rate** column for the port and compare this rate with the client equipment data rate. In this case, the rate should be ETHER. If the SFP (PPM) rate is differently provisioned, select the SFP (PPM), click **Delete**, then click **Create** and choose the correct rate for the equipment type.

Step 2 If there is no SFP (PPM) misprovisioning, check for a fiber cut.

Step 3 If there is no fiber cut or provisioning error, check the client-side equipment for any transmission errors on the line.

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

2.6.25 CHANLOSS

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

Logical Object: OCN

The SONET Section Layer DCC Termination Failure condition occurs when the ONS 15600 receives unrecognized data in the section layer DCC bytes.

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

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

Clear the CHANLOSS Condition

Step 1 In the absence of other alarms, determine whether the alarmed port is connected to another vendor's equipment. If so, you can mask the alarm on this path using a custom alarm profile. For more information about custom profiles, refer to the "Manage Alarms" chapter in the *Cisco ONS 15600 Procedure Guide*.

Step 2 If alternate vendor equipment is not the cause of the alarm, complete the "Soft-Reset a Card Using CTC" procedure on page 2-136 for the traffic card.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15600. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 3 If the alarm does not clear, complete the "Replace an OC-48 Card or OC-192 Card" procedure on page 2-140.

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).

2.6.26 CIDMISMATCH-A

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

Logical Object: EQPT

A Connection ID Mismatch on the Single Shelf Cross-Connect (SSXC) A (in Slot 6) alarm occurs when at least one internal connection ID mismatch is present at the STS-1 level on the traffic (OC-N) card outbound data path.

The alarm occurs under the following conditions:

- Head end of the connection between traffic cards is removed.
- VT tunnel if it does not have VT circuits provisioned on it.
- Circuit is not provisioned completely in an open ended STS circuit.

Note When an alarm includes a numeric or alphabetical designation, it indicates whether the alarm applies to the first or second card of a specific type on the shelf. A zero or A indicates that the alarm occurs against the first card of its type, from left to right, in the shelf. A one or B indicates that the alarm occurs against the second card of its type in the shelf.

Clear the CIDMISMATCH-A Alarm

Step 1 Depending on how many CIDMISMATCH alarms are raised, take one of the following actions:

- If two CIDMISMATCH alarms (CIDMISMATCH-A and the"CIDMISMATCH-B" alarm on page 2-31) are present, continue with Step 6.
- One CIDMISMATCH-x alarm indicates trouble related to one SSXC card. If an automatic switch to the alternate copy SSXC card occurred, the alarmed SSXC card can be serviced. If traffic has not switched, complete the "Request a Cross-Connect Card Preferred Copy Switch" procedure on page 2-138.

  To determine which SSXC card is the preferred copy and if it is currently being used, in node view click the **Maintenance > Preferred Copy** tabs. The Data Copy area Preferred field shows Copy A or Copy B. The Currently Used field shows the copy being used.

  Note In CTC, Copy A refers to the SSXC card in Slot 6. Copy B refers to the SSXC card in Slot 8. Either copy can be chosen as the preferred copy SSXC card. The other SSXC card is called the alternate SSXC card in this chapter.

Step 2 Complete the "Soft-Reset a Card Using CTC" procedure on page 2-136 for the alarmed SSXC card.

Step 3 If the alarm does not clear, ensure that an automatic protection switch has moved traffic to the protect port. If an APS switch occurred, continue with Step 4.

- A path protection APS is identified by an AUTOSW-type alarm or condition (such as AUTOSW-AIS, AUTOSW-LOP, AUTOSW-PDI, AUTOSW-SDBER, AUTOSW-SFBER, or AUTOSW-UNEQ).
- A 1+1 APS is identified in the node view Maintenance > Protection window. If you click the protection group, under the Selected Group list, the ports are designated as Working/Standby and Protect/Active.

If the reporting traffic card has 1+1 active ports and traffic has not switched to the protect ports, complete the "Initiate a 1+1 Protection Port Force Switch Command" procedure on page 2-128.

Step 4 Complete the "Reset a Card with a Card Pull (Reseat)" procedure on page 2-138 for the SSXC card.

Step 5 If the alarm does not clear, complete the "Replace an SSXC Card" procedure on page 2-139, "Replace an OC-48 Card or OC-192 Card" procedure on page 2-140, or "Replace a TSC Card" procedure on page 2-142 as appropriate 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).

Step 7 When the alarm clears, if an automatic switch to the alternate copy SSXC card occurred, traffic is restored to the preferred copy.

If the reporting card is a traffic card, traffic reverts to the working port if an automatic switch occurred. If traffic was manually switched in a 1+1 protection group, revert traffic to the original port by completing the "Clear a 1+1 Protection Port Force or Manual Switch Command" procedure on page 2-129. If traffic was manually switched in a path protection, revert traffic to the original path by completing the "Clear a Path Protection Span External Switching Command" procedure on page 2-133.

2.6.27 CIDMISMATCH-B

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

Logical Object: EQPT

A Connection ID Mismatch on SSXC-B (Slot 8) alarm occurs when at least one internal connection ID mismatch is present at the STS-1 level on the OC-48 or OC-192 card outbound data path.

The alarm occurs under the following conditions:

- Head end of the connection between traffic cards is removed.
- VT tunnel if it does not have VT circuits provisioned on it.
- Circuit is not provisioned completely in an open ended STS circuit.

Clear the CIDMISMATCH-B Alarm

Step 1 Complete the "Clear the CIDMISMATCH-A Alarm" procedure on page 2-30.

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).

2.6.28 CLKFAIL

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

Logical Object: EQPT

The Clock Fail alarm occurs when an internal clock module fails. If this alarm occurs against the standby TSC card, the card must be replaced. If the alarm occurs against the active TSC card, the card automatically becomes standby because the traffic and SSXC cards can only take timing from the active TSC card.

Clear the CLKFAIL Alarm

Step 1 Complete the "Replace a TSC Card" procedure on page 2-142 for the reporting TSC card.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15600. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Note When there are different versions of system software on the two TSC cards, it takes approximately 20 minutes for the active TSC card to transfer the system software to the newly installed standby TSC card. When the transfer completes, the TSC card reboots and goes into standby mode after approximately three minutes.

Note If the active and standby TSC cards have the same versions of software, it takes approximately three minutes for software to be updated on a standby TSC 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).

2.6.29 CONTBUS-CLK-A

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

Logical Object: EQPT

An Inbound Interconnection Timing Control Bus 0 Failure alarm on the Slot 10 TSC card occurs if the timing signal from the Slot 5 TSC card has an error. If the Slot 10 TSC card and all other cards on the shelf raise this alarm, the alarm processor on the Slot 5 TSC card clears the alarm on the other cards and raises this alarm against the Slot 5 TSC card only.

Clear the CONTBUS-CLK-A Alarm

Step 1 If a single traffic card is reporting the alarm and it is part of a path protection, complete the "Initiate a Force Switch for All Circuits on a Path Protection Span" procedure on page 2-131. If the traffic card is part of a 1+1 protection group, complete the "Initiate a 1+1 Protection Port Force Switch Command" procedure on page 2-128.

Note If the reporting card is an SSXC card, traffic should have already switched from the errored copy of the card.

Note If the active TSC is reporting the alarm, shelf control should already have switched off the card.

Step 2 Complete the appropriate procedure in the "2.8.4 Physical Card Reseating, Resetting, and Replacement" section on page 2-138 for the reporting 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).

When the alarm clears, if an automatic switch to the alternate copy SSXC occurred, traffic is automatically restored to the preferred copy.

Step 4 If traffic was manually switched in a 1+1 protection group, revert traffic to the original port by completing the "Clear a 1+1 Protection Port Force or Manual Switch Command" procedure on page 2-129. If traffic was manually switched in a path protection, revert traffic to the original path by completing the "Clear a Path Protection Span External Switching Command" procedure on page 2-133.

Step 5 When the alarm has been cleared, if desired, complete the "Soft-Reset a Card Using CTC" procedure on page 2-136.

2.6.30 CONTBUS-CLK-B

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

Logical Object: EQPT

An Inbound Interconnection Timing Control Bus 1 Failure alarm on the Slot 5 TSC card occurs if the timing signal from the Slot 10 TSC card has an error. If the Slot 5 TSC card and all other cards on the shelf raise the alarm, the processor on the Slot 10 TSC card clears the alarm on the other cards and raises this alarm against the Slot 10 TSC card only.

Note When an alarm includes a numeric or alphabetical designation, it indicates whether the alarm applies to the first or second card of a specific type on the shelf. A zero or A indicates that the alarm occurs against the first card of its type, from left to right, in the shelf. A one or B indicates that the alarm occurs against the second card of its type in the shelf.

Clear the CONTBUS-CLK-B Alarm

Step 1 Complete the "Clear the CONTBUS-CLK-A Alarm" procedure on page 2-33.

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).

2.6.31 CONTBUS-IO-A

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

Logical Object: EQPT

A TSC card A to Shelf A Slot Communication Failure alarm occurs when the active Slot 5 TSC card (TSC card 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 15600 switches to the standby TSC card. In the case of a TSC card protection switch, the alarm clears after the other cards establish communication with the newly active TSC card. If the alarm persists, the problem lies with the physical path of communication from the TSC card to the reporting card. The physical path of communication includes the TSC card, 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 display the provisioned type.

If the actual card type and the provisioned card type do not match, see the "MEA" alarm on page 2-95 for the reporting card.

Step 2 Complete the "Soft-Reset a Card Using CTC" procedure on page 2-136 for the alarmed card. For the LED behavior, see the "2.7 LED Behavior" section on page 2-125.

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

Step 3 If CONTBUS-IO-A is raised on several cards at the same time, complete the "Reset a Card with a Card Pull (Reseat)" procedure on page 2-138.

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 SRV LED indicates an active card.

Step 5 If the CTC reset does not clear the alarm, complete the "Reset a Card with a Card Pull (Reseat)" procedure on page 2-138 for the reporting card.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15600. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 6 If the reset card has not rebooted successfully, or the alarm has not cleared, call Cisco TAC (1-800-553-2447). If the Cisco TAC technician tells you to reseat the card, complete the "Reset a Card with a Card Pull (Reseat)" procedure on page 2-138. If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the "Replace a TSC Card" procedure on page 2-142.

2.6.32 CONTBUS-IO-B

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

Logical Object: EQPT

A TSC card B to Shelf Communication Failure alarm occurs when the active Slot 10 TSC card (TSC card B) has lost communication with another card in the shelf. The other card is identified by the Object column in the CTC alarm window.

The CONTBUS-IO-B alarm might appear briefly when the ONS 15600 switches to the protect TSC card. In the case of a TSC card protection switch, the alarm clears after the other cards establish communication with the newly active TSC card. If the alarm persists, the problem lies with the physical path of communication from the TSC card to the reporting card. The physical path of communication includes the TSC card, 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 display the provisioned type.

If the actual card type and the provisioned card type do not match, see the "MEA" alarm on page 2-95 for the reporting card.

Step 2 Complete the "Soft-Reset a Card Using CTC" procedure on page 2-136 for the alarmed card. For the LED behavior, see the "2.7 LED Behavior" section on page 2-125.

Step 3 If the alarm object is the standby Slot 5 TSC card, complete the "Reset a Card with a Card Pull (Reseat)" procedure on page 2-138.

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 "Soft-Reset a Card Using CTC" procedure on page 2-136.

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 SRV LED indicates an active card.

Step 6 If the CTC reset does not clear the alarm, complete the "Reset a Card with a Card Pull (Reseat)" procedure on page 2-138 for the reporting card.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15600. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 7 If the reset card has not rebooted successfully, or the alarm has not cleared, call Cisco TAC (1-800-553-2447). If the Cisco TAC technician tells you to reseat the card, complete the "Reset a Card with a Card Pull (Reseat)" procedure on page 2-138. If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the "Replace a TSC Card" procedure on page 2-142.

2.6.33 CONTCOM

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

Logical Object: EQPT

The Interconnection Control Communication Failure alarm occurs when the internal messaging processor on the reporting active TSC card fails.

A TSC card should boot and be in the ready state within approximately five minutes. If the CONTCOM alarm clears within this time frame and the TSC card goes to standby or active mode as applicable, no action is necessary.

If the communication equipment on the backplane fails, a CONTBUS alarm occurs instead of a CONTCOM alarm.

Clear the CONTCOM Alarm

Step 1 Complete the "Soft-Reset a Card Using CTC" procedure on page 2-136.

Step 2 If the CTC reset does not clear the alarm, complete the "Reset a Card with a Card Pull (Reseat)" procedure on page 2-138.

Step 3 If the alarm does not clear, complete the "Replace a TSC Card" procedure on page 2-142.

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).

Step 5 When the alarm has been cleared, complete the "Soft-Reset a Card Using CTC" procedure on page 2-136 as needed.

2.6.34 CTNEQPT-PB-A

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

Logical Object: EQPT

The SSXC-0 Data Payload Bus Interconnect Failure alarm occurs when the data path interconnection between equipment from SSXC-0 (Slot 6) to inbound or outbound traffic (OC-N) card slots has a failure. The SSXC card and the reporting card are no longer communicating through the backplane. The problem exists in the SSXC card, the reporting traffic card, or the backplane. If more than one traffic card on the shelf raises this alarm, the TSC card clears this alarm on the traffic cards and raises it alarm against SSXC-0.

Note When an alarm includes a numeric or alphabetical designation, it indicates whether the alarm applies to the first or second card of a specific type on the shelf. A zero or A indicates that the alarm occurs against the first card of its type, from left to right, in the shelf. A one or B indicates that the alarm occurs against the second card of its type in the shelf.

Note If you insert a new TSC card that has the same version of software as the active and standby TSC card, it takes approximately three minutes for the standby TSC card to become available.

Note It takes approximately 20 minutes for the active TSC card to transfer the system software to the newly installed TSC card. Software transfer occurs in instances where different software versions exist on the two cards. When the transfer completes, the TSC card reboots and goes into standby mode after approximately three minutes.

Clear the CTNEQPT-PB-A Alarm

Step 1 If the alarm occurs against a single traffic (OC-N) card, continue with Step 2. If the alarm occurs against multiple traffic cards, it indicates a problem with the SSXC card. Continue with Step 6.

Step 2 If the traffic card ports are part of a path protection, switch the single circuit on the span using instructions in the "Maintain the Node" chapter in the *Cisco ONS 15600 Procedure Guide*. If the ports are part of a 1+1 protection group, complete the "Initiate a 1+1 Protection Port Force Switch Command" procedure on page 2-128.

Step 3 Complete the "Hard-Reset a Card Using CTC" procedure on page 2-137.

Step 4 If the CTC reset does not clear the alarm, complete the "Reset a Card with a Card Pull (Reseat)" procedure on page 2-138 for the reporting card.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15600. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 5 If the alarm does not clear, complete the appropriate procedure in the "2.8.4 Physical Card Reseating, Resetting, and Replacement" section on page 2-138.

Note If the traffic card is implicated and you are able to continue using the traffic card with one port out of service, perform a bridge and roll to move the port traffic to a free port. Refer to the "Manage Circuits" chapter in the *Cisco ONS 15600 Procedure Guide* for instructions. Label the bad port and take it out of service until the card can be replaced.

Step 6 If you replace the traffic card and the alarm does not clear, an SSXC card problem is indicated. If an automatic switch to the alternate copy SSXC card occurred, the SSXC card can be serviced. If traffic has not switched, request a preferred copy switch by completing the "Request a Cross-Connect Card Preferred Copy Switch" procedure on page 2-138.

To determine which SSXC card is the preferred copy and whether it is currently being used, in node view go to the Maintenance > Preferred Copy window. The Data Copy area Preferred field shows Copy A or Copy B. The Currently Used field shows the copy being used.

Note In CTC, Copy A refers to the SSXC card in Slot 6. Copy B refers to the SSXC card in Slot 8. Either copy might be chosen as the preferred copy SSXC card. The other SSXC card is called the alternate SSXC card in this chapter.

Continue with Step 7.

Step 7 Perform a CTC soft reset on the SSXC card by completing the following steps:

a. Display node view.

b. Position the CTC cursor over the card.

c. Right-click and choose **Soft-reset Card** from the shortcut menu.

d. Click **Yes** in the Soft-reset Card dialog box.

Step 8 If the CTC reset does not clear the alarm, complete the "Reset a Card with a Card Pull (Reseat)" procedure on page 2-138 for the alarmed card.

Step 9 If the alarm does not clear, complete the "Replace an SSXC Card" procedure on page 2-139.

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) to report a Service-Affecting (SA) problem.

Step 11 Depending on which card raised the alarm, perform the following actions:

- If traffic was manually switched in a 1+1 protection group, revert traffic to the original port by completing the "Clear a 1+1 Protection Port Force or Manual Switch Command" procedure on page 2-129.
- If traffic was manually switched in a path protection, revert traffic to the original path by completing the "Clear a Path Protection Span External Switching Command" procedure on page 2-133.

Note If an automatic switch to the alternate copy SSXC card occurred, traffic is automatically restored to the preferred copy.

2.6.35 CTNEQPT-PB-B

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

Logical Object: EQPT

The SSXC-1 Data Payload Bus Interconnect Failure alarm occurs when the data path interconnection fails between equipment from SSXC-1 (Slot 8) and traffic card slots. If more than one traffic card on the shelf raises this alarm, the TSC card clears the alarm on the traffic cards and raises the alarm against the SSXC-1.

Note In CTC, Copy A refers to the SSXC card in Slot 6/7. Copy B refers to the SSXC card in Slot 8/9. Either copy might be chosen as the preferred copy SSXC card. The other SSXC card is called the alternate SSXC card in this chapter.

Clear the CTNEQPT-PB-B Alarm

Step 1 Complete the "Clear the CTNEQPT-PB-A Alarm" procedure on page 2-37.

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.

2.6.36 CXCHALT

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

Logical Object: EQPT

An SSXC Operation Suspended alarm indicates that operation on the alternate SSXC card has halted because of problems in fan tray 2, which services controller cards including the SSXC cards.

The CXCHALT alarm occurs five minutes after a fan failure alarm such as the "FAN-DEGRADE" alarm on page 2-58, the "FAN-FAIL" alarm on page 2-58, the "IMPROPRMVL (EQPT, PIM, PPM)" alarm on page 2-73, or the "FAN-FAIL-PARTIAL" alarm on page 2-59 halts alternate SSXC operation.

Caution If a CXCHALT occurs due to a fan failure, you should move a working fan assembly from tray 1 or 3 and install it in the tray 2 position because the remaining working SSXC card can be damaged in as little as 15 minutes. If damage occurs to the remaining SSXC Card, it restarts and then fails. Traffic is dropped until a replacement is installed.

Clear the CXCHALT Alarm

Step 1 Troubleshoot the fan alarm by following the "Clear the FAN-FAIL Alarm" procedure on page 2-58, which includes fan replacement.

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.

2.6.37 DATAFLT

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

Logical Object: NE

The Software Data Integrity Fault alarm occurs when the TSC exceeds its flash memory capacity.

Caution Configurations more than three minutes old are saved. Those newer than three minutes are not saved.

Clear the DATAFLT Alarm

Step 1 Complete the "Soft-Reset a Card Using CTC" procedure on page 2-136.

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).

2.6.38 DBOSYNC

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

Logical Object: NE

The Standby Database Out of Synchronization alarm occurs when the standby TSC card "To be Active" database does not synchronize with the active database on the active TSC card.

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

Clear the DBOSYNC Alarm

Step 1 Save a backup copy of the active TSC card database. Refer to the "Maintain the Node" chapter in the *Cisco ONS 15600 Procedure Guide* for instructions.

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

- **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).

2.6.39 DUP-IPADDR

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

Logical Object: NE

The Duplicate IP Address alarm indicates that the alarmed node IP address is already in use within the same DCC area. When this happens, 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 by completing the following steps:

- **a.** Connect to the alarmed node using the Craft port on the ONS 15600 chassis.
- **b.** Begin a CTC session.
- **c.** 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 formerly duplicated node IDs. (For instructions to log in or log out, refer to the "Set Up PC and Log Into the GUI" chapter in the *Cisco ONS 15600 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).

2.6.40 DUP-NODENAME

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

Logical Object: NE

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

Clear the DUP-NODENAME Alarm

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

Step 2 In the Node Name field, enter a unique name for the node.

Step 3 Click **Apply**.

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

2.6.41 ENCAP-MISMATCH-P

The ENCAP-MISMATCH-P alarm is not used in this platform in this release. It is reserved for future development.

2.6.42 EOC

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

Logical Object: OCN

The SONET DCC Termination Failure alarm occurs when the ONS 15600 loses its DCC. Although this alarm is primarily SONET, it can apply to dense wavelength division multiplexing (DWDM) in other platforms.

The section DCC (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 15600 uses the DCC on the SONET section layer to communicate network management information.

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

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

Note If a circuit shows an incomplete 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 2-87 is also reported, complete the "Clear the LOS (OCN) Alarm" procedure on page 2-87. (This procedure is also used for EOC.)

Step 2 If the "SF-L" condition on page 2-110 is reported, complete the "Clear the SD-L Condition" procedure on page 2-109. (This procedure is also used for EOC.)

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. If they are not, correct them. For more information about fiber connections and terminations, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15600 Procedure Guide*.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15600. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

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 SRV LED on each OC-N card is green.

Step 4 When the LEDs on the OC-N cards are correctly illuminated, complete the "2.8.5 Verify or Create Node DCC Terminations" procedure on page 2-145.

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 by completing the following steps:

a. Confirm that the OC-N card shows a green LED in CTC or on the physical card.

A green SRV LED indicates an active card.

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

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

d. Verify that the 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 click **IS** from the drop-down list. Click **Apply**.

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

Caution Using an optical test set disrupts service on the OC-N card. It could be necessary to manually switch traffic carrying circuits over to a protection path. Refer to the "2.8.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-128 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 "1.9.3 Optical Traffic Card Transmit and Receive Levels" section on page 1-69 for information.

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 15600 Procedure Guide*.

Step 10 If fiber connectors are properly fastened and terminated, complete the "Soft-Reset a Card Using CTC" procedure on page 2-136.

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

Resetting the active TSC card switches control to the standby TSC card. If the alarm clears when the ONS 15600 node switches to the standby TSC card, the user can assume that the previously active card is the cause of the alarm.

Step 11 If the TSC card reset does not clear the alarm, delete the problematic SDCC termination by completing the following steps:

a. From card view, click **View > Go to Previous View** if you have not already done so.

b. Click the **Provisioning > Comm Channels > SDCC** tabs.

c. Highlight the problematic DCC termination.

d. Click **Delete**.

e. Click **Yes** in the Confirmation Dialog box.

Step 12 Recreate the SDCC termination. Refer to the "Turn Up Network" chapter in the *Cisco ONS 15600 Procedure Guide* for instructions.

Step 13 Verify that both ends of the DCC have been recreated at the optical ports.

Step 14 If the alarm has not cleared, call Cisco TAC (1-800-553-2447). If the Cisco TAC technician tells you to reseat the card, complete the "Reset a Card with a Card Pull (Reseat)" procedure on page 2-138. If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the "Replace a TSC Card" procedure on page 2-142.

2.6.43 EOC-L

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

Logical Object: OCN

The Line DCC Termination Failure alarm occurs when the ONS 15600 loses its line DCC termination. The line DCC (LDCC) consists of nine bytes, D4 through D12, in the SONET overhead. The bytes convey information about OAM&P. The ONS 15600 uses the LDCCs on the SONET line layer to communicate network management information.

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

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

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

Clear the EOC-L Alarm

Step 1 Complete the "Clear the EOC Alarm" procedure on page 2-42.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15600. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

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 "Reset a Card with a Card Pull (Reseat)" procedure on page 2-138 for the affected card. (The procedure is similar for all cards.) If the Cisco TAC technician tells you to remove the card and reinstall a new one, replace it using the appropriate procedure in the "2.8.4 Physical Card Reseating, Resetting, and Replacement" section on page 2-138.

2.6.44 EQPT (CAP)

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

Logical Object: CAP

An Equipment Failure alarm for the CAP indicates that the customer access panel has a physical failure. Log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.45 EQPT (EQPT)

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

Logical Object: EQPT

An Equipment Failure alarm indicates that a hardware failure has occurred on the reporting card. If the EQPT alarm occurs with a BKUPMEMP alarm, refer to the "2.6.21 BKUPMEMP" section on page 2-27. 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. The standby path generates a path-type alarm.

Clear the EQPT Alarm

Step 1 Complete the appropriate procedure in the "2.8.3 CTC Card Resetting and Switching" section on page 2-136 section.

Step 2 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. For LED appearance, see the "2.7 LED Behavior" section on page 2-125.

Step 3 If the CTC reset does not clear the alarm, complete the appropriate procedure in the "2.8.4 Physical Card Reseating, Resetting, and Replacement" section on page 2-138 section procedure for the reporting card.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15600. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 4 If the physical reseat of the card fails to clear the alarm, complete the "Replace an OC-48 Card or OC-192 Card" section on page 2-140 procedure for the reporting card.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the ""2.8.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-128 for more information.

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

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

2.6.46 EQPT (PIM)

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

Logical Object: PIM

The EQPT alarm for the ASAP card pluggable input-output module 4PIO (or PIM) is raised when all ports on the four-port module fail.

Clear the EQPT (PIM) Alarm

Step 1 Complete the "Replace an ASAP 4PIO (PIM) Module" procedure on page 2-143.

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.

2.6.47 EQPT (PPM)

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

Logical Object: PPM

The EQPT alarm for the SFP (PPM) is raised when one of the SFP (PPM) ports on a four-port 4PIO (PIM) module fails.

Clear the EQPT (PPM) Alarm

Step 1 Replace the alarmed SFP (PPM) by completing the "Replace an ASAP SFP (PPM) Module" procedure on page 2-144.

Step 2 If the alarm does not clear, move traffic off any active PPMs (SFPs). See the "Initiate a 1+1 Protection Port Force Switch Command" procedure on page 2-128. After switching traffic, replace the 4PIO (PIM) using the instructions in the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15600 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) to report a Service-Affecting (SA) problem.

2.6.48 EQPT-BOOT

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

Logical Object: EQPT

An Equipment Boot Failure alarm occurs when a TSC card, SSXC card, or traffic (OC-N) card does not fully boot from the restart point after self-rebooting three times.

Clear the EQPT-BOOT Alarm

Step 1 Complete the "Clear the EQPT Alarm" procedure on page 2-45.

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.

2.6.49 EQPT-CC-PIM

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

Logical Object: PIM

The EQPT Alarm on a Carrier or 4PIO (PIM) is raised when an LOF or LOS alarm is shown on an ASAP card but this alarm is not also shown against the 4PIO (PIM) that carries the affected traffic. If multiple four-port 4PIOs (PIMs) do not show this LOF or LOS alarm, the EQPT-CC-PIM alarm raises against the ASAP carrier card itself.

Clear the EQPT-CC-PIM Alarm

Step 1 Complete the "Replace an ASAP 4PIO (PIM) Module" procedure on page 2-143.

Step 2 If the alarm does not clear, move traffic off any active 4PIOs (PIMs). Procedures and guidelines to do this are located in the "Maintain the Node" chapter in the *Cisco ONS 15600 Procedure Guide*. Then complete the "Replace an ASAP Carrier Module" procedure on page 2-143 and reinstall the 4PIOs (PIMs) by completing the "Replace an ASAP 4PIO (PIM) Module" procedure on page 2-143. For more information about removing or installing these modules, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15600 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) to report a Service-Affecting (SA) problem.

2.6.50 EQPT-HITEMP

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

Logical Object: EQPT

The Equipment Failure High Temperature alarm occurs when the TSC card, SSXC card, or traffic (OC-N) card internal temperature exceeds 185 degrees Fahrenheit (85 degrees Celsius).

Clear the EQPT-HITEMP Alarm

Step 1 Ensure that the room temperature is not abnormally high.

Step 2 If the room temperature is not the cause of the alarm, ensure that filler modules are installed in the ONS 15600 empty slots. Filler modules help airflow.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15600. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 3 If the "FAN-DEGRADE" alarm on page 2-58 or the "FAN-FAIL" alarm on page 2-58 accompanies the alarm, complete the "Clear the FAN-FAIL Alarm" procedure on page 2-58.

Step 4 If the alarm does not clear, check the condition of the air filter to see if it needs cleaning or replacement. Replace the air filter using the procedure located in the "Maintain the Node" chapter in the *Cisco ONS 15600 Procedure Guide* as needed.

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).

2.6.51 EQPT-PIM-PPM

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

Logical Object: PPM

The EQPT alarm for an SFP (PPM) is raised when a 4PIO (PIM) is reporting low electrical amplitude from an SFP (PPM). If this symptom shows up from multiple SFPs (PPMs) then the alarm should be against the 4PIO (PIM). Otherwise the alarm will be against the SFP (PPM) creating the problem.

Clear the EQPT-PIM-PPM Alarm

Step 1 Move any traffic away from the affected SFP (PPM), using guidelines and instructions in the "Maintain the Node" chapter in the *Cisco ONS 15600 Procedure Guide*, then replace the alarmed SFP (PPM) module using instructions in that guide.

Step 2 If the alarm does not clear, move any traffic away from the affected 4PIO (PIM), using the instructions in the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15600 Procedure Guide*, and replace the 4PIO (PIM).

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) to report a Service-Affecting (SA) problem.

2.6.52 E-W-MISMATCH

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

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, in the ONS 15600 system, Slot 2 is west and Slot 12 is east.

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

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

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

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

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

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

Step 5 Label the span ends on the diagram with the same information.

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 15600 Procedure Guide* for more information about cable installation in 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 **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

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

Step 10 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) 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 ID or Node ID Number" procedure on page 2-127 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 by completing the following steps:

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

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

c. Click **Create**.

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

e. Click **Finish**.

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

Step 7 Change the West Line drop-down list to the slot you recorded for the East Line in Step 3.

Step 8 Change the East Line drop-down list 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) to report a Service-Affecting (SA) problem.

2.6.53 EXERCISE-RING-FAIL

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

Logical Object: OCN

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

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

Clear the EXERCISE-RING-FAIL Condition

Step 1 Look for and clear, if present, the "LOF (OCN)" alarm on page 2-83, the "LOS (OCN)" alarm on page 2-87, or a BLSR alarm.

Step 2 Complete the "Initiate an Exercise Ring Switch on a BLSR" procedure on page 2-135.

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).

2.6.54 EXERCISE-RING-REQ

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

Logical Object: OCN

The Exercise Ring command issues ring protection switching of the requested channel without completing the actual bridge and switch. The EXERCISE-RING-REQ condition indicates that the command is being issued on the near end node.

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

2.6.55 EXERCISE-SPAN-FAIL

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

Logical Object: OCN

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

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

Clear the EXERCISE-SPAN-FAIL Condition

Step 1 Look for and clear, if present, the "LOF (OCN)" alarm on page 2-83, the "LOS (OCN)" alarm on page 2-87, or a BLSR alarm.

Step 2 Complete the "Initiate an Exercise Ring Switch on a BLSR" procedure on page 2-135.

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).

2.6.56 EXERCISING-RING

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

Logical Object: OCN

The Exercise Ring command issues span switching of the requested channel without completing the actual bridge and switch. The EXERCISING-RING condition is raised if the command was issued and accepted and the exercise is taking place. This condition appears on the network view Alarms and History tab, not on the Conditions tab.

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

2.6.57 EXERCISING-SPAN

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

Logical Object: OCN

The Exercise Span command issues span switching of the requested channel without completing the actual bridge and switch. The EXERCISING-SPAN condition is raised if the command was issued and accepted and the exercise is taking place. This condition appears on the network view Alarms and History tab, not on the Conditions tab.

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

2.6.58 EXT

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

Logical Object: ENVALRM

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

Clear the EXT Alarm

Step 1 Click the **Maintenance > Alarm Extenders > External Alarms** tab to gather further information about the EXT alarm.

Step 2 Follow your standard operating procedure to remedy environmental conditions that cause alarms. The alarm clears when the situation is remedied.

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).

2.6.59 EXTRA-TRAF-PREEMPT

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

Logical Object: OCN

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

Clear the EXTRA-TRAF-PREEMPT Alarm

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

Step 2 If a ring switch has occurred, clear the ring switch on the working system by following the appropriate alarm in this chapter. For more information about protection switches, refer to the “Maintain the Node” chapter in the *Cisco ONS 15600 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) to report a Service-Affecting (SA) problem.

2.6.60 FAILTOSW

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

Logical Object: OCN

The Failure to Switch to Protection Facility condition occurs when a working or protect electrical 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.

Step 2 If the condition does not clear, replace the working electrical (traffic) card that is reporting the higher priority alarm by following the correct replacement procedure in the "2.8.4 Physical Card Reseating, Resetting, and Replacement" procedure on page 2-138. This card is the working electrical card using the protect card and not reporting FAILTOSW.

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

Note If an ONS 15600 traffic (OC-N) card is implicated and you are able to continue using the traffic card with one port out of service, perform a bridge and roll to move the port traffic to a free port; refer to the "Manage Circuits" chapter in the *Cisco ONS 15600 Procedure Guide* for instructions. Label the bad port, and place it out of service until such time as the card can be replaced.

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

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

2.6.61 FAILTOSW-PATH

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

Logical Object: STSMON

The Fail to Switch to Protection Path condition occurs when the working circuit does not switch to the protection circuit on a path protection. Common causes of the FAILTOSW-PATH alarm include a missing or defective protect port, a lockout set on one of the path protection nodes, or path-level alarms that would cause a path protection switch to fail including the "AIS-P" condition on page 2-16, the "LOP-P" alarm on page 2-84, the "SD-P" condition on page 2-110, the "SF-P" condition on page 2-110, and the "UNEQ-P" alarm on page 2-121.

The "LOF (OCN)" alarm on page 2-83, the "LOS (OCN)" alarm on page 2-87, the "SD-L" condition on page 2-108, or the "SF-L" condition on page 2-110 can also occur on the failed path.

Clear the FAILTOSW-PATH Alarm in a Path Protection Configuration

Step 1 Look up and clear the higher priority alarm. Clearing this condition frees the standby card and clears the FAILTOSW-PATH condition. If the "AIS-P" condition on page 2-16, the "LOP-P" alarm on page 2-84, the "UNEQ-P" alarm on page 2-121, the "SF-P" condition on page 2-110, the "SD-P" condition on page 2-110, the "LOF (OCN)" alarm on page 2-83, the "LOS (OCN)" alarm on page 2-87, the "SD-L" condition on page 2-108, or the "SF-L" condition on page 2-110 are also occurring on the reporting port, complete the applicable alarm clearing procedure.

Step 2 If the alarm does not clear, physically check the fiber connections to the card and ports to ensure that they are securely fastened and intact. For more information about fiber connections and terminations, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15600 Procedure Guide*.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15600. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 3 Clear the attempted switch by completing the following steps:

a. In node view, click the **Circuits > Circuits** tabs.

b. Highlight the path where you tried to perform the switch. In the Switch State column, verify that the state is Clear. If it is not, select **Clear** from the list.

c. 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). If the alarm was reported against the ONS 15600, it is Service-Affecting (SA) and should be reported.

2.6.62 FAILTOSWR

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

Logical Object: OCN

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

FAILTOSWR clears in any of the following situations:

- A physical card pull of the active TSC card (done under Cisco TAC supervision).
- A node power cycle.
- A higher-priority event such as an external switch command.

- The next ring switch succeeds.
- The cause of the APS switch (such as the "SD-L" condition on page 2-108 or the "SF-L" condition on page 2-110) clears.

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

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

Clear the FAILTOSWR Condition in a Two-Fiber BLSR Configuration

Step 1 Perform the EXERCISE RING command on the reporting card by completing the following steps:

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

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

c. Select **Exercise Ring** in the drop-down list.

Step 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 FAILTOSW-RING 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 by completing the following steps:

a. Verify the LED status: a green SRV LED indicates an active card.

b. Double-click the card in CTC to display the card view.

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

d. Verify that the Admin State column lists the port as IS.

e. If the Admin State column lists the port as OOS,MT or OOS,DSBLD, click the column and choose **IS**. Click **Apply**.

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 "2.8.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-128 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 15600 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 "1.9.3 Optical Traffic Card Transmit and Receive Levels" section on page 1-69 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 "Replace an OC-48 Card or OC-192 Card" procedure on page 2-140 for the protect standby OC-N card.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.8.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-128 for commonly used traffic-switching procedures.

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

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

Step 14 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.63 FAILTOSWS

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

Logical Object: OCN

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

- A physical card pull of the active TSC card 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 2-108 or the "SF-L" alarm on page 2-110) clears.

Clear the FAILTOSWS Condition

Step 1 Perform the EXERCISE SPAN command on the reporting card by completing the following steps:

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 by completing the following steps:

a. Verify the LED status: A green SRV LED indicates an active card.

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

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

d. Verify that the Admin State column lists the port as IS.

e. If the Admin State column lists the port as OOS,MT or OOS,DSBLD, click the column and choose **IS**. Click **Apply**.

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 "2.8.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-128 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 15600 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 "1.9.3 Optical Traffic Card Transmit and Receive Levels" section on page 1-69 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 "Replace an OC-48 Card or OC-192 Card" procedure on page 2-140 for the protect standby OC-N card.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.8.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-128 for commonly used traffic-switching procedures.

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

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

Step 14 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.64 FAN-DEGRADE

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

Logical Object: FAN

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

Clear the FANDEGRADE Alarm

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

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).

2.6.65 FAN-FAIL

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

Logical Object: FAN

The Fan Failure alarm occurs when two or more fans (out of a total of six) have failed. The ONS 15600 has no standby fan. All fans should be active. The FAN-FAIL alarm can be accompanied by the "MFGMEM (FAN)" alarm on page 2-97 against the fan. This alarm can also be raised in conjunction with a "PWR" alarm on page 2-102.

Clear the FAN-FAIL Alarm

Step 1 If the "MFGMEM (FAN)" alarm on page 2-97 is also reported against the fan, complete the "Clear the MFGMEM (FAN) Alarm" procedure on page 2-97.

Step 2 If the alarm does not clear, check the condition of the air filter to see if it needs cleaning or replacement using the procedure located in the "Maintain the Node" chapter in the *Cisco ONS 15600 Procedure Guide*.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15600. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 3 If the alarm does not clear and if the filter is clean, remove the reporting fan trays from the ONS 15600.

Step 4 Reinsert the fan trays, making sure you can hear the fans start operating.

Fans should run immediately when correctly inserted.

Step 5 If the alarm does not clear or if the fans do not run, replace the fan trays using the procedure located in the "Maintain the Node" chapter in the *Cisco ONS 15600 Procedure Guide*.

Step 6 If the alarm does not clear or if the replacement fan trays do not operate correctly, 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.

2.6.66 FAN-FAIL-PARTIAL

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

Logical Object: FAN

The Partial Fan Failure alarm occurs when one of the six fans in the shelf fails.

Troubleshoot with the "Clear the FAN-FAIL Alarm" procedure on page 2-58 procedure. If the alarm does not clear, log on to http://www.cisco.com/tac for more information or call Cisco TAC at 1-800-553-2447.

2.6.67 FAN-PWR

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

Logical Object: FAN

The Fan Power Failure alarm occurs when a power feed (A or B) from the shelf to fan tray 1, 2, or 3 fails. Because fans are not able to differentiate the power feeds, there is only one alarm for A or B failure.

Clear the FAN-PWR Alarm

Step 1 Remove the reporting fan trays from the ONS 15600.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15600. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 2 Reinsert the fan trays, making sure you hear the fans start to operate.

Fans should run immediately when correctly inserted.

Step 3 If the alarm does not clear or if the fans do not run, replace the fan trays using the procedure located in the "Maintain the Node" chapter in the *Cisco ONS 15600 Procedure 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).

2.6.68 FE-EXERCISING-RING

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

Logical Object: OCN

The Exercise Ring command issues ring protection switching of the requested channel without completing the actual bridge and switch. The Far-End Exercising Ring condition indicates that the command is being executed on the far-end node.

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

2.6.69 FE-FRCDWKSWPR-RING

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

Logical Object: OCN

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

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

Clear the FE-FRCDWKSWPR-RING Condition

Step 1 To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an FE-AIS condition from the OC-48 card in Slot 12 of Node 1 could link to the main AIS condition from an OC-48 card in Slot 6 of Node 2.

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

Step 3 Clear the main alarm.

Step 4 If the FE-FRCDWKSWPR-RING condition does not clear, complete the "Clear a BLSR External Switching Command" procedure on page 2-136.

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).

2.6.70 FE-FRCDWKSWPR-SPAN

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

Logical Object: OCN

The Far End Working Facility Forced to Switch to Protection Span condition occurs when a far-end 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 WKSWPR.

Clear the FE-FRCDWKSWPR-SPAN Condition

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

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

Step 3 Clear the main alarm.

Step 4 If the FE-FRCDWKSWPR-SPAN condition does not clear, complete the "Clear a BLSR External Switching Command" procedure on page 2-136.

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).

2.6.71 FE-LOCKOUTOFPR-ALL

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

2.6.72 FE-LOCKOUTOFPR-SPAN

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

Logical Object: OCN

The Far-End Lock Out of Protection Span condition occurs when a BSLR span is locked out of the protection system from a 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.

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 2-136.

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).

2.6.73 FE-MANWKSWPR-RING

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

Logical Object: OCN

The Far End Ring Manual Switch of Working 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 2-136.

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).

2.6.74 FE-MANWKSWPR-SPAN

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

Logical Object: OCN

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

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.

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 2-136.

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).

2.6.75 FE-SDPRLF

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

Logical Object: OCN

The Far End Signal Degrade Protection Line Failure alarm occurs when an APS channel "SD-L" condition on page 2-108 occurs on the far-end protect card.

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

Clear the FE-SDPRLF Alarm

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

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

Step 3 Clear the main alarm, which in this case is probably the "SD-L" condition on page 2-108. If not, refer to the appropriate alarm section in this chapter in this chapter for instructions.

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

2.6.76 FE-SF-RING

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

Logical Object: OCN

The Far End Signal Failure BER Threshold Passed for a BLSR Ring alarm indicates that an "SF-L" alarm on page 2-110 has occurred at the far-end node, and it has in turn affected the ring's traffic.

Clear the FE-SF-RING Alarm

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

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

Step 3 Clear the main alarm, which in this case is probably the "SF-L" condition on page 2-110. If not, refer to the appropriate alarm section in this chapter in this chapter for 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).

2.6.77 FE-SF-SPAN

The FE-SF-SPAN condition is not used in this platform in this release. It is reserved for future development.

2.6.78 FORCED-REQ

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

Logical Object: STSMON

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.

Clear the FORCED-REQ Condition

Step 1 Complete the "Clear a 1+1 Protection Port Force or Manual Switch Command" procedure on page 2-129.

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).

2.6.79 FORCED-REQ-RING

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

Logical Object: OCN

The Force Switch Request Ring condition applies to optical trunk cards when the FORCE RING command is applied to 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 WKSWPR. 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 2-136.

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).

2.6.80 FORCED-REQ-SPAN

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

Logical Object: OCN

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

This condition can also 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 2-136.

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).

2.6.81 FRCDSWTOINT

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

Logical Object: NE-SREF

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

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

2.6.82 FRCDSWTOPRI

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

Logical Objects: EXT-SREF, NE-SREF

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

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

2.6.83 FRCDSWTOSEC

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

Logical Objects: EXT-SREF, NE-SREF

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

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

2.6.84 FRCDSWTOTHIRD

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

Logical Objects: EXT-SREF, NE-SREF

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

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

2.6.85 FREQ-MISMATCH

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

Logical Object: EQPT

The Frequency Mismatch alarm occurs when one of the two TSC cards has a timing module failure that causes an inconsistency between the TSC card timing frequencies. This alarm can be caused by the active or standby TSC card.

The ONS 15600 checks timing frequency synchronization in 83-minute (1:23 hours and minutes) cycles. The FREQ-MISMATCH alarm occurs if two consecutive timing check cycles show frequency mismatches. The alarm is cleared if one cycle shows a timing frequency match between the TSC cards.

Clear the FREQ-MISMATCH Alarm

Step 1 Complete the "Replace a TSC Card" procedure on page 2-142 for the standby TSC card.

Step 2 Wait for two intervals of 83 minutes (2:46 hours and minutes) and check the node view Alarms window to see whether the alarm is cleared.

During the initial 83-minute synchronization check cycle when the replacement standby TSC card is booting up, the replacement TSC card is attaining the timing from the BITS or internal source so it is normal that the two TSC cards are not synchronized. The ONS 15600 system disregards the result of this check cycle and begins keeping track of synchronization in the second 83-minute cycle. If the result of the cycle shows that the TSC cards are synchronized properly, the alarm is cleared.

Step 3 If the FREQ-MISMATCH alarm did not clear after two timing check cycles, it means that the second timing cycle resulted in a mismatch. Wait a third 83-minute cycle and check the alarm again.

If the alarm has cleared, it means a third cycle showed that the TSC card timing modules were synchronized. If the alarm remains, it means that the ONS 15600 system has had two frequency mismatch cycles, and indicates a problem with the other TSC card.

Step 4 If the FREQ-MISMATCH alarm remains after three 83-minute cycles, complete the "Soft-Reset a Card Using CTC" procedure on page 2-136 to make the TSC card standby.

Step 5 Complete the "Reset a Card with a Card Pull (Reseat)" procedure on page 2-138 for the standby TSC card.

The card removal and reboot temporarily clears the alarm.

Step 6 Wait for three intervals of 83 minutes (4:09 hours and minutes) and check CTC to see if the FREQ-MISMATCH alarm has recurred. If it has not recurred, the problem is solved.

Step 7 If the alarm has recurred after both TSC cards have been replaced, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.86 FRNGSYNC

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

Logical Object: NE-SREF

The Free Running Synchronization Mode condition occurs when the reporting ONS 15600 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 BITS timing source. After the 24-hour holdover period expires, timing slips could begin to occur on an ONS 15600 node relying on an internal clock.

Note If the ONS 15600 is configured to operate from its internal clock, disregard the FRNGSYNC condition.

Clear the FRNGSYNC Condition

Step 1 If the ONS 15600 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 15600 Reference Manual* for more information about it.

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 2-118 and the "SYNCSEC" alarm on page 2-119.

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).

2.6.87 FSTSYNC

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

Logical Object: EQPT

The Fast Synchronization Mode condition occurs when the ONS 15600 synchronizes its clock modules. Since the ONS 15600 uses Stratum 3E timing, synchronization can take about 12 minutes. This condition occurs on the TSC card where the timing distribution is sourced. Whenever this condition is active, any timing or controller switching might affect the traffic. Errorless switching is not guaranteed.The "UNPROT-SYNCCLK" alarm on page 2-122 can accompany this condition if there is no timing protection is available while the clock is synchronizing.

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

2.6.88 FULLPASSTHR-BI

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

Logical Object: OCN

The Bidirectional Full Pass-Through Active condition occurs on a nonswitching node in a BLSR when the protect channels on the node are active and carrying traffic and a change is present in the receive K byte from "No Request." (Both data and K bytes are in pass-through mode.)

Clear the FULLPASSTHR-BI Condition

Step 1 Complete the "Clear a BLSR External Switching Command" procedure on page 2-136.

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.

2.6.89 GFP-LFD

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

Logical Object: POS

The Generic Framing Procedure (GFP) Loss of Frame Delineation 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.

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.

2.6.90 GFP-UP-MISMATCH

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

Logical Object: POS

The GFP User Payload Mismatch alarm is raised when the ASAP card is provisioned with different values such as the near-end port media type not matching the remote port media type.

Clear the GFP-UP-MISMATCH Alarm

Step 1 Double-click the alarmed card to display the card view.

Step 2 Click the **Provisioning > Ethernet > POS Ports** tabs.

Step 3 Verify that the ENCAP CRC and Framing Type columns contain the same value. If they do not, change the incorrect one (depending on your network's requirements).

Step 4 Click **Apply**.

Step 5 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.

2.6.91 HELLO

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

Logical Object: OCN

The Open Shortest Path First (OSPF) Hello Fail alarm occurs when SONET DCC termination OSPF area IDs are mismatched between two DCC terminations for a span. On a span between two ONS 15600s, this alarm occurs at both nodes containing the mismatched DCC area IDs. On a span between an ONS 15600 and an ONS 15454, this alarm is raised only on the ONS 15600 node. Mismatched OSPF area IDs can cause CTC to lose management across the link.

Clear the HELLO Alarm

Step 1 Log into both end nodes with the DCC terminations.

Step 2 On the nodes where the alarm occurred, record the slot and port (from the Slot column and Port column in the Alarms window) that the Hello alarm occurs against. This information helps you determine which DCC termination is mismatched.

Tip You can log into another node by going to network view and double-clicking the node.

Step 3 On one node, in node view, click the **Provisioning > Network > OSPF** tabs.

Step 4 In the DCC OSPF Area ID Table area, locate the alarmed DCC termination by comparing slot and port numbers to the slot and port number indicated in the alarm on the node.

Step 5 Click the Area ID column cell for the mismatched DCC termination.

Step 6 Change the area ID in the cell to the same ID as its partner DCC termination. (The ONS 15600 defaults to 0.0.0.0 format addresses.)

Step 7 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).

2.6.92 HI-LASERBIAS

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

Logical Object: PPM

The Equipment High Transmit Laser Bias Current alarm indicates that the card laser has reached the maximum laser bias tolerance.

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

Clear the HI-LASERBIAS Alarm

Step 1 Complete the "Replace an ASAP Carrier Module" procedure on page 2-143, "Replace an ASAP 4PIO (PIM) Module" procedure on page 2-143, or "Replace an ASAP SFP (PPM) Module" procedure on page 2-144, depending upon which part is bad.

Caution Removing a facility or card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Refer to the *Cisco ONS 15600 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).

2.6.93 HI-RXPOWER

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

Logical Object: OCN

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

Note For more information about ASAP cards, refer to the *Cisco ONS 15600 Reference Manual*. For more information about how they and their component modules are provisioned, refer to the *Cisco ONS 15600 Procedure Guide*.

Clear the HI-RXPOWER Alarm

Step 1 Determine whether there are any faults for the SFP (PPM) or 4PIO (PIM) modules associated with the errored circuit. If there are, troubleshoot them using the procedures in this manual.

Step 2 If no faults are present on the other port(s) of the transmit or receive card, use a known-good loopback cable to complete the "Create the Facility (Line) Loopback or Payload Loopback on the Source Optical Port" procedure on page 1-7 and test the loopback.

Step 3 If the carrier module itself is bad and you need all of its port bandwidth, complete the "Replace an ASAP Carrier Module" procedure on page 2-143. If the port is bad but you can move the traffic to another port, complete the "Replace an ASAP 4PIO (PIM) Module" procedure on page 2-143 or "Replace an ASAP SFP (PPM) Module" procedure on page 2-144 as needed.

Caution Removing hardware that currently carries traffic can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.8.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-128 for commonly used traffic-switching procedures.

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

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).

2.6.94 HI-TXPOWER

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

Logical Objects: PPM

The Equipment High Transmit Power alarm is an indicator on the ASAP 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 ASAP cards, refer to the *Cisco ONS 15600 Reference Manual*.

Clear the HI-TXPOWER Alarm

Step 1 Display the ASAP card view.

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

Step 3 Increase the TX Power Low column value by 0.5 dBm.

Step 4 If the card transmit power setting cannot be increased without affecting the signal, complete the "Replace an ASAP SFP (PPM) Module" procedure on page 2-144.

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).

2.6.95 HLDOVRSYNC

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

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 15600 relying on an internal clock.

Clear the HLDOVRSYNC Condition

Step 1 Clear additional alarms that relate to timing, such as:

- 2.6.86 FRNGSYNC, page 2-67
- 2.6.87 FSTSYNC, page 2-67
- 2.6.111 LOF (BITS), page 2-82
- 2.6.116 LOS (BITS), page 2-86
- 2.6.127 MANSWTOINT, page 2-93
- 2.6.128 MANSWTOPRI, page 2-93
- 2.6.129 MANSWTOSEC, page 2-93
- 2.6.130 MANSWTOTHIRD, page 2-93
- 2.6.181 SWTOPRI, page 2-116
- 2.6.182 SWTOSEC, page 2-116
- 2.6.183 SWTOTHIRD, page 2-117
- 2.6.186 SYNC-FREQ, page 2-117
- 2.6.187 SYNCPRI, page 2-118
- 2.6.188 SYNCSEC, page 2-119
- 2.6.189 SYNCTHIRD, page 2-119

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 15600 Procedure Guide* to find one.

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.

2.6.96 IMPROPRMVL (CAP)

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

Logical Object: CAP

The Improper Removal CAP alarm occurs when a CAP is not correctly installed on the backplane or is missing altogether. The problem is not user serviceable. Contact the Cisco TAC at 1-800-553-2447.

2.6.97 IMPROPRMVL (EQPT, PIM, PPM)

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

Logical Objects: EQPT, PIM, PPM

The Improper Removal equipment (IMPROPRMVL (EQPT, PIM, PPM)) 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 TSC 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, or if no PPM is inserted into the 4PIO (PIM).
- Electrical issues such as short circuit or failure of DC-DC conversion.

Clear the IMPROPRMVL (EQPT, PIM, PPM) 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. However if none of these services is provisioned, you can delete an IS card.

Step 3 If any ports on the card are in service, place them out of service (OOS,MT) by completing the following steps:

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

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

Step 4 If a circuit has been mapped to the card, delete it using the procedure in the "Manage Circuits" chapter in the *Cisco ONS 15600 Procedure Guide*.

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 by completing the following steps:

a. Click **View > Go to Previous View** to return to node view.

b. If you are already in node view, click the **Provisioning > Protection** tabs.

c. Click the protection group of the reporting card.

d. Click **Delete**.

Step 6 If the card is provisioned for DCC, delete the DCC provisioning by completing the following steps:

a. Click the node view **Provisioning > Comm Channels > SDCC** tabs.

b. Click the slots and ports listed in DCC terminations.

c. Click **Delete** and click **Yes** in the dialog box that appears.

Step 7 If the card is used as a timing reference, change the timing reference by completing the following steps:

a. Click the **Provisioning > Timing > General** tabs.

b. Under NE Reference, click the drop-down arrow for **Ref-1**.

c. Change Ref-1 from the listed OC-N card to **Internal Clock**.

d. Click **Apply**.

Step 8 If the alarm does not 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.

2.6.98 IMPROPRMVL (EQPT for the SSXC or TSC Card)

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

Logical Object: EQPT

The Improper Removal SSXC, Traffic Card, or TSC card alarm occurs when a TSC card, SSXC card, or traffic (OC-N) card is physically removed from its slot. This alarm can occur if the card is recognized by CTC and the active TSC card but is not in service. For example, it could be inserted in the slot but not fully plugged into the backplane.

If the removed TSC card or SSXC card is the last one on the shelf, the severity is Critical (CR) and traffic is affected. Otherwise, the alarm is Minor (MN).

Caution Do not remove and reinsert (reseat) a card during a card reboot. If CTC begins to reboot a card before you remove the card, allow the card to finish rebooting. After the card reboots, delete the card in CTC again and physically remove the card before it begins to reboot.

Note After deleting a card in CTC, the software allows you approximately 15 seconds to physically remove the card before CTC begins a card reboot.

Clear the IMPROPRMVL (SSXC, TSC) Alarm

Step 1 Complete the "Reset a Card with a Card Pull (Reseat)" procedure on page 2-138 for the TSC card or SSXC. (The procedure is similar for both.)

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).

2.6.99 IMPROPRMVL (FAN)

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

Logical Object: FAN

The Improper Removal Fan alarm occurs when fan tray 1, 2, or 3 is physically removed from its slot.

Clear the IMPROPRMVL (FAN) Alarm

Step 1 Refer to the "Maintain the Node" chapter in the *Cisco ONS 15600 Procedure Guide* for procedures to replace the fan-tray assembly.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15600. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 2 If the fan tray does not run immediately, troubleshoot with the "Clear the FAN-FAIL Alarm" procedure on page 2-58.

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).

2.6.100 IMPR-XC

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

Logical Object: NE

The Improper Cross-Connect Card alarm indicates that the CXC card is being used rather than the SSXC (the preferred cross-connect card for R5.0 and onward). The alarm remains standing as long as a CXC is present on the node. Since a CXC card is still capable of passing traffic, the alarm is not Service-Affecting (SA). However, a system containing a CXC card and the current software release is not fully guaranteed for functionality.

Note IMPR-XC is an informational alarm and does not require troubleshooting. However, if you are experiencing cross-connect related problems at this site, also report this alarm to the Cisco TAC.

2.6.101 INTRUSION-PSWD

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

Logical Object: NE

The Security Intrusion Incorrect Password condition occurs after a user attempts a provisionable (by Superuser) number of unsuccessful logins, a login with an expired password, or an invalid password. The alarmed user is locked out of the system, and INTRUSION-PSWD condition is raised. 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 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).

2.6.102 INVMACADR

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

Logical Object: BPLANE

The Invalid MAC Address alarm occurs when the ONS 15600 MAC address retrieval fails and the node does not have a valid MAC address to support the operating system (OS). Do not attempt to troubleshoot an INVMACADR alarm. Contact the Cisco Technical Assistance Center (TAC) at (1-800-553-2447).

Clear the INVMACADR Alarm

Step 1 Check for any outstanding alarms that were raised against the active and standby TSC and resolve them.

Step 2 At the earliest maintenance window, reset the standby TSC:

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 TSC.

   A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

c. Right-click the standby TSC.

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 TSC is still in standby mode and that the other TSC 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 TSC fails to boot into standby mode, then open a case with Cisco TAC (1 800 553-2447) for assistance.

Step 3 If the standby TSC rebooted successfully into standby mode, complete the "Reset a Card with a Card Pull (Reseat)" procedure.

Resetting the active TSC causes the standby TSC to become active. The standby TSC keeps a copy of the chassis MAC address. If its stored MAC address is valid, the alarm should clear.

Step 4 After the reset, note whether or not the INVMACADR alarm has cleared or is still present.

Step 5 Complete the "Soft-Reset a Card Using CTC" procedure again to place the standby TSC 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 TSC resets, proceed to Step 7.

If the INVMACADR was raised during one TSC reset and cleared during the other, the TSC that was active while the alarm was raised needs to be replaced. Continue with Step 6.

Step 6 If the faulty TSC is currently in standby mode, complete the "Replace a TSC Card" procedure for this card. If the faulty TSC is currently active, during the next available maintenance window complete the "Soft-Reset a Card Using CTC" procedure and then complete the "Replace a TSC Card" procedure.

Note If the replacement TSC is loaded with a different software version from the current TSC, the card bootup could take up to 30 minutes. During this time, the card LEDs flicker between Fail and Act/Sby as the active TSC version software is copied to the new standby card.

Step 7 Open a case with Cisco TAC (1 800 553-2447) for assistance with determining the node's previous MAC address.

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.

2.6.103 ISIS-ADJ-FAIL

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

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 15600 Reference Manual*. For more information about configuring OSI, refer to the "Turn Up Node" chapter in the *Cisco ONS 15600 Procedure Guide*.

Clear the ISIS-ADJ-FAIL Alarm

Step 1 Ensure that both ends of the comm channel are using the correct Layer 2 protocol and settings (LAPD or PPP). To do this, complete the following steps:

a. At the local node, in node view, click the **Provisioning > Comm Channels > SDCC** tabs.

b. Click the row of the circuit. Click **Edit**.

c. 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.

d. Click **Cancel**.

e. Log in 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 15600 Procedure Guide* for the procedure.

Step 3 If the nodes use PPP Layer 2, complete the "Clear the EOC Alarm" procedure on page 2-42. 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 communication channels at both ends by completing the following steps:

a. Click **Provisioning > OSI > Routers > Setup**.

b. View the router entry under the **Status** column. If the status is Enabled, check the other end.

c. If the Status is Disabled, click the router entry and click **Edit**.

d. 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 comm channel have a common MAA by completing the following steps:

a. Click the **Provisioning > OSI > Routers > Setup** tabs.

b. 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 15600 Procedure Guide* for instructions to do this.

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).

2.6.104 KB-PASSTHR

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

Logical Object: OCN

The K Byte 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 2-136.

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).

2.6.105 KBYTE-APS-CHANNEL-FAILURE

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

Logical Object: OCN

The APS Channel Failure alarm is raised when a span is provisioned for different APS channels on each side. For 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 AIS-P, LOF, LOS, or SF-BER alarms.

Clear the KBYTE-APS-CHANNEL-FAILURE Alarm

Step 1 The alarm is most frequently raised due to mismatched span provisioning. In this case, reprovision one side of the span with the same parameters. To do this, refer to the "Manage Circuits" chapter in the *Cisco ONS 15600 Procedure Guide* for procedures.

Step 2 If the error is not caused by incorrect provisioning, it is because of checksum errors within an OC-N, cross-connect, or TSC card. In this case, complete the "Request a Cross-Connect Card Preferred Copy Switch" procedure on page 2-138 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).

2.6.106 LASER-BIAS

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

Logical Objects: EQPT, PPM

The High Laser Bias Current alarm occurs when a port on an OC-192 card is transmitting a laser current outside of the acceptable preset range. The alarm occurs at the card level rather than at the port level. The alarm is typically accompanied by signal or bit errors on the downstream node.

Note The difference between this alarm and the laser bias current performance-monitoring parameter is that the alarm indicates a serious physical condition in the transmitter.

Clear the LASER-BIAS Alarm

Step 1 If the alarm is reported against the working OC-192 facility and traffic has not automatically switched to protect, initiate a Force switch. If it is part of a path protection, complete the "Initiate a Force Switch for All Circuits on a Path Protection Span" procedure on page 2-131. If is part of a 1+1 protection group, complete the "Initiate a 1+1 Protection Port Force Switch Command" procedure on page 2-128.

Step 2 Complete the "Replace an OC-48 Card or OC-192 Card" procedure on page 2-140 for the reporting card.

Step 3 If the alarm does not clear after replacing the card, 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.

Step 4 Traffic reverts to the working port if working port if an automatic switch occurred. If the alarm cleared and traffic was switched in Step 1, revert traffic by completing the "Clear a 1+1 Protection Port Force or Manual Switch Command" procedure on page 2-129. If traffic was manually switched in a path protection, revert traffic to the original path by completing the "Clear a Path Protection Span External Switching Command" procedure on page 2-133.

2.6.107 LASER-OVER-TEMP

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

Logical Objects: EQPT, PPM

The Port-Level High Temperature OC-192 equipment alarm accompanies a fault in one of the four OC-192 ports. The fault causes output signal bit errors that are detected by the downstream node, which performs an APS.

If more than one card has this condition, troubleshoot with the "Clear the EQPT-HITEMP Alarm" procedure on page 2-47. Any time an OC-192 card or port reports an over-temperature condition, follow the "Clear the LASER-BIAS Alarm" procedure on page 2-80. If the alarm does not 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.

2.6.108 LKOUTPR-S

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

Logical Object: OCN

The Lockout of Protection Span condition occurs on a BSLR node when traffic is locked out of a protect span using the LOCKOUT SPAN command. This condition is visible on the network view Alarms, Conditions, and History tabs after the lockout has occurred and accompanies the FE-LOCKOUTPR-SPAN condition. 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 2-136.

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).

2.6.109 LOCKOUT-REQ

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

Logical Objects: OCN, STSMON

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 allows protection switching and clears the LOCKOUT-REQ condition.

Clear the LOCKOUT-REQ Condition

Step 1 Complete the "Clear a Card or Port Lock On or Lock Out Command" procedure on page 2-131.

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).

2.6.110 LOCKOUT-REQ-RING

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

The Lockout Switch Request on Ring condition occurs when a user initiates a lockout switch request for an OC-N card or a lockout switch request on the BLSR ring level. A lockout prevents protection switching. Clearing the lockout again allows protection switching and clears the LOCKOUT-REQ-RING condition.

Clear the LOCKOUT-REQ-RING Condition

Step 1 Complete the "Clear a BLSR External Switching Command" procedure on page 2-136.

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).

2.6.111 LOF (BITS)

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

Logical Object: BITS

The Loss of Frame (BITS) alarm is Major (MJ) if there is no backup TSC card BITS source and Minor (MN) if one of the TSC cards BITS sources fails. If one of the pair fails, a timing APS is activated on the second source.

Clear the LOF (BITS) Alarm

Step 1 Verify that the framing and coding match between the BITS input and the TSC card by completing the following steps:

a. Find the coding and framing formats of the external BITS timing source. This should be in the user documentation for the external BITS timing source or on the external timing source itself.

b. Click the node view **Provisioning > Timing > BITS Facilities** tabs.

c. Verify that the Coding setting matches the Coding setting of the BITS timing source (either B8ZS or AMI).

d. If the coding does not match, click **Coding** to display a drop-down list. Choose the appropriate coding.

e. Verify that the Framing matches the framing of the BITS timing source (either ESF or SF [D4]).

f. If the framing does not match, click **Framing** to display the drop-down list. Choose the appropriate framing.

Note In the Timing window, 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 Ensure that the BITS clock is operating properly.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15600. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

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).

2.6.112 LOF (OCN)

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

Logical Object: OCN

The Line Loss of Frame Alignment alarm occurs when a port on the reporting traffic (OC-N) card has an LOF. LOF indicates that the receiving ONS 15600 has lost frame delineation in the incoming data and when the SONET overhead loses a valid framing pattern for three milliseconds. Receiving two consecutive valid A1/A2 framing patterns clears the alarm.

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

If the port is in 1+1 protection and successfully switches, the alarm severity is MN, NSA. If the port is unprotected or if protection switching is prevented, the severity is CR, SA.

Clear the LOF (OCN) Alarm

Step 1 Verify that the automatic protection switch to the protect port was successful.

- A path protection APS is identified by an AUTOSW-type alarm or condition (such as AUTOSW-AIS, AUTOSW-LOP, AUTOSW-PDI, AUTOSW-SDBER, AUTOSW-SFBER, or AUTOSW-UNEQ).
- A 1+1 APS is identified in the node view Maintenance > Protection window. If you click the protection group, under the Selected Group list, the ports are designated as Working/Standby and Protect/Active.

Step 2 Verify that the traffic (OC-N) card and port on the upstream node is in service.

- On an in-service traffic card, the green SRV and Laser On LEDs are illuminated.
- If the card ports are in service, in the card view Provisioning window, the Status column for the port(s) show In Service. If the ports are not in service, click the port column and choose **In Service**, then click **Apply**.

Step 3 If the alarm does not clear, clean the optical fiber connectors by completing the following steps:

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15600. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

a. Clean the fiber connectors according to local site practice.

b. If no local practice exists, use a CLETOP Real-Type or equivalent fiber-optic cleaner and follow the instructions accompanying the product and/or refer to the procedures in the "Maintain the Node" chapter in the *Cisco ONS 15600 Procedure Guide*.

Step 4 If you continue to receive the LOF alarm, see the "1.9.3 Optical Traffic Card Transmit and Receive Levels" section on page 1-69 for acceptable standards.

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.

2.6.113 LO-LASERBIAS

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

Logical Object: PPM

The Equipment Low Transmit Laser Bias Current 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.

Clear the LO-LASERBIAS Alarm

Step 1 Complete the "Replace an OC-48 Card or OC-192 Card" procedure on page 2-140.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Refer to the *Cisco ONS 15600 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).

2.6.114 LOP-P

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

Logical Object: STSMON

A Loss of Pointer Path alarm indicates that the transmitted optical circuit size is different from the provisioned optical circuit size. LOP-P occurs when valid H1/H2 pointer bytes are missing from the SONET overhead. Receiving equipment monitors the H1/H2 pointer bytes to locate the SONET payload. An LOP-P alarm means that eight, nine, or ten consecutive frames do not have valid pointer values. The alarm clears when three consecutive valid pointers are received.

One of the conditions that can cause this alarm is a transmitted STSc circuit that is different from the provisioned STSc. This condition causes a mismatch of the path type on the concatenation facility. It occurs when there are eight to ten new data flags received, or eight to ten invalid pointers. For example, if an STS-3c or STS-1 is sent across a path provisioned for STS-12c, an LOP alarm occurs.

Clear the LOP-P Alarm

Step 1 Complete the "Initiate a Force Switch for All Circuits on a Path Protection Span" procedure on page 2-131 or the "Initiate a 1+1 Protection Port Force Switch Command" procedure on page 2-128 as appropriate.

Step 2 Use a test set to verify that the incoming signal is valid; refer to the "Create Circuits" chapter in the *Cisco ONS 15600 Procedure Guide* for instructions on testing optical circuits. If the upstream signal is not valid, troubleshoot upstream.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15600. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 3 If the incoming signal is valid, complete the "Replace an OC-48 Card or OC-192 Card" procedure on page 2-140 for the reporting card.

Note If the traffic (OC-N) card is implicated and you are able to continue using the traffic card with one port out of service, perform a bridge and roll to move the port traffic to a free port. Refer to the "Manage Circuits" chapter in the *Cisco ONS 15600 Procedure Guide* for instructions. Label the bad port, and place it out of service until the card can be replaced.

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.

2.6.115 LO-RXPOWER

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

Logical Object: OCN

The Equipment Low Receive Power alarm is an indicator of the optical signal power that is transmitted to the ASAP card. 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 ASAP cards, refer to the *Cisco ONS 15600 Reference Manual*. For more information about how they and their component modules are provisioned, refer to the *Cisco ONS 15600 Procedure Guide*.

Clear the LO-RXPOWER Alarm

Step 1 Determine whether there are any faults for the SFP (PPM) or 4PIO (PIM) modules associated with the errored circuit. If there are, troubleshoot them using the procedures in this manual.

Step 2 If no faults are present on the other port(s) of the transmit or receive card, use a known-good loopback cable to complete the "Create the Facility (Line) Loopback or Payload Loopback on the Source Optical Port" procedure on page 1-7 and test the loopback.

Step 3 If the carrier module itself is bad and you need all of its port bandwidth, complete the "Replace an ASAP Carrier Module" procedure on page 2-143. If the port is bad but you can move the traffic to another port, complete the "Replace an ASAP 4PIO (PIM) Module" procedure on page 2-143 or "Replace an ASAP SFP (PPM) Module" procedure on page 2-144 as needed.

Caution Removing hardware that currently carries traffic can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.8.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-128 for commonly used traffic-switching procedures.

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

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).

2.6.116 LOS (BITS)

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

Logical Object: BITS

The Loss of Signal BITS alarm is Major (MJ) if there is no backup TSC card BITS source, and Minor (MN) if one of the TSC card BITS sources fails. If one of the pair fails, a timing APS is activated on the second source.

Clear the LOS (BITS) Alarm

Step 1 Check the wiring connection from the ONS 15600 backplane BITS clock pin fields to the timing source. For more information about backplane wiring connections, refer to the "Install the Bay and Backplane Connections" chapter in the *Cisco ONS 15600 Procedure Guide*.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15600. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 2 Ensure 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) to report a Service-Affecting (SA) problem.

2.6.117 LOS (OCN)

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

Logical Object: OCN

A Loss of Signal Line alarm for either an OC-48 or OC-192 port occurs when the port on the card is in service but no signal is being received. The cabling might not be correctly connected to the ports, or no signal exists on the line. Possible causes for a loss of signal include upstream equipment failure or a fiber cut. It clears when two consecutive valid frames are received.

Clear the LOS (OCN) Alarm

Step 1 Verify fiber continuity to the port. To verify cable continuity, follow site practices.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15600. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 2 If the cabling is good, verify that the correct port is in service by completing the following steps:

a. Confirm that the LED is correctly illuminated on the physical card.

   A green SRV LED indicates an active card.

b. To determine whether the OC-N port is in service, double-click the card in CTC to display the card view by completing the following steps:

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

d. Verify that the Admin State column lists the port as IS.

e. If the Admin State column lists the port as OOS,MT or OOS,DSBLD, click the column and choose **IS**.

f. Click **Apply**.

Step 3 If the correct port is in service, clean the fiber according to site practice. If no site practice exists, complete the procedure in the "Maintain the Node" chapter in the *Cisco ONS 15600 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 "1.9.3 Optical Traffic Card Transmit and Receive Levels" section on page 1-69 lists these specifications for each OC-N card.

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 "Replace an OC-48 Card or OC-192 Card" procedure on page 2-140 for the reporting card.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.8.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-128 for commonly used traffic-switching procedures.

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

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

2.6.118 LO-TXPOWER

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

Logical Object: PPM

The Equipment Low Transmit Power alarm is an indicator for ASAP card transmitted optical signal power. LO-TXPOWER occurs when the measured optical power of the transmitted signal falls under the threshold, which is user-provisionable.

Note For more information about ASAP cards, refer to the *Cisco ONS 15600 Reference Manual*.

Clear the LO-TXPOWER Alarm

Step 1 Display the ASAP card view.

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

Step 3 Increase the TX Power Low column value by 0.5 dBm.

Step 4 If the card transmit power setting cannot be increased without affecting the signal, complete the "Replace an ASAP SFP (PPM) Module" procedure on page 2-144.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.8.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-128 for commonly used traffic-switching procedures.

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).

2.6.119 LPBKCRS

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

Logical Object: STSMON

The Loopback Cross-Connect condition indicates that a software cross-connect loopback is active between a traffic (OC-N) card and a cross-connect card.

Loopback is a commonly used troubleshooting technique. A signal is sent out on a link or section of the network and returned to the sending device. If the signal does not return or returns with errors, the test confirms that the problem is present in the tested link. By setting up loopbacks on various parts of the node and excluding other parts, you can logically isolate the source of the problem. For more information about loopbacks, see the "Troubleshooting Optical Circuits with Loopbacks" procedure in Chapter 1.

Three types of loopbacks are available: Cross-Connect, Facility, and Payload. Cross-connect loopbacks troubleshoot OC-48 signals on SSXC cards. Facility loopbacks troubleshoot OC-48 ports only and are generally performed locally or at the near end. Payload loopbacks troubleshoot OC-192 ports only and are generally performed locally or at the near end.

Clear the LBKCRS Condition

Step 1 To remove the loopback cross-connect condition, double-click the traffic (OC-N) card in node view.

Step 2 Click the **Provisioning > STS** tabs.

Step 3 In the XC Loopback column, deselect the check box for the port.

Step 4 Click **Apply**.

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

2.6.120 LPBKFACILITY (GIGE)

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

Logical Object: GIGE

A Loopback Facility condition for a Gigabit Ethernet (GE) port occurs when a software facility (line) loopback is active for an ASAP card client 4PIO (PIM) provisioned at the ONE_GE port rate.

For information about troubleshooting these circuits with loopbacks, refer to the "1.3 Troubleshooting an Ethernet Circuit Path With Loopbacks" section on page 1-25.

Note For more information about ASAP cards, refer to the *Cisco ONS 15600 Reference Manual*.

Clear the LPBKFACILITY (GIGE) Condition

Step 1 Complete the "Clear the LBKFACILITY (OCN) Condition" procedure on page 2-90.

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).

2.6.121 LPBKFACILITY (OCN)

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

Logical Object: OCN

A Facility Loopback Active condition for an OC-N occurs on OC-48 cards or OC-192 cards when a software facility loopback is active for a port on the reporting card, and the facility entity is out of service.

Caution Before performing a facility loopback on an OC-48 card, make sure the card contains at least two section DCC paths to the node where the card is installed. A second section 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 section DCC is not necessary if you are directly connected to the ONS 15600 containing the loopback OC-N.

Clear the LBKFACILITY (OCN) Condition

Step 1 To remove the loopback facility condition, double-click the reporting card in node view.

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

Step 3 In the Loopback Type column, click the correct row for the port and choose **None** from the drop-down list.

Step 4 Click **Apply**.

Step 5 Click the **Provisioning > Line** tabs.

Step 6 In the Admin State column, click the correct row for the port and choose **IS,AINS** from the drop-down list.

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).

2.6.122 LPBKPAYLOAD

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

Logical Object: OCN

A Payload Loopback Active condition occurs on OC-192 cards when a software payload loopback is active for a port on the OC-192 card, and the facility entity is out of service.

Clear the LPBKPAYLOAD Condition

Step 1 To remove the loopback payload condition, double-click the reporting card in node view.

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

Step 3 In the Loopback Type column, click the correct row for the port and choose **None** from the drop-down list.

Step 4 Click **Apply**.

Step 5 Click the **Provisioning > Line** tabs.

Step 6 In the Admin State column, click the correct row for the port and choose **IS,AINS** from the drop-down list.

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).

2.6.123 LPBKTERMINAL (GIGE)

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

Logical Object: GIGE

A Loopback Terminal condition for a Gigabit Ethernet port occurs when a software terminal (inward) loopback is active for an ASAP card client SFP (PPM) provisioned at the ONE_GE port rate.

For information about troubleshooting these circuits with loopbacks, refer to the "1.3 Troubleshooting an Ethernet Circuit Path With Loopbacks" section on page 1-25].

Clear the LPBKTERMINAL (GIGE) Condition

Step 1 Complete the "Clear the LBKTERMINAL (OCN) Condition" procedure on page 2-92.

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).

2.6.124 LPBKTERMINAL (OCN)

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

Logical Object: OCN

A Terminal Loopback Active condition for OC-N occurs on OC-48 cards or OC-192 cards when a software facility loopback is active for a port on the reporting card, and the facility entity is out of service.

Caution Before performing a terminal loopback on an OC-48 card, make sure the card contains at least two section DCC paths to the node where the card is installed. A second section DCC path provides a nonlooped path to log into the node after the loopback is applied, thus enabling you to remove the terminal loopback. Ensuring a second section DCC is not necessary if you are directly connected to the ONS 15600 containing the loopback OC-N.

Clear the LBKTERMINAL (OCN) Condition

Step 1 To remove the loopback facility condition, double-click the reporting card in node view.

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

Step 3 In the Loopback Type column, click the correct row for the port and choose **None** from the drop-down list.

Step 4 Click **Apply**.

Step 5 Click the **Provisioning > Line** tabs.

Step 6 In the Admin State column, click the correct row for the port and choose **IS,AINS** from the drop-down list.

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).

2.6.125 MAN-REQ

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

Logical Object: STSMON

The Manual Switch Request condition occurs when a user initiates a Manual switch request on an OC-N port. Clearing the Manual switch clears the MAN-REQ condition. You do not need to clear the switch if you want the manual switch to remain.

Clear the MAN-REQ Condition

Step 1 Complete the "Initiate a 1+1 Protection Port Manual Switch Command" procedure on page 2-129.

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).

2.6.126 MANRESET

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

Logical Objects: EQPT, PIM, PPM

A Manual System Reset condition occurs when you right-click a TSC card, SSXC card, or traffic (OC-N) card in CTC and choose Hard-reset Card or Soft-reset Card. Resets performed during a software upgrade also prompt the alarm. This condition clears automatically when the card finishes resetting.

Note The hard-reset option is enabled only when the card is placed in the OOS-MA, MT service state.

2.6.127 MANSWTOINT

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

Logical Object: NE-SREF

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

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

2.6.128 MANSWTOPRI

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

Logical Objects: EXT-SREF, NE-SREF

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

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

2.6.129 MANSWTOSEC

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

Logical Objects: EXT-SREF, NE-SREF

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

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

2.6.130 MANSWTOTHIRD

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

Logical Objects: EXT-SREF, NE-SREF

The Manual Synchronization Switch to Third Reference condition occurs when the NE (node) timing source is manually switched to a third source.

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

2.6.131 MANUAL-REQ-RING

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

Logical Object: OCN

The Manual Switch Request on Ring condition occurs when a user initiates a MANUAL RING command on a BLSR ring 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 2-136.

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).

2.6.132 MANUAL-REQ-SPAN

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

Logical Object: OCN

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 2-136.

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).

2.6.133 MATECLK

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

Logical Object: EQPT

The Mate Clock alarm occurs when the active TSC card cannot detect the clock from the standby TSC card.

Clear the MATECLK Alarm

Step 1 In CTC, check for any alarms that indicate that there are faulty clock references, such as the "HLDOVRSYNC" alarm on page 2-72 or the "FRNGSYNC" alarm on page 2-67, and resolve these alarms.

Step 2 If the MATECLK persists, complete the "Reset a Card with a Card Pull (Reseat)" procedure on page 2-138 for the standby TSC card and wait 15 minutes.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15600. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 3 If the MATECLK still persists, complete the "Replace a TSC Card" procedure on page 2-142 for the active TSC card, using the standby TSC card to replace the active TSC 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) to report a Service-Affecting (SA) problem.

2.6.134 MEA

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

Logical Objects: EQPT, PIM, PPM

The Mismatch Between Equipment Type and Provisioned Attributes alarm is reported against a card slot when the physical card or port does not match the card type provisioned in CTC. Deleting the incompatible card or port, SFP (PPM), or 4PIO (PIM) in CTC or physically removing the card clears the alarm.

Clear the MEA Alarm

Step 1 Physically verify the type of card that sits in the slot reporting the MEA alarm.

Step 2 In CTC, click the node view **Inventory** tab to display the provisioned card type.

Step 3 If you prefer the card type depicted by CTC, complete the "Replace an OC-48 Card or OC-192 Card" procedure on page 2-140 for the reporting card and replace it with the card type depicted by CTC (provisioned for that slot).

Note CTC does not allow you to delete a card if at least one port on the card is in service, has a path mapped to it, is paired in a working-protection scheme, has DCC enabled, or is used as a timing reference.

Step 4 If you want to leave the installed card in the slot but it is not in service, delete any circuits mapped to it. Refer to the "Manage Circuits" chapter in the *Cisco ONS 15600 Procedure Guide* for procedures.

Step 5 Place the cursor over the provisioned card in CTC and right-click to choose **Delete Card**.

When the card is deleted in CTC, the card that physically occupies the slot automatically reboots and appears in CTC.

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) to report a Service-Affecting (SA) problem.

2.6.135 MEM-GONE

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

Logical Object: EQPT

The Memory Gone alarm occurs when data generated by software operations exceeds the memory capacity of the TSC card. The TSC 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 preceeds the MEM-GONE alarm.

2.6.136 MEM-LOW

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

Logical Object: EQPT

The Free Memory of Card Almost Gone alarm occurs when data generated by software operations is close to exceeding the memory capacity of the TSC card. 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 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)

2.6.137 MFGMEM (CAP)

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

Logical Object: CAP

The Manufacturing Data Memory Failure CAP alarm occurs if the ONS 15600 cannot access the data in the EEPROM on the backplane. MFGMEM is caused by EEPROM failure on the backplane, or fuse failure for the EEPROM.

The EEPROM stores manufacturing data that is needed for compatibility and inventory issues. If the alarm is accompanied by the "PWR-FA" alarm on page 2-103, the 5-VDC fuse for the EEPROM might be tripped. If that is the case, use the procedure below to eliminate the TSC card as the cause of the alarm, but do not attempt to troubleshoot it further. Contact the Cisco TAC at 1-800-553-2447.

Clear the MFGMEM Alarm on the CAP by Resetting the TSC Card

Step 1 Complete the "Soft-Reset a Card Using CTC" procedure on page 2-136.

Wait for the "FSTSYNC" condition on page 2-67 to clear.

Step 2 If the alarm does not clear, complete the "Soft-Reset a Card Using CTC" procedure on page 2-136.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447). The standby TSC card might also need replacement. If the alarm continues after both TSC cards have been replaced, the problem lies in the EEPROM on the CAP, and this must be replaced.

Step 3 When the alarm is cleared, you can make the standby TSC card active again by completing the "Soft-Reset a Card Using CTC" procedure on page 2-136.

2.6.138 MFGMEM (FAN)

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

Logical Object: FAN

The Manufacturing Data Memory Fan alarm occurs if the ONS 15600 EEPROM on a fan tray fails. MFGMEM can be accompanied by the "FAN-FAIL" alarm on page 2-58.

Clear the MFGMEM (FAN) Alarm

Step 1 Pull out the fan tray.

Step 2 Reinsert the fan trays, making sure you can hear the fans start operating. Fans should run immediately when correctly inserted.

Step 3 If a fan does not run or the alarm persists, refer to the "Maintain the Node" chapter in the *Cisco ONS 15600 Procedure Guide* for instructions to replace the fan tray.

Step 4 If a replacement fan tray does not operate correctly, 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.

2.6.139 MFGMEM (for the PIM, PPM, SSXC, Traffic Card, or TSC Card)

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

Logical Objects: EQPT, PIM, PPM

The Manufacturing Data Memory Failure SSXC, Traffic (OC-N) Card, TSC card alarm occurs if the ONS 15600 EEPROM on one of these cards fails.

Clear the MFGMEM Alarm (for the PIM,PPM, SSXC, Traffic Card, or TSC Card)

Step 1 If the alarm is reported against a TSC card, troubleshoot with the "Clear the MFGMEM Alarm on the CAP by Resetting the TSC Card" procedure on page 2-97.

Step 2 If the reporting card is an active traffic line port in a 1+1 protection group or a path protection, ensure that an APS traffic switch has occurred to move traffic to the protect port.

- A path protection APS is identified by an AUTOSW-type alarm or condition (such as AUTOSW-AIS, AUTOSW-PDI, AUTOSW-SDBER, AUTOSW-SFBER, or AUTOSW-UNEQ).
- A 1+1 APS is identified in the node view Maintenance > Protection window. If you click the protection group, under the Selected Group list, the ports are designated as Working/Standby and Protect/Active.

Step 3 If the reporting port is part of a path protection, complete the "Initiate a Force Switch for All Circuits on a Path Protection Span" procedure on page 2-131. If the port is part of a 1+1 protection group, complete the "Initiate a 1+1 Protection Port Force Switch Command" procedure on page 2-128.

Step 4 If the reporting card is a SSXC card and an automatic switch to the preferred copy SSXC card occurred, traffic automatically switches to the alternate copy.

Complete a "Hard-Reset a Card Using CTC" procedure on page 2-137 for the reporting card (or "Soft-Reset a Card Using CTC" procedure on page 2-136 for the SSXC.

Step 5 If the reset does not clear the alarm, complete the "Reset a Card with a Card Pull (Reseat)" section on page 2-138 for the TSC card, or complete the "Request a Cross-Connect Card Preferred Copy Switch" section on page 2-138 for the SSXC.

Step 6 If the physical reseat of the card or switch does not clear the alarm, complete the appropriate procedure in the "Replace a TSC Card" section on page 2-142 or "Replace an SSXC Card" section on page 2-139 as needed.

Note If the traffic (OC-N) card is implicated and you are able to continue using the traffic card with one port out of service, perform a bridge and roll to move the port traffic to a free port using the "Bridge and Roll Traffic" procedure in the "Manage Circuits" chapter in the *Cisco ONS 15600 Procedure Guide*. Label the bad port, and place it out of service until such time as the card can be replaced.

Step 7 If the MFGMEM alarm continues to report after you replaced the card, the problem lies in the EEPROM. Log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

Step 8 If the alarm clears and it was reported by a traffic card, traffic reverts to the working port if an automatic switch occurred. If traffic was manually switched in a 1+1 protection group, revert traffic to the original port by completing the "Clear a 1+1 Protection Port Force or Manual Switch Command" procedure on page 2-129. If traffic was manually switched in a path protection, revert traffic to the original path by completing the "Clear a Path Protection Span External Switching Command" procedure on page 2-133.

If an automatic switch to the alternate copy SSXC card occurred, traffic is automatically restored to the preferred copy.

Step 9 If the reporting card is a TSC card and you want to make the standby TSC card active again, complete the "Soft-Reset a Card Using CTC" procedure on page 2-136.

2.6.140 NOT-AUTHENTICATED

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

Logical Object: SYSTEM

The NOT-AUTHENTICATED alarm is raised by CTC (not by the NE) when it fails to log into a node. This alarm only displays in CTC where the login failure occurred. This alarm differs from the "INTRUSION-PSWD" alarm on page 2-76 in that INTRUSION-PSWD occurs when a user exceeds the login failures threshold.

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

2.6.141 OPEN-SLOT

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

Logical Object: EQPT

The OPEN-SLOT alarm indicates that one of the I/O slots (Slot 1 through 4 and 11 through 14) does not contain a traffic card or filler card.

Clear the OPEN-SLOT Alarm

Step 1 Insert a filler card or OC-N card into the empty slot.

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).

2.6.142 PDI-P

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

Logical Object: STSMON

A Payload Defect Indication Path condition indicates that a signal label mismatch failure (SLMF) in the STS-1 signal. An invalid C2 byte in the SONET path overhead causes an SLMF. The C2 byte is the signal-label byte that tells the equipment what the SONET payload envelope contains and how it is constructed. It enables a SONET device to transport multiple types of services.

The ONS 15600 encounters an SLMF when the payload, such as an asynchronous transport mode (ATM), does not match what the signal label is reporting. The "AIS-P" condition on page 2-16 often accompanies the PDI-P alarm. If the PDI-P is the only alarm reported with an AIS-P, clear the PDI-P alarm to clear the AIS-P alarm. PDI-P can also occur during an upgrade, but usually clears itself and is not a valid alarm.

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

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

Clear the PDI-P Condition

Step 1 Check the incoming signal overhead with an optical test to verify that the C2 byte is correct. Refer to the "Create Circuits" chapter in the *Cisco ONS 15600 Procedure Guide* for circuit test procedures.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15600. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 2 If the C2 byte is not correct, it indicates an upstream equipment problem (typically with path-terminating equipment [PTE]). Troubleshoot the upstream equipment.

Step 3 If the condition does not clear, complete the "Replace an OC-48 Card or OC-192 Card" procedure on page 2-140 for the reporting card.

Note If the traffic (OC-N) card is implicated and you are able to continue using the traffic card with one port out of service, perform a bridge and roll to move the port traffic to a free port; refer to the "Manage Circuits" chapter in the *Cisco ONS 15600 Procedure Guide* for instructions. Label the bad port and place it out of service until the card can be replaced.

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).

2.6.143 PLM-P

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

Logical Object: STSMON

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).

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

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

Clear the PLM-P Alarm

Step 1 Complete the "Clear the PDI-P Condition" procedure on page 2-100.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15600. 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.

2.6.144 PRC-DUPID

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

Logical Object: OCN

The Procedural Error Duplicate Node ID alarm indicates that two identical node IDs exist in the same BLSR. The ONS 15600 requires each node in the BLSR to have a unique node ID.

Clear the PRC-DUPID Alarm

Step 1 Log into a node on the ring.

Step 2 Find the node ID by completing the "Identify a BLSR Ring ID or Node ID Number" procedure on page 2-127.

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

Step 4 If two nodes have an identical node ID number, complete the "Change a BLSR Node ID Number" procedure on page 2-128 so that each node ID is unique.

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

2.6.145 PROV-MISMATCH

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

Logical Object: PPM

The Provisioning Mismatch for an SFP alarm is raised against an SFP (PPM) connector on the ASAP card under one of the following circumstances:

- The physical SFP (PPM) range or wavelength does not match the provisioned value. PPMs (SFPs) have static wavelength values which must match the wavelengths provisioned for the port.
- The SFP (PPM) reach (loss) value does not meet the reach value needed for the port.

Clear the PROV-MISMATCH Alarm

Step 1 Determine what the SFP (PPM) wavelength range should be by viewing the frequency provisioned for the card by completing the following steps:

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

b. Click the **Provisioning > Optical** tabs (or **Ethernet** tab, as appropriate).

c. Record the values shown in the **Reach** and **Wavelength** columns.

Step 2 Complete the "Replace an ASAP SFP (PPM) Module" procedure on page 2-144.

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).

2.6.146 PWR

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

Logical Object: PWR

The NE Power Failure at Connector 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 alarm is necessary for troubleshooting.

Effects of this alarm depend upon the shutdown order of the two power supplies. If PWR B of the right-side power feed and PWR A of the left-side power feed are shut down, this causes all three fans to turn off and a "FAN-FAIL" alarm on page 2-58 to be raised. In this case, after power is restored all three fans work in high-speed mode for a few minutes until CTC returns them to normal speed. All alarms are cleared.

Clear the PWR Alarm

Step 1 At the site, determine which battery is not present or operational.

Step 2 Remove the power cable from the faulty supply. For instructions, refer to the "Install the Bay and Backplane Cable" chapter in the *Cisco ONS 15600 Procedure Guide* and reverse the power cable installation procedure.

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

2.6.147 PWR-FA

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

Logical Object: BPlane

The Backplane Power Fuse Failure alarm indicates that the backplane EEPROM memory 5-VDC fuse fails, but the equipment is still in service. Service is not currently affected, but network management can be affected because the ONS 15600 system uses a default NE (node) IP address instead of a programmed one in this case. This alarm might be accompanied by the "INVMACADR" alarm on page 2-76, which appears in the alarm history when network management capability is restored.

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

2.6.148 PWR-FAIL-A

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

Logical Objects: CAP, 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 CAP, SSXC card, traffic (OC-N) cards, or TSC card.

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

Clear the PWR-FAIL-A Alarm

Step 1 If a single card has reported the alarm, take one of the following actions depending what kind of card reported it:

- 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.
  - A path protection APS is identified by an AUTOSW-type alarm or condition (such as AUTOSW-AIS, AUTOSW-PDI, AUTOSW-SDBER, AUTOSW-SFBER, or AUTOSW-UNEQ).
  - A 1+1 APS is identified in the node view Maintenance > Protection window. If you click the protection group, under the Selected Group list, the ports are designated as Working/Standby and Protect/Active.

  - If the reporting port is part of a path protection, complete the "Initiate a Force Switch for All Circuits on a Path Protection Span" procedure on page 2-131. If the port is part of a 1+1 protection group, complete the "Initiate a 1+1 Protection Port Force Switch Command" procedure on page 2-128. Continue with Step 3.

- If an automatic switch to the alternate copy SSXC card occurred, the SSXC card can be serviced. If the switch has not occurred, complete the "Request a Cross-Connect Card Preferred Copy Switch" procedure on page 2-138. Continue with Step 3.

  To determine which SSXC card is the preferred copy and if it is currently being used, open the node view Maintenance > Preferred Copy window. The Data Copy area Preferred field shows Copy A or Copy B. The Currently Used field shows the copy being used.

Note In CTC, Copy A refers to the SSXC card in Slot 6/7. Copy B refers to the SSXC card in Slot 8/9. Either copy might be chosen as the preferred copy SSXC card. The other SSXC card is called the alternate SSXC card in this chapter.

Step 2 Complete the "Soft-Reset a Card Using CTC" procedure on page 2-136 for the reporting card.

Step 3 If the alarm does not clear, complete the "Reset a Card with a Card Pull (Reseat)" procedure on page 2-138.

Step 4 Check the pins on the backplane connector, including the power pins on the edge of the card. Also inspect the pins on the backplane. A bent pin can cause power failure.

Caution If a backplane pin is bent, do not insert another card in the slot until the problem is remedied.

Step 5 If the alarm does not clear, complete the "Replace an SSXC Card" procedure on page 2-139, "Replace an OC-48 Card or OC-192 Card" procedure on page 2-140, or "Replace a TSC Card" procedure on page 2-142 as needed.

Step 6 If the single card reseat and replacement does not clear the alarm, or if multiple cards report the alarm, verify the office power; refer to the "Install the Bay and Backplane Connections" chapter in the *Cisco ONS 15600 Procedure Guide* for power installation instructions.

Step 7 If the alarm does not clear, reseat the power cable connection to the connector. For more information about ONS 15600 power connections, refer to the "Install the Bay and Backplane Connections" chapter in the *Cisco ONS 15600 Procedure Guide*.

Step 8 If the alarm does not clear, physically replace the power cable connection to the connector.

Step 9 If the alarm does not clear, a problem with the power distribution unit (PDU) is indicated and it could need to be replaced. Complete the procedure located in the "Maintain the Node" chapter in the *Cisco ONS 15600 Procedure Guide*.

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).

Step 11 If the alarm clears and it was reported by a traffic (OC-N) card, traffic reverts to the working port if an automatic switch occurred. If traffic was manually switched to a 1+1 protect port, revert traffic by completing the "Clear a 1+1 Protection Port Force or Manual Switch Command" procedure on page 2-129. If traffic was manually switched in a path protection, revert traffic to the original path by completing the "Clear a Path Protection Span External Switching Command" procedure on page 2-133.

Step 12 If the alarm was reported by a SSXC card and an automatic switch to the alternate copy SSXC card occurred, traffic is automatically restored to the preferred copy.

Step 13 If the reporting card was reported by a TSC card and you want to make the standby card active, complete the "Soft-Reset a Card Using CTC" procedure on page 2-136.

2.6.149 PWR-FAIL-B

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

Logical Objects: CAP, 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 CAP, SSXC card, traffic (OC-N) cards, or TSC card.

Troubleshoot this alarm with the "Clear the PWR-FAIL-A Alarm" procedure on page 2-103.

2.6.150 PWR-FAIL-RET-A

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

Logical Object: EQPT

The Equipment Power Failure at Power Return A alarm occurs when the main power return path is not available. This alarm occurs on the TSC card, SSXC card, or traffic (OC-N) cards. Troubleshoot using the "Clear the PWR-FAIL-A Alarm" procedure on page 2-103.

2.6.151 PWR-FAIL-RET-B

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

Logical Object: EQPT

The Equipment Power Failure at Power Return B alarm occurs when the main power return path is not available. This alarm occurs on the TSC card, SSXC card, or traffic (OC-N) cards.

Troubleshoot using the "Clear the PWR-FAIL-A Alarm" procedure on page 2-103.

2.6.152 PWRRESTART

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

Logical Object: EQPT

The Power-Up Restart condition occurs when the shelf is restarted while no CTC connection is present. The Slot 5 TSC card on the shelf does not report this condition because the card is inactive when the condition occurs. You can see this condition in the Alarm History window when the CTC connection resumes.

2.6.153 RFI-L

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

Logical Object: OCN

An RFI Line condition occurs when the ONS 15600 detects an RFI in the SONET overhead of OC-48 and OC-192 cards because of a fault in another node. Resolving the fault in the adjoining node clears the RFI-L alarm in the reporting node.

RFI-L indicates that the alarm is occurring at the line level. The line layer is the segment between two SONET devices in the circuit and is also known as a maintenance span. The line layer deals with SONET payload transport. The line layer functions include multiplexing and synchronization.

Clear the RFI-L Condition

Step 1 Log into the node at the far end.

Step 2 Check for alarms, especially the "LOS (OCN)" alarm on page 2-87.

Step 3 Resolve alarms in the far-end node using the "Clear the LOF (OCN) Alarm" procedure on page 2-83. This procedure also clears LOS.

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).

2.6.154 RFI-P

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

Logical Object: STSMON

An RFI Path condition occurs when the ONS 15600 detects an RFI in the SONET overhead of the STS-1 signal because of a fault in another node. Resolving the fault in the adjoining node clears the RFI-P alarm in the reporting node.

RFI-P occurs in the node that terminates a path. The path layer is the segment between the originating equipment and the terminating equipment. This segment might encompass several consecutive line segments. An RFI-P error message on the ONS 15600 indicates that the node reporting the RFI-P is the terminating node on that path segment.

Clear the RFI-P Condition

Step 1 Verify that the ports are enabled and in-service on the reporting ONS 15600.

In the card-level view, traffic port state is indicated by the color of the port:

- Gray—Out of service (OOS)
- Green—In service (IS)
- Red—Critical (CR) alarm
- Yellow—Minor (MN) alarm
- Orange—Major (MJ) alarm

Step 2 If a port is OOS, click the **Provisioning > Line** tabs and choose **In Service** from the drop-down list for that port. Click **Apply**.

Step 3 To find the path and node failure, verify the integrity of the SONET circuit path at each of the intermediate SONET nodes, checking for inconsistencies in path size or protection configuration.

Step 4 Identify and resolve alarms in the reporting node. The "UNEQ-P" alarm on page 2-121 frequently also needs to be resolved. Complete the "Clear the UNEQ-P Alarm" procedure on page 2-121.

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).

2.6.155 RING-MISMATCH

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

Logical Object: OCN

At least one node in the BLSR has an incorrect node ID. The RING-MISMATCH alarm clears when all nodes in the BLSR have the correct node IDs.

Clear the RING-MISMATCH Alarm

Step 1 Complete the "Identify a BLSR Ring ID or Node ID Number" procedure on page 2-127 to verify each node's ID number.

Step 2 Repeat Step 1 for all nodes in the ring.

Step 3 If one node has an incorrect node ID number, complete the "Change a BLSR Node ID Number" procedure on page 2-128 to change one node's ID number so that each node ID is unique.

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).

2.6.156 RING-SW-EAST

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

Logical Object: OCN

The Ring Switch Is Active East Side condition occurs when a ring switch occurs at the east side of a BLSR using a Force Ring command. The condition clears when the switch is cleared. 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.

2.6.157 RING-SW-WEST

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

Logical Object: OCN

The Ring Switch Is Active West Side condition occurs when a ring switch occurs at the west side of a BLSR using a Force Ring command. The condition clears when the switch is cleared. 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.

2.6.158 ROLL

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

Logical Object: STSMON

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.

2.6.159 ROLL-PEND

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

Logical Object: STSMON

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.

2.6.160 SD-L

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

Logical Object: OCN

A Signal Degrade Line condition occurs for an optical port that detects a signal degrade condition. Signal degrade is defined by Telcordia as a "soft failure" condition. SD-L and the SF-L condition (see the "SF-L" condition on page 2-110) monitor the incoming BER and are similar. SD is triggered at a lower bit error rate than SF.

The BER threshold on the ONS 15600 is user-provisionable and has a range for SD from 1E–9 dBm to 1E–5 dBm.

SD-L causes a switch from the working card to the protect card at the line (facility) level. A line- or facility-level SD alarm travels on the B2 byte of the SONET overhead.

The SD condition clears when the BER level falls to one tenth of the threshold level that triggered the alarm. A BER increase is sometimes caused by a physical fiber problem, including a faulty or incorrectly plugged fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice.

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

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

Clear the SD-L Condition

Step 1 Verify that the user-provisionable BER threshold is set at the expected level by completing the following steps:

a. From node view, double-click the card reporting the alarm to display the card view.

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

c. Under the SD BER column in the Provisioning window, verify that the cell entry is consistent with what the system was originally provisioned for. The default setting is 1E–7 dBm.

d. If the entry is consistent with what the system was originally provisioned for, continue with Step 2.

e. If the entry is not consistent the original provisioning, click the cell to display a drop-down list of choices and choose the entry consistent with the original provisioning.

f. Click **Apply**.

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 15600 Procedure Guide*.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15600. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 3 Use an optical test set to measure the power level of the line to ensure it is within guidelines. Refer to the "Create Circuits" chapter in the *Cisco ONS 15600 Procedure Guide* for circuit test procedures.

Step 4 Verify that optical receive levels are within the acceptable range.

Step 5 Clean the fiber connectors at both ends for a line signal degrade by completing the following steps:

a. Clean the fiber connectors according to local site practice.

b. If no local practice exists, use a CLETOP Real-Type, 3M OGI connector cleaner, or equivalent fiber-optic cleaner and follow the instructions accompanying the product and/or refer to the procedures in the "Maintain the Node" chapter in the *Cisco ONS 15600 Procedure Guide*.

Step 6 Clean the optical transmitter and receiver by following site practice.

Step 7 Verify that a single-mode laser is used at the far end.

Step 8 If the problem persists, complete the "Replace an OC-48 Card or OC-192 Card" procedure on page 2-140 on the transmitter card at the other end of the optical line.

Note If the traffic card is implicated and you are able to continue using the traffic card with one port out of service, perform a bridge and roll to move the port traffic to a free port using procedures in the "Manage Circuits" chapter in the *Cisco ONS 15600 Procedure Guide*. Label the bad port, and place it out of service until such time as the card can be replaced.

2.6.161 SD-P

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

Logical Object: STSMON

The Signal Degrade Path condition occurs when the B3 error count in the SONET overhead exceeds the limit. Troubleshoot with the "Clear the SD-L Condition" procedure on page 2-109.

2.6.162 SF-L

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

Logical Object: OCN

A Signal Fail Line condition occurs when the quality of the signal on OC-48 and OC-192 cards causes the BER on the incoming optical line to exceed the SF threshold. Signal failure is defined by Telcordia as a "hard failure" condition. SD and SF both monitor the incoming BER error rate and are similar, but SF is triggered at a higher BER than SD. The default value of NA is determined by Telcordia GR-253-CORE.

The BER threshold on the ONS 15600 is user-provisionable and has a range for SF from 1E–5 dBm to 1E–3 dBm.

SF-L causes a switch from the working port to the protect port at the line (facility) level. A line or facility level SF condition travels on the B2 byte of the SONET overhead. The SF clears when the BER level falls to one-tenth of the threshold level that triggered the alarm. 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. Troubleshoot with the "Clear the SD-L Condition" procedure on page 2-109.

2.6.163 SF-P

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

Logical Object: STSMON

The Signal Fail Path condition occurs when the B3 error count in the SONET overhead exceeds the limit. Troubleshoot with the "Clear the SD-L Condition" procedure on page 2-109.

2.6.164 SFTWDOWN

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

Logical Object: EQPT

A Software Download in Progress condition occurs when a TSC card is downloading or transferring software. No action is necessary. Wait for the transfer or the software download to complete. If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

Note It takes approximately 20 minutes for the active TSC card to transfer the system software to the newly installed TSC card. Software transfer occurs in instances where different software versions exist on the two cards. When the transfer completes, the TSC card reboots and goes into standby mode after approximately three minutes.

Note If the active and standby TSC cards have the same versions of software, it takes approximately three minutes for software to be updated on a standby TSC card.

2.6.165 SNTP-HOST

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

Logical Object: NE

The Simple Network Timing Protocol (SNTP) Host Failure alarm indicates that an ONS node serving as an IP proxy for the other ONS nodes in the ring is not forwarding SNTP information to the other ONS nodes in the network. The forwarding failure can result from two causes, either the IP network attached to the ONS proxy node is experiencing problems, or the ONS proxy node itself is not functioning properly.

Clear the SNTP-HOST Alarm

Step 1 Ping the SNTP host from a workstation in the same subnet to ensure that communication is possible within the subnet by completing the "Ping the ONS 15600" procedure on page 1-52.

Step 2 If the ping fails, contact the network administrator who manages the IP network that supplies the SNTP information to the proxy and determine whether the network is experiencing problems which might affect the SNTP server/router connecting to the proxy ONS 15600.

Step 3 If no network problems exist, ensure that the ONS 15600 proxy is provisioned correctly by completing the following steps:

- **a.** In node view for the ONS node serving as the proxy, click the **Provisioning > General** tabs.
- **b.** Ensure that the Use NTP/SNTP Server check box is checked.
- **c.** If the Use NTP/SNTP Server check box is not checked, click it.
- **d.** Ensure that the Use NTP/SNTP Server field contains a valid IP address for the server.

Step 4 If proxy is correctly provisioned, refer to the "Management Network Connectivity" chapter in the *Cisco ONS 15600 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).

2.6.166 SPAN-SW-EAST

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

Logical Object: OCN

The Span Switch Is Active West Side condition occurs when a span switch occurs at the west side of a four-fiber BLSR span using a Force Span command. The condition clears when the switch is cleared. 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.

2.6.167 SPAN-SW-WEST

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

Logical Object: OCN

The Span Switch Is Active East Side condition occurs when a span switch occurs at the west side of a four-fiber BLSR span using a 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.

2.6.168 SQUELCH

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

Logical Object: OCN

The Ring Squelching Traffic condition occurs in a BLSR when a node that originates or terminates STS circuits fails or is isolated by multiple fiber cuts or maintenance FORCE RING commands. The isolation or failure of the node disables circuits that originate or terminate on the failed node. Squelch alarms appear on one or both of the nodes on either side of the isolated/failed node. The "AIS-P" condition on page 2-16 also appears on all nodes in the ring except the isolated node.

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

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

Clear the SQUELCH Condition

Step 1 Determine the isolated node by completing the following steps:

a. In the node view, click **View > Go to Network View**.

b. The grayed out node with red spans is the isolated node.

Step 2 Verify fiber continuity to the ports on the isolated node. To verify cable continuity, follow site practices.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15600. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 3 If fiber continuity is OK, verify that the proper ports are in service by completing the following steps:

a. Confirm that the OC-N card shows a green LED in CTC or on the physical card.

A green LED indicates an active card.

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 **State** column lists the port as IS.

e. If the State column lists the port as OOS,DSLB or OOS,MT, click the column and choose **IS**. Click **Apply**.

Step 4 If the correct ports are in service, use an optical test set to verify that a valid signal exists on the line. For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving card as possible.

Step 5 If the signal is valid, verify that the power level of the optical signal is within the optical (traffic) card's receiver specifications. Refer to the"1.9.3 Optical Traffic Card Transmit and Receive Levels" section on page 1-69.

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 "Replace an OC-48 Card or OC-192 Card" procedure on page 2-140 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).

2.6.169 SSM-DUS

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

Logical Objects: BITS, OCN

The Synchronization Status Messaging (SSM) Changed to Do Not Use (DUS) condition occurs when the synchronization status message quality level changes to DUS.

The port that reports the condition is not at fault. The condition applies to the timing source. SSM-DUS prevents timing loops by providing a termination point for the signal usage.

2.6.170 SSM-FAIL

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

Logical Objects: BITS, OCN

The SSM Failed to Receive Synchronization alarm occurs when SSM received by the ONS 15600 fails. The problem is external to the ONS 15600. If one of two sources fails, the alarm is Minor (MN). If there is no backup source, the alarm is Major (MJ). This alarm indicates that although the ONS 15600 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 Use an optical test set to determine whether the external timing source is delivering SSM; refer to the "Create Circuits" chapter in the *Cisco ONS 15600 Procedure Guide* for circuit test procedures.

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).

2.6.171 SSM-OFF

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

Logical Objects: BITS, OCN

The SSM Changed to Off condition occurs when SSM is disabled by a user.

SSM communicates information about the quality of the timing source. SSM is carried on the S1 byte of the SONET line layer. It enables SONET devices to automatically select the highest quality timing reference and to avoid timing loops. Troubleshoot with the "Clear the SSM-FAIL Alarm" procedure on page 2-114 if desired.

2.6.172 SSM-PRS

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

Logical Objects: BITS, NE-SREF, OCN

The SSM Quality Level Changed to PRS condition occurs when SSM transmission level changes to Stratum 1 Traceable.

2.6.173 SSM-RES

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

Logical Objects: BITS, NE-SREF, OCN

The SSM Quality Level Changed to Reserved (RES) condition occurs when the synchronization message quality level changes to RES.

2.6.174 SSM-SMC

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

Logical Objects: BITS, NE-SREF, OCN

The SSM Quality Level Changed to SONET Minimum Clock Traceable (SMC) condition occurs when the synchronization message quality level changes to SMC.

2.6.175 SSM-ST2

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

Logical Objects: BITS, NE-SREF, OCN

The SSM Quality Level Changed to Stratum 2 Traceable (ST2) condition occurs when the synchronization message quality level changes to ST2.

2.6.176 SSM-ST3

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

Logical Objects: BITS, NE-REF, OCN

The SSM Quality Level Changed to Stratum 3 Traceable (ST3) condition occurs when the synchronization message quality level changes to ST3.

2.6.177 SSM-ST3E

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

Logical Objects: BITS, NE-SREF, OCN

The SSM Quality Level Changed to ST3E condition occurs when the synchronization message quality level changes to ST3E from a lower level of synchronization.

2.6.178 SSM-ST4

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

Logical Objects: BITS, NE-SREF, OCN

The SSM Quality Level Changed to ST4 condition occurs when the synchronization message quality level changes to ST4.

2.6.179 SSM-STU

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

Logical Objects: BITS, NE-SREF, OCN

The SSM Synchronization Traceability Unknown condition occurs when the reporting node is timed to a reference that does not support SSM, but the ONS 15600 has SSM support enabled. SSM-STU can also be raised if the timing source is sending out SSM messages but SSM is not enabled on the ONS 15600.

Clear the SSM-STU Condition

Step 1 Click the node view **Provisioning > Timing > BITS Facilities** tabs.

Step 2 If the **Sync. Messaging Enabled** check box is checked, click the box to deselect it.

Step 3 If the **Sync. Messaging Enabled** check box is unchecked, click the box to select it.

Step 4 Click **Apply**.

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).

2.6.180 SSM-TNC

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

Logical Objects: BITS, NE-SREF, OCN

The SSM Quality Level Changed to Transit Node Clock Traceable (TNC) condition occurs when the synchronization message quality level changes to TNC.

2.6.181 SWTOPRI

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

Logical Objects: EXT-SREF, NE-SREF

The Synchronization Switched to Primary Reference condition occurs when the ONS 15600 switches to the primary timing source (reference 1). The ONS 15600 uses three ranked timing references. The timing references are typically two BITS-level or line-level sources and an internal reference.

2.6.182 SWTOSEC

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

Logical Objects: EXT-SREF, NE-SREF

The Synchronization Switched to Second Reference condition occurs when the ONS 15600 has switched to a second timing source (reference 2). To clear the SWTOSEC condition, complete the "Clear the SYNCPRI Alarm" procedure on page 2-118.

2.6.183 SWTOTHIRD

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

Logical Objects: EXT-SREF, NE-SREF

The Synchronization Switched to Third Reference condition occurs when the ONS 15600 has switched to a third timing source (reference 3). To clear the SWTOTHIRD condition, complete the "Clear the SYNCPRI Alarm" procedure on page 2-118.

2.6.184 SW-VER

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

Logical Object: EQPT

The Software Version condition is reported when a new software version is activated on the ONS 15600. When a new version of software is uploaded, it results in the active TSC card running the new version and the standby TSC card running the old version. This situation raises the SW-VER condition. It remains until the user accepts the new version in the CTC. The acceptance causes the standby TSC card to reboot and upload the new version.

If the user does not accept the version, the active TSC card switches to the standby TSC card with the original version. After the switch, the new standby TSC card reverts to the previous version.

2.6.185 SYNCCLK

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

Logical Object: NE

A Synchronization Clock Unavailable alarm occurs when both TSC cards lose their timing function.

Clear the SYNCCLK Alarm

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

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

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

Step 4 If the primary reference clock is an incoming port on the ONS 15600, complete the "Clear the LOF (OCN) Alarm" procedure on page 2-83.

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).

2.6.186 SYNC-FREQ

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

Logical Objects: BITS, OCN

The Synchronization Reference Frequency Out of Bounds alarm occurs when the synchronization frequency reference for the NE (node) is not within acceptable boundaries.

Clear the SYNC-FREQ Alarm

Step 1 Verify that the internal or BITS timing reference is stable. The timing reference is located on the active TSC card. Check for any alarms against this card and troubleshoot them.

Step 2 If the alarm does not clear, complete the "Soft-Reset a Card Using CTC" procedure on page 2-136.

Step 3 If the alarm clears, complete the "Replace a TSC Card" procedure on page 2-142.

Note It takes approximately 20 minutes for the active TSC card to transfer the system software to the newly installed TSC card. Software transfer occurs in instances where different software versions exist on the two cards. When the transfer completes, the TSC card reboots and goes into standby mode after approximately three minutes.

Note If the active and standby TSC cards have the same versions of software, it takes approximately three minutes for software to be updated on a standby TSC card.

Step 4 If the SYNC-FREQ alarm continues to report after replacing the TSC card, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.187 SYNCPRI

Default Severity: Minor (MN), Non-Service-Affecting (NSA) for EXT-SREF; Major (MJ), Service-Affecting (SA) for NE-SREF

Logical Objects: EXT-SREF, NE-SREF

A Primary Synchronization Reference Failure alarm occurs at the NE (node) level when the ONS 15600 loses the primary timing source (reference 1). The ONS 15600 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 15600 should switch to its second timing source (reference 2). This switch also triggers the SWTOSEC alarm.

Clear the SYNCPRI Alarm

Step 1 From node view, click the **Provisioning > Timing > General** tabs and identify the timing source in REF-1 of the NE Reference.

Step 2 If REF-1 is Internal, this refers to the active TSC card. Look for any alarms related to the TSC card and troubleshoot them.

Step 3 If REF-1 is BITS, follow the "Clear the LOF (BITS) Alarm" procedure on page 2-82.

Step 4 If the primary reference clock is an incoming port on the ONS 15600, follow the "Clear the LOF (OCN) Alarm" procedure on page 2-83.

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).

2.6.188 SYNCSEC

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

Logical Objects: EXT-SREF, NE-SREF

A Second Synchronization Reference Failure Alarm occurs at the NE (node) level when the ONS 15600 loses the second timing source (reference 2). If SYNCSEC occurs, the ONS 15600 should switch to a third timing source (reference 3) to obtain valid timing for the ONS 15600. This switch also triggers the "SWTOTHIRD" condition on page 2-117.

Clear the SYNCSEC Alarm

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

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

Step 3 If the second reference is a BITS input, follow the "Clear the LOS (BITS) Alarm" procedure on page 2-86.

Step 4 If the second timing source is an incoming port on the ONS 15600, follow the "Clear the LOF (OCN) Alarm" procedure on page 2-83.

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).

2.6.189 SYNCTHIRD

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

Logical Object: EXT-SREF

A Loss of Timing on Third Reference alarm occurs when the ONS 15600 loses the third timing source (reference 3). If SYNCTHIRD occurs and the ONS 15600 uses an internal reference for source three, the TSC card might have failed. The ONS 15600 often reports either the "FRNGSYNC" alarm on page 2-67 or the "HLDOVRSYNC" condition on page 2-72 after a SYNCTHIRD alarm.

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 "Change Node Settings" chapter in the *Cisco ONS 15600 Procedure Guide*.

Step 3 If the third timing source is a BITS input, complete the "Clear the LOS (BITS) Alarm" procedure on page 2-86.

Step 4 If the third timing source is an incoming port on the ONS 15600, complete the "Clear the LOF (OCN) Alarm" procedure on page 2-83.

Step 5 If the third timing source uses the internal ONS 15600 timing, complete the "Soft-Reset a Card Using CTC" procedure on page 2-136.

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 reseat the card, complete "Reset a Card with a Card Pull (Reseat)" procedure on page 2-138. If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the "Replace an OC-48 Card or OC-192 Card" procedure on page 2-140.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15600. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

2.6.190 SYSBOOT

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

Logical Object: NE

The System Reboot alarm indicates that new software is booting on the node or shelf TSC card. No action is required. The alarm clears when all cards finish rebooting the new software. The reboot takes approximately three minutes.

2.6.191 TIM-P

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

Logical Object: STSMON

The STS TIM-P alarm occurs when the current expected STS-1 path trace string does not match the current received path trace string. Path Trace Mode must be set to manual for this alarm to occur.

In manual mode in the Path Trace area, the user can type a new expected string into the field. This string must match the string typed into the Current Received String field for the sending port. If these fields do not match, it is typically because of upstream PTE error.

Clear the TIM-P Alarm

Step 1 Log into CTC at the circuit source and note which slot and port is reporting the alarm in the Alarms window.

Step 2 Click the **Circuits > Circuits** tabs.

Step 3 Select the circuit reporting the alarm by identifying it according to its Source or Destination column slots and ports. This circuit has probably switched to the protect port.

Step 4 Click the **Edit** button.

Step 5 In the Edit Circuit window, check the **Show Detailed Circuit Map** check box and click **Apply**.

Step 6 On the detailed circuit map, right-click the drop/destination circuit port and choose **Edit Path Trace** from the shortcut menu.

Step 7 Compare the Current Received String and Current Expected String entries in the path trace dialog box.

Step 8 If the strings differ and the Current Received String is correct but the Current Expected String is not, correct the Transmit or Expected strings and click **Apply**.

Step 9 If the strings differ and the Current Expected String is correct but the Current Received String is not, there is a problem with the PTE upstream. Troubleshoot the problem in the PTE.

Step 10 Click **Close**.

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).

2.6.192 TPTFAIL (POS)

The TPTFAIL alarm for packet over SONET (POS) is not used in this platform in this release. It is reserved for future development.

2.6.193 UNEQ-P

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

Logical Object: STSMON

An SLMF Unequipped Path Signal Label Mismatch Failure alarm occurs when the path does not have a valid sender. The 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.

UNEQ-P occurs in the node that terminates a path. The path layer is the segment between the originating equipment and the terminating equipment. This segment can encompass several consecutive line segments.

An UNEQ-P error message on the ONS 15600 indicates that the node reporting the "RFI-P" condition on page 2-106 is the terminating node on that path segment.

Note If you have created a new path but it has no signal, an UNEQ-P alarm is reported on the traffic (OC-N) cards and an AIS-P alarm is reported on the terminating cards. These alarms clear when the path carries a signal.

Clear the UNEQ-P Alarm

Step 1 From node view, navigate to the **Circuits > Circuits** tabs.

Under the State column, check for any circuit that has the status INCOMPLETE. (A completed circuit has ACTIVE status.)

Note Circuits have an incomplete status while they are in the process of being routed on the system. If you have created a large number of circuits, this status can remain for several minutes before it changes to active.

Step 2 If the alarm remains for some time and the circuit does not clear the alarm, delete the circuit by completing the following steps:

a. Click the incomplete circuit to highlight it.

b. Click **Delete**.

Step 3 Recreate the circuit as necessary; refer to the "Create Circuits" chapter in the *Cisco ONS 15600 Procedure Guide* for instructions.

Step 4 If the alarm does not clear after re-creation, ensure that the circuit continues to pass traffic using an optical test set; refer to the "Create Circuits" chapter in the *Cisco ONS 15600 Procedure Guide* for circuit test procedures.

Step 5 If the alarm does not clear, verify that the incoming signal is valid by testing with an optical test set.

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) to report a Service-Affecting (SA) problem.

2.6.194 UNPROT-SYNCCLK

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

Logical Object: NE

The Unprotected Synchronization or Clock Equipment alarm indicates that only one TSC card has acquired the primary timing reference. The alarm is reported if there is no standby TSC card, or if the standby TSC card has restarted and 700 seconds (in FSTSYNC mode) have not elapsed.

This condition is normal following a change to the system timing reference (such as BITS to Line or Line to BITS). Changing the clock reference causes both TSC cards to raise the "FSTSYNC" condition on page 2-67, for 700 seconds. The UNPROT-SYNCCLK alarm occurs during this period. If both TSC cards are reset within 700 seconds of each other, this alarm occurs also and remains until both TSC cards attains the clock reference. If the alarm does not clear, follow the procedure below.

Clear the UNPROT-SYNCCLK Alarm

Step 1 Determine whether one or both TSC cards have the "FSTSYNC" condition on page 2-67 raised. If either TSC card has a FSTSYNC condition, wait 700 seconds for the condition and the UNPROT-SYNCCLK alarm to clear.

Step 2 If FSTSYNC was reported and continues after 700 seconds, replace the standby TSC card. Continue with Step 7.

Step 3 If FSTSYNC is not reported, from node view, click the **Provisioning > Timing > General** tabs.

Step 4 Verify the current configuration for REF-1 of the NE Reference.

If the primary reference clock is an incoming port on the ONS 15600, follow the "Clear the LOF (OCN) Alarm" procedure on page 2-83.

Step 5 If no protect TSC card is installed, install one. Refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15600 Procedure Guide* for instructions.

Step 6 If the alarm persists, remove and reinsert (reseat) the standby TSC card by completing the following steps and wait 700 seconds for the TSC card to acquire the reference.

a. Open the card ejectors.

b. Slide the card out of the slot.

c. Slide the card into the slot along the guide rails.

d. Close the ejectors.

Step 7 If the alarm reappears after you perform the switch, complete the "2.8.5 Verify or Create Node DCC Terminations" procedure on page 2-145 on the standby TSC card and wait 700 seconds for the TSC card to acquire the reference.

Note It takes approximately 20 minutes for the active TSC card to transfer the system software to the newly installed TSC card. Software transfer occurs in instances where different software versions exist on the two cards. When the transfer completes, the TSC card reboots and goes into standby mode after approximately three minutes.

Note If the active and standby TSC cards have the same versions of software, it takes approximately three minutes for software to be updated on a standby TSC card.

2.6.195 UNPROT-XCMTX

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

Logical Object: NE

The Unprotected Cross-Connection Matrix Equipment alarm indicates that only one functional SSXC card on the node supports the cross-connection. The alarm clears if the redundant SSXC card is installed. This alarm could be accompanied by the "2.6.98 IMPROPRMVL (EQPT for the SSXC or TSC Card)" procedure on page 2-74 or the "EQPT (EQPT)" alarm on page 2-44.

Clear the UNPROT-XCMTX Alarm

Step 1 If there is no protect SSXC card installed, install one.

Allow the newly installed SSXC card to boot.

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).

2.6.196 UNROUTEABLE-IP

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

Logical Object: NE

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

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

Clear the EXERCISE-SPAN-FAIL Condition

Step 1 Look for and clear, if present, the "LOF (OCN)" alarm on page 2-83, the "LOS (OCN)" alarm on page 2-87, or a BLSR alarm.

Step 2 Complete the "Initiate an Exercise Ring Switch on a BLSR" procedure on page 2-135.

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).

2.6.197 UPGRADE

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

Logical Object: NE

The System Upgrade in Progress condition indicates that a system upgrade is occurring on the TSC card.

When software is downloaded, it is loaded into the available code volume on the active TSC card. The software is copied to the available code volume on the standby TSC card next. The "SFTWDOWN" condition on page 2-111 occurs at that time. When the user activates the load, the UPGRADE condition occurs.

Note Whenever TSC cards are changed from active to standby, it takes approximately 12 minutes to completely synchronize to the timing source because the Stratum 3E timing module is being adopted.

2.6.198 WKSWPR

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

Logical Objects: OCN, STSMON

The Working Switched To Protection condition occurs when a line has a failure, the "LOS (OCN)" alarm on page 2-87 or the "SD-L" condition on page 2-108.

This condition is also raised when you use the FORCE RING, FORCE SPAN, 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 LOF (OCN) Alarm" procedure on page 2-83. (It is also used for LOS.)

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).

2.6.199 WTR

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

Logical Objects: OCN, STSMON

The Wait to Restore condition indicates that revertive switching is specified and that a switch to protection occurred. When the working path is viable, this condition occurs while the wait to restore timer has not expired. The condition clears when the timer expires and traffic switches back to the working path.

2.6.200 XCMTX

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

Logical Object: NE

The Unavailable Cross-Connection Matrix Equipment alarm indicates no cross-connection matrix on the NE (node). If there was previously a single SSXC card running in unprotected mode, that card fails. If there were two cards running in protected mode, the matrix has become unavailable on both. Troubleshoot with the "Clear the UNPROT-XCMTX Alarm" procedure on page 2-123.

2.7 LED Behavior

The following the subsections describe LED behaviors of the TSC card, SSXC card, and OC-N cards.

2.7.1 TSC Card-Level Indicators

Table 2-13 lists typical card-level TSC card LED behaviors. Table 2-14 lists typical network-level TSC card LED behaviors.

Table 2-13 TSC Card-Level Indicators

Indicator LED	Color	Definition
STAT	Red	Indicates a hardware fault; this LED is off during normal operation. Replace the card if the STAT LED persists. During diagnostics, the LED flashes quickly during initialization and slowly during configuration synchronization.
SRV	Green	The service mode of the card; green indicates that the card is in use and no light indicates that the card can be removed for service.
ACT/STBY	Green	The ACT/STBY (Active/Standby) LED indicates that the TSC card is active (green) or standby (off). It is not present on the optical cards.

2.7.2 TSC Card Network-Level Indicators

Table 2-14 TSC Card Network-Level Indicators

Indicator LED	Color	Definition
LINE	Green	Node timing is synchronized to a line timing reference.
EXTERNAL	Green	Node timing is synchronized to an external timing reference.
FREE RUN	Green	The node is not using an external timing reference. Indicated when the timing mode is set to an internal reference or after all external references are lost.
HOLDOVER	Amber	External/line timing references have failed. The TSC card has switched to internal timing and the 24-hour holdover period has not elapsed.
ACO	Amber	The alarm cutoff (ACO) push button has been activated. After pressing the ACO button, the amber ACO LED turns on. The ACO button opens the audible closure on the backplane. The ACO state is stopped if a new alarm occurs. After the originating alarm is cleared, the ACO LED and audible alarm control are reset.

2.7.3 SSXC Card-Level Indicators

Table 2-15 describes the functions of the card-level LEDs on the SSXC card faceplate.

Table 2-15 SSXC Card-Level Indicators

Indicators LED	Color	Definition
STAT	Red	Indicates a hardware fault; this LED is off during normal operation. Replace the card if the STAT LED persists. During diagnostics, the LED flashes quickly during initialization and flashes slowly during configuration synchronization.
SRV	Green	The service mode of the card. Green indicates the card is in use; no light indicates that the card can be removed for service.
	Amber	The service mode of the card. Amber indicates the card is in use; no light indicates that the card can be removed for service.

2.7.4 OC-N Card Indicators

Table 2-16 describes the functions of the card-level LEDs on the OC48 and OC-192 cards.

Note OC-N card SF and SD card-level LEDs are not displayed in CTC.

Table 2-16 OC-N Card-Level Indicators

Indicators	Color	Description
STAT LED	Red	Indicates a hardware fault; this LED is off during normal operation. Replace the card if the STAT LED persists. During diagnostics, the LED flashes quickly during initialization and flashes slowly during configuration synchronization.
SRV LED	Green	The service mode of the card; green indicates that the card is in use and no light indicates that the card can be removed for service.
LASER ON	Green	The green LASER ON LED indicates that at least one of the card's lasers is active.

2.8 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 more detailed procedures in the *Cisco ONS 15600 Procedure Guide*.

2.8.1 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 ID or Node ID Number

Step 1 In node view, click **View > Go to Network View**.

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

Step 3 From the Ring ID column, record the Ring ID, or in the nodes column, record the Node IDs in the BLSR. The Node IDs are the numbers in parentheses next to the node name.

Change a BLSR Ring ID Number

Step 1 In node view, click **View > Go to Network View**.

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

Step 3 Highlight the ring and click **Edit**.

Step 4 In the BLSR window, enter the new ID in the Ring ID field.

Step 5 Click **Apply**.

Step 6 Click **Yes** in the Changing Ring ID dialog box.

Change a BLSR Node ID Number

Step 1 In node view, click **View > Go to Network View**.

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

Step 3 Highlight the ring and click **Edit**.

Step 4 In the BLSR window, right-click the node on the ring map.

Step 5 Select **Set Node ID** from the shortcut menu.

Step 6 Enter the new ID in the field.

Step 7 Click **Apply**.

Verify Node Visibility for Other Nodes

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

Step 2 Highlight a BLSR.

Step 3 Click **Ring Map**.

Step 4 Verify that each node in the ring appears on the ring map with a node ID and IP address.

Step 5 Click **Close**.

2.8.2 Protection Switching, Lock Initiation, and Clearing

The following sections give instructions for port, ring, and span switching and switch-clearing commands, as well as lock-ons and lockouts.

Initiate a 1+1 Protection Port Force Switch Command

This procedure switches 1+1 protection group traffic from one port in the group to the other using a Force switch.

Caution The Force command overrides normal protective switching mechanisms. Applying this command incorrectly can cause traffic outages.

Caution Traffic is not protected during a Force protection switch.

Note A Force command switches traffic on a working path even if the path has signal degrade (SD) or signal fail (SF) conditions. A Force switch does not switch traffic on a protect path. A Force switch preempts a Manual switch.

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

Step 2 In the Protection Groups area, select the protection group with the port you want to switch.

Step 3 In the Selected Groups area, select the port belonging to the card you are replacing. You can carry out this command for the working or protect port. For example, if you need to replace the card with the Protect/Standby port, click this port.

Step 4 In the Switch Commands area, click **Force**.

Step 5 Click **Yes** in the Confirm Force Operation dialog box.

Step 6 If the switch is successful, the group says "Force to working" in the Selected Groups area.

Initiate a 1+1 Protection Port Manual Switch Command

This procedure switches 1+1 protection group traffic from one port in the group to the other using a Manual switch.

Note A Manual command switches traffic if the path has an error rate less than the signal degrade. A Manual switch is preempted by a Force switch.

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

Step 2 In the Protection Groups area, select the protection group with the port you want to switch.

Step 3 In the Selected Groups area, select the port belonging to the card you are replacing. You can carry out this command for the working or protect port. For example, if you need to replace the card with the protect/standby port, click this port.

Step 4 In the Switch Commands area, click **Manual**.

Step 5 Click **Yes** in the Confirm Force Operation dialog box.

Step 6 If the switch is successful, the group now says "Manual to working" in the Selected Groups area.

Clear a 1+1 Protection Port Force or Manual Switch Command

Note If the 1+1 protection group is configured as revertive, clearing a Force switch to protect (or working) moves traffic back to the working port. In revertive operation, the traffic always switches back to working. There is no revert to protect. If ports are not configured as revertive, clearing a Force switch to protect does not move traffic back.

Note If the Force Switch was user-initiated, the reversion occurs immediately when the clear command is issued. The five-minute WTR period is not needed in this case. If the Force was system-initiated, allow the five-minute waiting period (during WTR) before the reversion occurs.

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

Step 2 In the Protection Groups area, choose the protection group containing the port you want to clear.

Step 3 In the Selected Group area, choose the port you want to clear.

Step 4 In the Switching Commands area, click **Clear**.

Step 5 Click **Yes** in the Confirmation Dialog box.

The Force switch is cleared. Traffic immediately reverts to the working port if the group was configured for revertive switching.

Initiate a Card or Port Lock On Command

Note For 1:1 and 1:N electrical protection groups, working or protect cards can be placed in the Lock On state. For a 1+1 optical protection group, only the working port can be placed in the Lock On state.

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

Step 2 In the Protection Groups list, click the protection group where you want to apply a lock-on.

Step 3 If you determine that the protect card is in standby mode and you want to apply the lock-on to the protect card, make the protect card active if necessary by completing the following steps:

a. In the Selected Group list, click the protect card.

b. In the Switch Commands area, click **Force**.

Step 4 In the Selected Group list, click the active card where you want to lock traffic.

Step 5 In the Inhibit Switching area, click **Lock On**.

Step 6 Click **Yes** in the confirmation dialog box.

Initiate a Card or Port Lock Out Command

Note For 1:1 or 1:N electrical protection groups, working or protect cards can be placed in the Lock Out state. For a 1+1 optical protection group, only the protect port can be placed in the Lock Out state.

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

Step 2 In the Protection Groups list, click the protection group that contains the card you want to lock out.

Step 3 In the Selected Group list, click the card that you want to lock traffic out of.

Step 4 In the Inhibit Switching area, click **Lock Out**.

Step 5 Click **Yes** in the confirmation dialog box.

The lockout has been applied and traffic is switched to the opposite card.

Clear a Card or Port Lock On or Lock Out Command

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

Step 2 In the Protection Groups list, click the protection group that contains the card that you want to clear.

Step 3 In the Selected Group list, click the card that you want to clear.

Step 4 In the Inhibit Switching area, click **Unlock**.

Step 5 Click **Yes** in the confirmation dialog box.

The lock-on or lockout is cleared.

Initiate a 1:1 Card Switch Command

Note The Switch command only works on the Active card, whether it is Working or Protect. It does not work on the Standby card.

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

Step 2 Click the protection group that contains the card you want to switch.

Step 3 Under Selected Group, click the active card.

Step 4 Next to Switch Commands, click **Switch**.

The working slot should change to Working/Active and the protect slot should change to Protect/Standby.

Initiate a Force Switch for All Circuits on a Path Protection Span

This procedure forces all circuits in a path protection from the working span to the protect. It is used to remove traffic from a card that originates or terminates path protection circuits.

Caution The Force command overrides normal protective switching mechanisms. Applying this command incorrectly can cause traffic outages.

Caution Traffic is not protected during a Force protection switch.

Step 1 Log into a node on the network. If you are already logged in, continue with Step 3.

Step 2 Click **View > Go to Network View**.

Step 3 Right-click a network span and choose **Circuits**.

The Circuits on Span dialog box shows the path protection circuits, including circuit names, locations, and a color code showing which circuits are active on the span.

Step 4 Click the **Perform UPSR span switching** field.

Step 5 Choose **Force Switch Away** from the drop-down list.

Step 6 Click **Apply**.

Step 7 In the Confirm UPSR Switch dialog box, click **Yes**.

Step 8 In the Protection Switch Result dialog box, click **OK**.

In the Circuits on Span dialog box, the switch state for all circuits is FORCE. Unprotected circuits do not switch.

Initiate a Manual Switch for All Circuits on a Path Protection Span

This procedure manually switches all circuits in a path protection from the working span to the protect. It is used to remove traffic from a card that originates or terminates path protection circuits.

Caution The Manual command does not override normal protective switching mechanisms.

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 Right-click a network span and choose **Circuits**.

The Circuits on Span dialog box shows the path protection circuits, including circuit names, locations, and a color code showing which circuits are active on the span.

Step 3 Click the **Perform UPSR span switching** field.

Step 4 Choose **Manual** from the drop-down list.

Step 5 Click **Apply**.

Step 6 In the Confirm UPSR Switch dialog box, click **Yes**.

Step 7 In the Protection Switch Result dialog box, click **OK**.

In the Circuits on Span dialog box, the switch state for all circuits is Manual. Unprotected circuits do not switch.

Initiate a Lock Out of Protect Switch for All Circuits on a Path Protection Span

This procedure prevents all circuits in a path protection working span from switching to the protect span. It is used to keep traffic off cards that originate or terminate path protection circuits.

Caution The Lock Out of Protect command does not override normal protective switching mechanisms.

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 Right-click a network span and choose **Circuits**.

The Circuits on Span dialog box shows the path protection circuits, including circuit names, locations, and a color code showing which circuits are active on the span.

Step 3 Click the **Perform UPSR span switching** field.

Step 4 Choose **Lock Out of Protect** from the drop-down list.

Step 5 Click **Apply**.

Step 6 In the Confirm UPSR Switch dialog box, click **Yes**.

Step 7 In the Protection Switch Result dialog box, click **OK**.

In the Circuits on Span dialog box, the switch state for all circuits is FORCE. Unprotected circuits do not switch.

Clear a Path Protection Span External Switching Command

Note If the ports terminating a span are configured as revertive, clearing a Force switch to protect (or working) moves traffic back to the working port. If ports are not configured as revertive, clearing a Force switch to protect does not move traffic back.

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 Right-click a network span and choose **Circuits**.

The Circuits on Span dialog box shows the path protection circuits, including circuit names, locations, and a color code showing which circuits are active on the span.

Step 3 Initiate a Force switch for all circuits on the span by completing the following steps:

a. Click the **Perform UPSR span switching** field.

b. Choose **Clear** from the drop-down list.

c. Click **Apply**.

d. In the Confirm UPSR Switch dialog box, click **Yes**.

e. In the Protection Switch Result dialog box, click **OK**.

In the Circuits on Span dialog box, the switch state for all circuits is Clear. Unprotected circuits do not switch.

Initiate a Force Ring Switch on a BLSR

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 In network view, click the **Provisioning > BLSR** tabs.

Step 4 Click the row of the BLSR you are switching, then click **Edit**.

Step 5 Right-click a BLSR node west port and choose **Set West Protection Operation**.

Step 6 In the Set West Protection Operation dialog box, choose **Force Ring** from the drop-down list.

Step 7 Click **OK**.

Step 8 Click **Yes** in the two Confirm BLSR Operation dialog boxes that appear.

Initiate a Force Span Switch on a Four-Fiber BLSR

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 In network view, click the **Provisioning > BLSR** tabs.

Step 4 Click the row of the BLSR you are switching, then click **Edit**.

Step 5 Right-click a BLSR node west port and choose **Set West Protection Operation**.

Step 6 In the Set West Protection Operation dialog box, choose **Force Span** from the drop-down list.

Step 7 Click **OK**.

Step 8 Click **Yes** in the two Confirm BLSR Operation dialog boxes that appear.

Initiate a Manual 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**.

Step 5 In the Set West Protection Operation dialog box or the Set East Protection Operation dialog box, choose **Manual Ring** from the drop-down list.

Step 6 Click **OK**.

Step 7 Click **Yes** in the two Confirm BLSR Operation dialog boxes.

Initiate a Lock Out on a BLSR Protect Span

Step 1 From the View menu, choose **Go to Network View**.

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

Step 3 Choose the BLSR and click **Edit**.

Step 4 Right-click the BLSR node channel (port) and choose **Set West Protection Operation** (if you chose a west channel) or **Set East Protection Operation** (if you chose an east channel).

Step 5 In the Set West Protection Operation dialog box or the Set East Protection Operation dialog box, choose **Lockout Protect Span** from the drop-down list.

Step 6 Click **OK**.

Step 7 Click **Yes** in the two Confirm BLSR Operation dialog boxes.

Initiate an Exercise Ring Switch on a BLSR

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 Click **View > Go to Network View**.

Step 3 Click the **Provisioning > BLSR** tabs.

Step 4 Click the row of the BLSR you are exercising, then click **Edit**.

Step 5 Right-click the west port of a node and choose **Set West Protection Operation**.

Step 6 In the Set West Protection Operation dialog box, choose **Exercise Ring** from the drop-down list.

Step 7 Click **OK**.

Step 8 Click **Yes** in the Confirm BLSR Operation dialog box.

Initiate an Exercise Ring Switch on a Four Fiber BLSR

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 Click **View > Go to Network View**.

Step 3 Click the **Provisioning > BLSR** tabs.

Step 4 Click the row of the BLSR you are exercising, then click **Edit**.

Step 5 Right-click the west port of a node and choose **Set West Protection Operation**.

Step 6 In the Set West Protection Operation dialog box, choose **Exercise Span** from the drop-down list.

Step 7 Click **OK**.

Step 8 Click **Yes** in the Confirm BLSR Operation dialog box.

Clear a BLSR External Switching Command

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 Click **View > Go to Network View**.

Step 3 Click the **Provisioning > BLSR** tabs.

Step 4 Click the BLSR you want to clear.

Step 5 Right-click the west port of the BLSR node where you invoked the switch and choose **Set West Protection Operation**.

Step 6 In the Set West Protection Operation dialog box, choose **Clear** from the drop-down list.

Step 7 Click **OK**.

Step 8 Click **Yes** in the Confirm BLSR Operation dialog box.

2.8.3 CTC Card Resetting and Switching

This section gives instructions for TSC cards and SSXC cross-connect cards.

Soft-Reset a Card Using CTC

This procedure is used to force system control from the active card, including the TSC card, SSXC, or optical (traffic) card. In this kind of reset, the card is rebooted but the flash memory is not cleared.

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

Note Whenever TSC cards are changed from active to standby, it takes approximately 12 minutes to completely synchronize to the timing source because the Stratum 3E timing module is being adopted.

Step 1 If you are resetting a TSC card, determine whether it is active and which is standby by positioning the cursor over the active card. An active TSC card has a green ACT/STBY LED illuminated.

Step 2 Right-click the card to display the shortcut menu.

Step 3 Click **Soft-reset Card**.

Step 4 Click **Yes** when the confirmation dialog box appears.

Step 5 Click **OK** when the “Lost connection to node, changing to Network View” dialog box appears.

Note The TSC card takes several minutes to reboot. Refer to the "Card Features and Functions" chapter in the *Cisco ONS 15600 Reference Manual* for more information about LED behavior during TSC card reboots.

Step 6 If you reset a TSC card, confirm that it is in standby mode after the reset.

Tip If you run the cursor over the TSC card in CTC, a popup displays the card's status (whether active or standby).

Hard-Reset a Card Using CTC

This procedure is used to force system control from the active TSC card to the standby TSC card, or it is used to reset the SSXC or an optical (traffic) card. This kind of reset reboots the card and clears the flash memory, making it appear like a newly inserted card.

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

Caution Use hard resets with caution. There could be up to 15 other sets of bandwidth affected by a hard reset.

Note The hard-reset option is enabled only when the card is placed in the OOS-MA,MT service state.

Note When a TSC card changes from active to standby, the node takes approximately 12 minutes to synchronize completely to the timing source because of the more accurate Stratum 3E timing module being adopted.

Step 1 If you are resetting a TSC card, determine which one is the active card and which is the standby card. (Position the cursor over the active card. An active TSC card has a green ACT/STBY LED illuminated.)

Step 2 Right-click the card (or active TSC card) to display the shortcut menu.

Step 3 Click **Hard-reset Card**.

Step 4 Click **Yes** when the confirmation dialog box appears.

Step 5 Click **OK** when the "Lost connection to node, changing to Network View" dialog box appears.

Note The TSC card takes several minutes to reboot. Refer to the "Card Features and Functions" chapter in the *Cisco ONS 15600 Reference Manual* for more information about LED behavior during TSC card reboots.

Step 6 If you reset a TSC card, confirm that this TSC card you reset is in standby mod.

If you run the cursor over the TSC card in CTC, a popup displays the card's status (whether active or standby).

Tip If you run the cursor over the TSC card in CTC, a popup displays the card's status (whether active or standby).

Request a Cross-Connect Card Preferred Copy Switch

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

Step 1 Determine which SSXC card is the preferred copy and which is currently in use.

In node view, click the **Maintenance > Preferred Copy** tabs.

Step 2 In the Set Preferred drop-down list, select the alternate copy. (For example, if the Slot 8 Copy B is preferred and in use, select the Slot 6 Copy A.

Caution Do not select the copy that you want to replace.

Step 3 Click **Apply**.

Step 4 Click **Yes** in the confirmation dialog box.

Note If you attempt a preferred copy switch and the switch is unsuccessful, it indicates a problem on the alternate SSXC card.

Step 5 Click **Refresh** until the tab shows that the alternate copy you selected is now the preferred copy. The Currently Used field dynamically changes to display the newly selected preferred copy.

2.8.4 Physical Card Reseating, Resetting, and Replacement

This section gives instructions for physically reseating and replacing TSC card, SSXC cards, and traffic cards.

Reset a Card with a Card Pull (Reseat)

Note If you are pulling a TSC card, determine whether a TSC card is active or standby by positioning the cursor over the TSC card graphic to view the status.

Note Resetting a standby TSC card does not change its status to active.

Step 1 Ensure that the card you want to reset is in standby mode.

(A TSC card that is ready for service has a green SRV LED illuminated. An active TSC card has a green ACT/STBY LED illuminated, but a standby card does not have this LED illuminated.)

If you run the cursor over the TSC card in CTC, a popup displays the card's status (whether active or standby).

Step 2 Unlatch the top and bottom ejector levers on the card.

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 ejector levers.

Note A TSC card takes several minutes to reboot. Refer to the "Card Features and Functions" chapter in the *Cisco ONS 15600 Reference Manual* for more information about LED behavior during TSC card reboots.

Note When a standby TSC card is removed and reinserted (reseated), all three fan lights might momentarily illuminate, indicating that the fan controller cards have also reset.

Replace an SSXC Card

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

Note The ONS 15600 system dynamically changes the preferred copy status from one SSXC to the redundant copy if an error is detected on a card port. You can see this change in the CTC node view Maintenance > Preferred Copy window Currently Used field. If errors are detected on both SSXC copies, the Currently Used field says Both.

Note You do not need to make any changes to the database if you are replacing it with a card of exactly the same type.

Note Card removal raises an improper removal (IMPROPRMVL) alarm, but this clears after the card replacement is complete.

Step 1 Physically remove the card to be replaced from the ONS 15600 shelf by completing the following steps:

a. Open the card ejectors.

b. Slide the card out of the slot.

Step 2 Physically replace the SSXC card in the shelf by completing the following steps:

a. Open the ejectors on the replacement card.

b. Slide the replacement card into the slot along the guide rails until it contacts the backplane.

c. Close the ejectors.

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

Replace an OC-48 Card or OC-192 Card

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

Note Card removal raises an improper removal (IMPROPRMVL) alarm, but this clears after the card replacement is completed.

Step 1 Ensure that the card you are replacing does not carry traffic in a 1+1 protection group by completing the following steps:

a. In node view, click the **Maintenance > Protection** tabs.

b. Choose the first group listed under Protection Groups.

c. Verify that the slot number for the card you are replacing does not appear in the Selected Groups list. For example, if you are replacing the OC-48 card in Slot 3, ensure Selected Groups does not contain any entries that start with s3, regardless of the port.

d. Repeat Steps b and c for each protection group.

e. If any of the groups contain a port on the card you want to replace, complete the "Initiate a 1+1 Protection Port Force Switch Command" procedure on page 2-128.

Step 2 Ensure that the card you are replacing does not carry path protection circuit traffic by completing the following steps:

Note A port can be part of a 1+1 protection group or part of a path protection, but it cannot be configured for both. However, different ports on one card can be configured in different ways. If you move all of the traffic off some 1+1 ports, you still need to check whether the remaining ports are carrying path protection traffic.

a. From the **View** menu, choose Go to Parent View.

b. Click the **Circuits** tab.

c. View the circuit source and destination ports and slots. If any circuits originate or terminate in the slot containing the card you are replacing, perform the "Initiate a Force Switch for All Circuits on a Path Protection Span" procedure on page 2-131.

Note If the card you are replacing is not configured for any port or circuit protection, but does carry traffic, bridge and roll this traffic onto another card. Follow the "Bridge and Roll Traffic" procedure in the "Manage Circuits" chapter in the *Cisco ONS 15600 Procedure Guide*.

Step 3 Ensure that the card you are replacing does not carry BLSR circuit traffic by completing the following steps.

a. In the CTC node view, click **View > Go to Parent View**.

b. Click the **Circuits** tab.

c. View the circuit source and destination ports and slots. If any circuits originate or terminate in the slot containing the card you are replacing, perform the "Initiate a Force Span Switch on a Four-Fiber BLSR" procedure on page 2-134.

Note If the card you are replacing is not configured for any port or circuit protection, but does carry traffic, bridge and roll this traffic onto another card. Refer to the "Manage Circuits" chapter in the *Cisco ONS 15600 Procedure Guide*.

Step 4 Remove any fiber optic cables from the ports.

Step 5 Physically remove the card that you want to replace from the ONS 15600 shelf by completing the following steps:

a. Open the card ejectors.

b. Slide the card out of the slot.

Step 6 Physically replace the OC-48 or OC-192 card in the shelf by completing the following steps:

a. Open the ejectors on the replacement card.

b. Slide the replacement card into the slot along the guide rails until it contacts the backplane.

c. Close the ejectors.

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

Step 7 Clear the Force switches.

- To clear 1+1 Force switches, complete the "Clear a 1+1 Protection Port Force or Manual Switch Command" procedure on page 2-129.
- To clear path protection Force switches, complete the "Clear a Path Protection Span External Switching Command" procedure on page 2-133.

Step 8 When the card is in service and receiving traffic, reset the card's physical receive power level threshold in CTC by completing the following steps:

a. Double-click the newly installed card in CTC node view.

b. Click the **Provisioning > Threshold** tabs.

c. Click the **Physical** radio button.

d. Click **Set OPM** for each port on the card.

Replace a TSC Card

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

Note When an error is detected on a TSC card, the ONS 15600 system switches control to the second TSC card; therefore, so it should not be necessary to change control when you replace the card.

Note You do not need to make any changes to the database if you are replacing it with a card of exactly the same type.

Note Card removal raises an improper removal (IMPROPRMVL) alarm, but this clears after the card replacement is completed.

Step 1 Ensure that the card you are replacing is not the active TSC card: Run the mouse over the card in CTC. If the card says Active, switch it to Standby by completing the following steps:

a. Right-click the active TSC card to display the shortcut menu.

b. Click **Soft-reset Card**.

c. Click **Yes** when the confirmation dialog box appears.

d. Click **OK** when the "Lost connection to node, changing to Network View" dialog box appears.

Note The TSC card takes several minutes to reboot. Refer to the "Card Features and Functions" chapter in the *Cisco ONS 15600 Reference Manual* for more information about LED behavior during TSC card reboots.

Note Whenever TSC cards are changed from active to standby, it takes approximately 12 minutes to completely synchronize to the new system clock source due to the more accurate Stratum 3E timing module being adopted.

Step 2 Confirm that the TSC card you reset is in standby mode after the reset.

A TSC card that is ready for service has a green SRV LED illuminated. An active TSC card has a green ACT/STBY LED illuminated, but a standby card does not have this LED illuminated.

Tip If you run the cursor over the TSC card in CTC, a popup displays the card's status (whether active or standby).

Step 3 Physically remove the card you want to replace from the ONS 15600 by completing the following steps:

a. Open the card ejectors.

b. Slide the card out of the slot.

Step 4 Insert the replacement TSC card into the empty slot by completing the following steps:

a. Open the ejectors on the replacement card.

b. Slide the replacement card into the slot along the guide rails until it contacts the backplane.

c. Close the ejectors.

Step 5 If you want to make the replaced TSC card active, complete Steps b through d in Step 2 again.

Replace an ASAP Carrier Module

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

Note You do not need to make any changes to the database if you are replacing it with a card of exactly the same type.

Note Card removal raises an improper removal (IMPROPRMVL) alarm, but this clears after the card replacement is completed.

Step 1 Verify that the card is not carrying any traffic. If it is, switch it using the appropriate procedure.

Step 2 Physically remove the ASAP carrier module from the ONS 15600 by completing the following steps:

a. Open the card ejectors.

b. Slide the card out of the slot.

Step 3 Insert the replacement carrier module into the empty slot by completing the following steps:

a. Open the ejectors on the replacement card.

b. Slide the replacement card into the slot along the guide rails until it contacts the backplane.

c. Close the ejectors.

Replace an ASAP 4PIO (PIM) Module

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

Note You do not need to make any changes to the database if you are replacing it with a card of exactly the same type.

Note Card removal raises an improper removal (IMPROPRMVL) alarm, but this clears after the card replacement is completed.

Step 1 Use a Phillips screwdriver to loosen the screws at the top right and bottom left of the 4PIO (PIM) module.

Step 2 Carefully slide the motherboard of the module along the top and bottom guide rails out of the slot.

Step 3 Carefully slide the motherboard of the new module into the slot.

Step 4 Tighten the screws at the top right and bottom left of the 4PIO (PIM) module.

Note The 4PIO (PIM) LEDs do not light until a fixed-rate PIM is installed in the associated slot or a multirate optical (MRO) PIM is installed and an optical rate is provisioned.

Note If you insert a card into a slot provisioned for a different card, all red LEDs turn on and you will see a mismatched equipment (MEA) alarm for that slot when you open CTC.

Step 5 After you have logged into CTC, verify that the card appears in CTC card view.

Replace an ASAP SFP (PPM) Module

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

Note You do not need to make any changes to the database if you are replacing it with a card of exactly the same type.

Note Card removal raises an improper removal (IMPROPRMVL) alarm, but this clears after the card replacement is completed.

Step 1 Unlatch the bail clasp by moving it to the left before removing the bad SFP (PPM) from the slot.

Step 2 Slide the SFP (PPM) out of the slot.

Step 3 Verify that the new SFP (PPM) is correct for your network and ASAP card. Refer to the *Cisco ONS 15600 Reference Manual* for more information.

Step 4 Orient the new SFP so that the Cisco serial number label is facing away from the shelf (to the right).

Step 5 Slide the SFP into the slot and move the bail clasp to the right to secure the SFP.

Caution Do not remove the protective caps until you are ready to attach the network fiber-optic cable.

Note Multirate SFPs (PPMs) must be provisioned in CTC; single-rate SFPs (PPMs) do not need to be provisioned. Refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15600 Procedure Guide* for provisioning instructions.

2.8.5 Verify or Create Node DCC Terminations

Step 1 In node view, click the **Provisioning > Comm Channels > SDCC** tabs (or other tab as appropriate).

Step 2 View the Port column entries to see where terminations are present for a node. If terminations are missing, proceed to Step 3.

Step 3 If necessary, create a DCC termination by completing the following steps:

a. Click **Create**.

b. In the Create SDCC Terminations dialog box, click the ports where you want to create the DCC termination. To select more than one port, press the Shift key.

c. In the Port State area, click the **Set to IS** radio button.

d. Verify that the Disable OSPF on Link check box is unchecked.

e. Click **OK**.

Set the Optical Power Received Nominal Value

Step 1 In node view, double-click the OC-N card that you want to provision. The card view appears.

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

Step 3 From the Types list, choose **Physical** and click **Refresh**.

Step 4 For the port you want to provision, click the **Set** button in the Set OPR column. In the confirmation dialog box, click **OK**.