

Contents

- 1 MAN-REQ
 - ◆ 1.1 Clear the MAN-REQ Condition
- 2 MANRESET
- 3 MANSWTOINT
- 4 MANSWTOPRI
- 5 MANSWTOSEC
- 6 MANSWTOTHIRD
- 7 MANUAL-REQ-RING
 - ◆ 7.1 Clear the MANUAL-REQ-RING Condition
- 8 MANUAL-REQ-SPAN
 - ◆ 8.1 Clear the MANUAL-REQ-SPAN Condition
- 9 MAX-STATIONS
 - ◆ 9.1 Clear the MAX-STATIONS Alarm
- 10 MEA (AIP)
 - ◆ 10.1 Clear the MEA (AIP) Alarm
- 11 MEA (BIC)
 - ◆ 11.1 Clear the MEA (BIC) Alarm
 - ◇ 11.1.1 Table 2-18: BIC Compatibility Matrix
- 12 MEA (EQPT)
 - ◆ 12.1 Clear the MEA (EQPT) Alarm
- 13 MEA (FAN)
 - ◆ 13.1 Clear the MEA (FAN) Alarm
- 14 MEA (PPM)
- 15 MEA (SHELF)
- 16 MEM-GONE
- 17 MEM-LOW
- 18 MFGMEM
 - ◆ 18.1 Clear the MFGMEM Alarm
- 19 MS-DEG
- 20 MS-EXC
- 21 MT-OCHNC
- 22 NO-CONFIG
 - ◆ 22.1 Clear the NO-CONFIG Condition
- 23 NON-CISCO-PPM
 - ◆ 23.1 Clear the NON-CISCO-PPM Condition
- 24 NOT-AUTHENTICATED
- 25 OCHNC-INC
- 26 OCHTERM-INC
- 27 ODUK-1-AIS-PM
- 28 ODUK-2-AIS-PM
- 29 ODUK-3-AIS-PM
- 30 ODUK-4-AIS-PM
- 31 ODUK-AIS-PM
- 32 ODUK-BDI-PM
- 33 ODUK-LCK-PM
- 34 ODUK-OCI-PM
- 35 ODUK-SD-PM
- 36 ODUK-SF-PM
- 37 ODUK-TIM-PM
- 38 OOU-TPT

- ◆ 38.1 Clear the OOT-TPT Condition
- 39 OPEN-SLOT
 - ◆ 39.1 Clear the OPEN-SLOT Condition
- 40 OPTNTWMIS
- 41 OPWR-HDEG
- 42 OPWR-HFAIL
- 43 OPWR-LDEG
- 44 OPWR-LFAIL
- 45 OSRION
- 46 OTUK-AIS
- 47 OTUK-BDI
- 48 OTUK-IAE
- 49 OTUK-LOF
- 50 OTUK-SD
- 51 OTUK-SF
- 52 OTUK-TIM
- 53 OUT-OF-SYNC
- 54 PARAM-MISM
- 55 PDI-P
 - ◆ 55.1 Clear the PDI-P Condition
- 56 PEER-NORESPONSE
 - ◆ 56.1 Clear the PEER-NORESPONSE Alarm
- 57 PLM-P
 - ◆ 57.1 Clear the PLM-P Alarm
- 58 PLM-V
 - ◆ 58.1 Clear the PLM-V Alarm
- 59 PMI
- 60 PORT-FAIL
- 61 PORT-MISMATCH
- 62 PRC-DUPID
 - ◆ 62.1 Clear the PRC-DUPID Alarm
- 63 PROTNA
 - ◆ 63.1 Clear the PROTNA Alarm
- 64 PROV-MISMATCH
- 65 PTIM
- 66 PWR-FAIL-A
 - ◆ 66.1 Clear the PWR-FAIL-A Alarm
- 67 PWR-FAIL-B
 - ◆ 67.1 Clear the PWR-FAIL-B Alarm
- 68 PWR-FAIL-RET-A
 - ◆ 68.1 Clear the PWR-FAIL-RET-A Alarm
- 69 PWR-FAIL-RET-B
 - ◆ 69.1 Clear the PWR-FAIL-RET-A Alarm
- 70 RAI
 - ◆ 70.1 Clear the RAI Condition
- 71 RCVR-MISS
 - ◆ 71.1 Clear the RCVR-MISS Alarm
- 72 RSV-RT-EXCD-RINGLETO
 - ◆ 72.1 Clear the RSV-RT-EXCD-RINGLETO Alarm
- 73 RSV-RT-EXCD-RINGLET1
 - ◆ 73.1 Clear the RSV-RT-EXCD-RINGLET1 Alarm
- 74 RFI
- 75 RFI-L

- ◆ 75.1 Clear the RFI-L Condition
- 76 RFI-P
 - ◆ 76.1 Clear the RFI-P Condition
- 77 RFI-V
 - ◆ 77.1 Clear the RFI-V Condition
- 78 RING-ID-MIS
 - ◆ 78.1 Clear the RING-ID-MIS Alarm
- 79 RING-MISMATCH
 - ◆ 79.1 Clear the RING-MISMATCH Alarm
- 80 RING-SW-EAST
- 81 RING-SW-WEST
- 82 ROLL
- 83 ROLL-PEND
- 84 ROUTE-OVERFLOW
 - ◆ 84.1 Clear the ROUTE-OVERFLOW Condition
- 85 RPR-PASSTHR
 - ◆ 85.1 Clear the RPR-PASSTHR Condition
- 86 RPR-PEER-MISS
 - ◆ 86.1 Clear the RPR-PEER-MISS Condition
- 87 RPR-PROT-ACTIVE
 - ◆ 87.1 Clear the RPR-PROT-ACTIVE Condition
- 88 RPR-PROT-CONFIG-MISM
 - ◆ 88.1 Clear the RPR-PROT-CONFIG-MISM Alarm
- 89 RPR-RI-FAIL
 - ◆ 89.1 Clear the RPR-RI-FAIL Condition
- 90 RPR-SD
 - ◆ 90.1 Clear the RPR-SD Condition
- 91 RPR-SF
 - ◆ 91.1 Clear the RPR-SF Condition
- 92 RPR-SPAN-MISMATCH
 - ◆ 92.1 Clear the RPR-SPAN-MISMATCH Alarm
- 93 RPRW
 - ◆ 93.1 Clear the RPRW Condition
- 94 RUNCFG-SAVENEED
- 95 SD (DS1, DS3)
 - ◆ 95.1 Clear the SD (DS1, DS3) Condition
- 96 SD (E1)
 - ◆ 96.1 Clear the SD (E1) Condition
- 97 SD (TRUNK)
- 98 SD-L
 - ◆ 98.1 Clear the SD-L Condition
- 99 SD-L (TRUNK)
- 100 SD-P
 - ◆ 100.1 Clear the SD-P Condition
- 101 SD-V
 - ◆ 101.1 Clear the SD-V Condition
- 102 SF (DS1, DS3)
 - ◆ 102.1 Clear the SF (DS1, DS3) Condition
- 103 SF (E1)
 - ◆ 103.1 Clear the SF (E1) Condition
- 104 SF (TRUNK)
- 105 SF-L
 - ◆ 105.1 Clear the SF-L Condition

- 106 SF-L (TRUNK)
- 107 SF-P
 - ◆ 107.1 Clear the SF-P Condition
- 108 SFTWDOWN
- 109 SF-V
 - ◆ 109.1 Clear the SF-V Condition
- 110 SHELF-COMM-FAIL
- 111 SH-IL-VAR-DEG-HIGH
- 112 SH-IL-VAR-DEG-LOW
- 113 SHUTTER-OPEN
- 114 SIGLOSS
 - ◆ 114.1 Clear the SIGLOSS Alarm
- 115 SNTP-HOST
 - ◆ 115.1 Clear the SNTP-HOST Alarm
- 116 SPANLEN-OUT-OF-RANGE
- 117 SPAN-SW-EAST
- 118 SPAN-SW-WEST
- 119 SQUELCH
 - ◆ 119.1 Clear the SQUELCH Condition
- 120 SQUELCHED
 - ◆ 120.1 Clear the SQUELCHED Condition
- 121 SQM
 - ◆ 121.1 Clear the SQM Alarm
- 122 SSM-DUS
- 123 SSM-FAIL
 - ◆ 123.1 Clear the SSM-FAIL Alarm
- 124 SSM-LNC
- 125 SSM-OFF
 - ◆ 125.1 Clear the SSM-OFF Condition
- 126 SSM-PRC
- 127 SSM-PRS
- 128 SSM-RES
- 129 SSM-SDH-TN
- 130 SSM-SETS
- 131 SSM-SMC
- 132 SSM-ST2
- 133 SSM-ST3
- 134 SSM-ST3E
- 135 SSM-ST4
- 136 SSM-STU
 - ◆ 136.1 Clear the SSM-STU Condition
- 137 SSM-TNC
- 138 STS-SQUELCH-L
- 139 SW-MISMATCH
 - ◆ 139.1 Clear the SW-MISMATCH Condition
- 140 SWMTXMOD-PROT
 - ◆ 140.1 Clear the SWMTXMOD-PROT Alarm
- 141 SWMTXMOD-WORK
 - ◆ 141.1 Clear the SWMTXMOD-WORK Alarm
- 142 SWTOPRI
- 143 SWTOSEC
 - ◆ 143.1 Clear the SWTOSEC Condition
- 144 SWTOTHIRD

- ◆ 144.1 Clear the SWTOTHIRD Condition
- 145 SYNC-FREQ
 - ◆ 145.1 Clear the SYNC-FREQ Condition
- 146 SYNCLOSS
 - ◆ 146.1 Clear the SYNCLOSS Alarm
- 147 SYNCPRI
 - ◆ 147.1 Clear the SYNCPRI Alarm
- 148 SYNCSEC
 - ◆ 148.1 Clear the SYNCSEC Alarm
- 149 SYNCTHIRD
 - ◆ 149.1 Clear the SYNCTHIRD Alarm
- 150 SYSBOOT
- 151 TEMP-MISM
 - ◆ 151.1 Clear the TEMP-MISM Condition
- 152 TIM
 - ◆ 152.1 Clear the TIM Alarm
- 153 TIM-MON
 - ◆ 153.1 Clear the TIM-MON Alarm
- 154 TIM-P
 - ◆ 154.1 Clear the TIM-P Alarm
- 155 TIM-S
 - ◆ 155.1 Clear the TIM-S Alarm
- 156 TIM-V
 - ◆ 156.1 Clear the TIM-V Alarm
- 157 TPTFAIL (CEMR, CE100T, CE1000)
 - ◆ 157.1 Clear the TPTFAIL (CEMR, CE100T, CE1000) Alarm
- 158 TPTFAIL (FCMR)
 - ◆ 158.1 Clear the TPTFAIL (FCMR) Alarm
- 159 TPTFAIL (G1000)
 - ◆ 159.1 Clear the TPTFAIL (G1000) Alarm
- 160 TPTFAIL (ML100T, ML1000, MLFX)
 - ◆ 160.1 Clear the TPTFAIL (ML100T, ML1000, MLFX) Alarm
- 161 TRMT
 - ◆ 161.1 Clear the TRMT Alarm
- 162 TRMT-MISS
 - ◆ 162.1 Clear the TRMT-MISS Alarm
- 163 TX-AIS
 - ◆ 163.1 Clear the TX-AIS Condition
- 164 TX-LOF
 - ◆ 164.1 Clear the TX-LOF Condition
- 165 TX-RAI
 - ◆ 165.1 Clear the TX-RAI Condition
- 166 UNC-WORD
- 167 UNEQ-P
 - ◆ 167.1 Clear the UNEQ-P Alarm
- 168 UNEQ-V
 - ◆ 168.1 Clear the UNEQ-V Alarm
- 169 UNQUAL-PPM
 - ◆ 169.1 Clear the UNQUAL-PPM Condition
- 170 UT-COMM-FAIL
- 171 UT-FAIL
- 172 VCG-DEG
 - ◆ 172.1 Clear the VCG-DEG Condition

- 173 VCG-DOWN
 - ◆ 173.1 Clear the VCG-DOWN Condition
- 174 VOA-HDEG
- 175 VOA-HFAIL
- 176 VOA-LDEG
- 177 VOA-LFAIL
- 178 VOLT-MISM
 - ◆ 178.1 Clear the VOLT-MISM Condition
- 179 VT-SQUELCH-L
- 180 WKSWPR
 - ◆ 180.1 Clear the WKSWPR Condition
- 181 WORK-QUEUE-FULL
- 182 WTR
 - ◆ 182.1 Clear the WTR Condition on an IEEE 802.17b-Based RPR Span
- 183 WVL-MISMATCH
- 184 Traffic Card LED Activity
 - ◆ 184.1 Typical Traffic Card LED Activity After Insertion
 - ◆ 184.2 Typical Traffic Card LED Activity During Reset
 - ◆ 184.3 Typical Card LED State After Successful Reset
 - ◆ 184.4 Typical Cross-Connect LED Activity During Side Switch
- 185 Frequently Used Alarm Troubleshooting Procedures
 - ◆ 185.1 Node and Ring Identification, Change, Visibility, and Termination
 - ◇ 185.1.1 Identify a BLSR Ring Name or Node ID Number
 - ◇ 185.1.2 Change a BLSR Ring Name
 - ◇ 185.1.3 Change a BLSR Node ID Number
 - ◇ 185.1.4 Verify Node Visibility for Other Nodes
 - ◆ 185.2 Protection Switching, Lock Initiation, and Clearing
 - ◇ 185.2.1 Initiate a 1+1 Force Switch Command
 - ◇ 185.2.2 Initiate a 1+1 Manual Switch Command
 - ◇ 185.2.3 Clear a 1+1 Force or Manual Switch Command
 - ◇ 185.2.4 Initiate a Lock-On Command
 - ◇ 185.2.5 Initiate a Card or Port Lockout Command
 - ◇ 185.2.6 Clear a Lock-On or Lockout Command
 - ◇ 185.2.7 Initiate a 1:1 Card Switch Command
 - ◇ 185.2.8 Initiate a Force Switch for All Circuits on a Path Protection Span
 - ◇ 185.2.9 Initiate a Manual Switch for All Circuits on a Path Protection Span
 - ◇ 185.2.10 Initiate a Lockout for All Circuits on a Protect Path Protection Span
 - ◇ 185.2.11 Clear an External Switching Command on a Path Protection Span
 - ◇ 185.2.12 Initiate a Force Ring Switch on a BLSR
 - ◇ 185.2.13 Initiate a Force Span Switch on a Four-Fiber BLSR
 - ◇ 185.2.14 Initiate a Manual Span Switch on a BLSR
 - ◇ 185.2.15 Initiate a Manual Ring Switch on a BLSR
 - ◇ 185.2.16 Initiate a Lockout on a BLSR Protect Span

- ◇ [185.2.17 Initiate an Exercise Ring Switch on a BLSR](#)
- ◇ [185.2.18 Initiate an Exercise Ring Switch on a Four Fiber BLSR](#)
- ◇ [185.2.19 Clear a BLSR External Switching Command](#)
- ◆ [185.3 CTC Card Resetting and Switching](#)
 - ◇ [185.3.1 Reset a Traffic Card in CTC](#)
 - ◇ [185.3.2 Reset an Active TCC2/TCC2P Card and Activate the Standby Card](#)
 - ◇ [185.3.3 Side Switch the Active and Standby Cross-Connect Cards](#)
- ◆ [185.4 Physical Card Reseating, Resetting, and Replacement](#)
 - ◇ [185.4.1 Remove and Reinsert \(Reseat\) the Standby TCC2/TCC2P Card](#)
 - ◇ [185.4.2 Remove and Reinsert \(Reseat\) Any Card](#)
 - ◇ [185.4.3 Physically Replace a Traffic Card](#)
 - ◇ [185.4.4 Physically Replace an In-Service Cross-Connect Card](#)
- ◆ [185.5 Generic Signal and Circuit Procedures](#)
 - ◇ [185.5.1 Verify the Signal BER Threshold Level](#)
 - ◇ [185.5.2 Delete a Circuit](#)
 - ◇ [185.5.3 Verify or Create Node Section DCC Terminations](#)
 - ◇ [185.5.4 Clear an OC-N Card Facility or Terminal Loopback Circuit](#)
 - ◇ [185.5.5 Clear an OC-N Card Cross-Connect \(XC\) Loopback Circuit](#)
 - ◇ [185.5.6 Clear a DS3XM-6, DS3XM-12, or DS3E-12 Card Loopback Circuit](#)
 - ◇ [185.5.7 Clear Other Electrical Card or Ethernet Card Loopbacks](#)
 - ◇ [185.5.8 Clear an MXP, TXP, or FC MR-4 Card Loopback Circuit](#)
- ◆ [185.6 Air Filter and Fan Procedures](#)
 - ◇ [185.6.1 Inspect, Clean, and Replace the Reusable Air Filter](#)
 - ◇ [185.6.2 Remove and Reinsert a Fan-Tray Assembly](#)
 - ◇ [185.6.3 Replace the Fan-Tray Assembly](#)
- ◆ [185.7 Interface Procedures](#)
 - ◇ [185.7.1 Replace the Electrical Interface Assembly](#)
 - ◇ [185.7.2 Replace the Alarm Interface Panel](#)

MAN-REQ

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)
SONET Logical Objects: EQPT, ML1000, ML100T, MLFX, STSMON, VT-MON

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

MAN-REQ is raised for an IEEE 802.17b-based RPR span if the manual switch was requested in the Cisco IOS CLI with the "rpr-ieee protection request manual-switch {east | west}" command. It clears from the IEEE 802.17b-based RPR span when you remove the switch in the CLI. For the RPR-IEEE, MAN-REQ suppresses the "RPR-SD" alarm, and the "WTR" alarm. This condition is suppressed by the following

alarms:

- FORCED-REQ
- RPR-PASSTHR
- RPR-SF

Clear the MAN-REQ Condition

1. If the condition is raised against a SONET entity, complete the Initiate a 1+1 Manual Switch Command.
2. If the condition is raised on an IEEE 802.17b-based RPR span, enter the following CLI command in RPR-IEEE interface configuration mode:

```
router(config-if)#no rpr-ieee protection request manual-switch  
{east | west}
```

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.

MANRESET

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

A User-Initiated Manual Reset condition occurs when you right-click a card in CTC and choose Reset.

Note: MANRESET is an informational condition and does not require troubleshooting.

MANSWTOINT

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

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

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

MANSWTOPRI

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

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

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

MANSWTOSEC

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

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

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

MANSWTOSECOND

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

The Manual Switch To Third Reference condition occurs when the NE timing source is manually switched to a third timing source.

Note: MANSWTOSECOND is an informational condition and does not require troubleshooting.

MANSWTOSECOND

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

The Manual Switch Request on Ring condition occurs when a user initiates a MANUAL RING command on BLSR rings to switch from working to protect or protect to working. This condition is visible on the network view Alarms, Conditions, and History tabs and is accompanied by WKSWPR. The port where the MANUAL RING command originated is marked with an "M" on the network view detailed circuit map.

Clear the MANUAL-REQ-RING Condition

1. Complete the [Clear a BLSR External Switching Command](#).
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.

MANUAL-REQ-RING

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)
SONET Logical Object: EC1, OCN
DWDM Logical Objects: 2R, ESCON, FC, GE, ISC, TRUNK

The Manual Switch Request on Ring condition occurs on BLSRs when a user initiates a Manual Span command to move BLSR traffic from a working span to a protect span. This condition appears on the network view Alarms, Conditions, and History tabs. The port where the MANUAL SPAN command was applied is marked with an "M" on the network view detailed circuit map.

Clear the MANUAL-REQ-SPAN Condition

1. Complete the [Clear a BLSR External Switching Command](#).
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.

MANUAL-REQ-SPAN

Default Severity: Major (MJ), Service-Affecting (SA)
SONET Logical Object: RPRIF

The Maximum IEEE 802.17b-based RPR Station Number Exceeded alarm can be raised by all ML card stations on a ring when the maximum quantity of stations, 255, is exceeded. This excess causes the IEEE 802.17b-based RPR scheme-and traffic-to break down.

IEEE 802.17b-based RPR messaging uses time-to-live (TTL), an 8-bit value. The maximum value these 8 bits (one byte) can have is 255. As a message travels (or hops) from station to station, the TTL is decremented by each station. Thus one station cannot communicate with another station more than 255 hops away.

If you are creating a large ring (more than 127 nodes), the MAX-STATIONS alarm might be raised until the ring is closed and stable.

MAX-STATIONS does not suppress any other alarms. However, this alarm is suppressed by the "RPR-PASSTHR" alarm.

Clear the MAX-STATIONS Alarm

1. Remove the extra stations from the ring to clear this alarm in all other stations and to restore traffic in the ring. For procedures to add or remove IEEE 802.17b-based RPR stations, refer to the *Cisco ONS 15454 and Cisco ONS 15454 SDH Ethernet Card Software Feature and Configuration Guide*.
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.

MEA (AIP)

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

If the Mismatch of Equipment Attributes (MEA) alarm is reported against the AIP, the fuse in the AIP board blew or is missing. The MEA alarm also occurs when an old AIP board with a 2-A fuse is installed in a newer ANSI 10-Gbps-compatible shelf assembly (15454-SA-ANSI or 15454-SA-HD).

Clear the MEA (AIP) Alarm

1. Complete the [Replace the Alarm Interface Panel](#).
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.

MEA (BIC)

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

The Missing Equipment Attributes alarm for the backplane interface connector (BIC) indicates a compatibility issue in using high-density DS-3 cards with universal backplane interface connectors (UBIC) and an older shelf backplane. The backplane on the high-density shelf assembly, 15454-SA-HD, is compatible with the UBIC with horizontal connectors (UBIC-H) and UBIC with vertical connectors (UBIC-V) that the high-density EC-1, DS-1, and DS-3 electrical connections require. The MEA alarm is raised if you attempt to install a high-density card in Slot 4, 5, 6, 12, 13, or 14 in a shelf assembly with an older, incompatible backplane. The card is not usable in this case. It is also raised if you attempt to use an older BIC (also known as electrical interface assemblies [EIAs]) with the newer shelf assembly.

Clear the MEA (BIC) Alarm

1. Click the Provisioning > Inventory tabs to determine your backplane model. If the backplane is not a 15454-SA-HD, replace the backplane or do not attempt to use high-density DS-3 cards. [Table 2-18](#) lists the BICs that are compatible with various backplanes.

Table 2-18: BIC Compatibility Matrix

BIC Type	Part No.
BICs that work with the newer and older backplanes	MANUF_EQPT_ID_BIC_A_SMB_HD_BP
	MANUF_EQPT_ID_BIC_B_SMB_HD_BP
	MANUF_EQPT_ID_BIC_A_BNC_24_HD_BP
	MANUF_EQPT_ID_BIC_A_BNC_48_HD_BP
	MANUF_EQPT_ID_BIC_B_SMB
	MANUF_EQPT_ID_BIC_B_SMB_ALT
	MANUF_EQPT_ID_BIC_B_BNC_24
New HD BICs that work only with the new backplanes	MANUF_EQPT_ID_BIC_B_BNC_48
	MANUF_EQPT_ID_BIC_A_UNIV_VERT
	MANUF_EQPT_ID_BIC_B_UNIV_VERT
	MANUF_EQPT_ID_BIC_A_UNIV_HORIZ
	MANUF_EQPT_ID_BIC_B_UNIV_HORIZ
	MANUF_EQPT_ID_BIC_A_MINI_BNC_HD_BP
High-density BICs that work only with 15454-SA-HD	MANUF_EQPT_ID_BIC_B_MINI_BNC_HD_BP
	MANUF_EQPT_ID_BIC_A_SMB
	MANUF_EQPT_ID_BIC_A_SMB_ALT
	MANUF_EQPT_ID_BIC_A_BNC_24
	MANUF_EQPT_ID_BIC_A_BNC_48

2. If you determine that your BIC type and backplane are compatible despite the MEA alarm, or if the alarm does not clear after you resolve the incompatibilities, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.

MEA (EQPT)

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

The MEA alarm for equipment is reported against a card slot when the physical card inserted into a slot does not match the card type that is provisioned for that slot in CTC. The alarm also occurs when certain cards introduced in Release 3.1 or later are inserted into an older shelf assembly or when older Ethernet cards (E1000-2 and E100T-12) are used in a newer 10-Gbps-compatible shelf assembly.

Removing the incompatible cards clears the alarm.

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

Note: If an OC3-8 card is installed in Slot 5 to 6 and Slot 12 to 13, it does not appear in CTC and raises an MEA.

Clear the MEA (EQPT) Alarm

1. Physically verify the type of card that is installed in the slot reporting the MEA alarm. In node view, click the **Inventory** tab and compare it to the actual installed card.
2. Determine whether the ONS 15454 shelf assembly is a newer 10-Gbps-compatible shelf assembly (15454-SA-ANSI or 15454-SA-HD) or an earlier shelf assembly. Under the HW Part # column, if the part number is 800-19857-XX or 800-19856-XX, then you have a 15454-SA-ANSI shelf. If the part number is 800-24848-XX, then you have a 15454-SA-HD shelf. If the number is not one of those listed above, then you are using an earlier shelf assembly.

Note: On the 15454-SA-HD (P/N: 800-24848), 15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1 (P/N: 800-07149) shelves, the AIP cover is clear plastic. On the 15454-SA-ANSI shelf (P/N: 800-19857), the AIP cover is metal.
3. Verify the type of card that sits in the slot reported in the object column of the MEA row on the Alarms window by reading the name at the top of the card faceplate.
 - ◇ If you have a newer 10-Gbps-compatible shelf assembly (15454-SA-ANSI or 15454-SA-HD) and the card reporting the alarm is not an E1000-2 or E100T-12, proceed to Step 4.
 - ◇ If you have a newer 10-Gbps-compatible shelf assembly (15454-SA-ANSI or 15454-SA-HD) and the card reporting the alarm is an E1000-2 or E100T-12, then that version of the Ethernet card is incompatible and must be removed. Proceed to Step 4.

Note: The E1000-2-G and E100T-G cards are compatible with the newer ANSI 10-Gbps-compatible shelf assembly and are the functional equivalent of the older, noncompatible E1000-2 and E100T-12 cards. E1000-2-G and E100T-G cards can be used as replacements for E1000-2 and E100T-12 cards in a 10-Gbps-compatible shelf assembly.
 - ◇ If you have an older shelf assembly and the card reporting the alarm is not a card introduced in Release 3.1 or later, which includes the OC-192, E1000-2-G, E100T-G, or OC-48 any slot (AS), proceed to Step 4.
 - ◇ If you have an older shelf assembly and the card reporting the alarm is a card introduced in Release 3.1 or later, which includes the OC-192, E1000-2-G, E100T-G, or OC-48 any slot (AS), the reporting card is incompatible with the shelf assembly and must be removed. Proceed to Step 4.
4. If you prefer the card type depicted by CTC, complete the [Physically Replace a Traffic Card](#) for the reporting card.
5. If you prefer the card that physically occupies the slot but the card is not in service, does not have circuits mapped to it, and is not part of a protection group, place the cursor over the provisioned card in CTC and right-click to choose **Delete Card**.

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

Note: If the card is in service, does have circuits mapped to it, is paired in a working protection scheme, has DCC communications turned on, or is used as a timing reference, CTC does not allow you to delete the card.

6. If any ports on the card are in service, place them out of service (OOS,MT): **Caution!** Before placing ports out of service, ensure that live traffic is not present.
 1. Double-click the reporting card to open the card view.
 2. Click the **Provisioning** tab.
 3. Click the admin state of any in-service ports.
 4. Choose OOS,MT to take the ports out of service.
7. If a circuit has been mapped to the card, complete the Delete a Circuit. **Caution!** Before deleting the circuit, ensure that live traffic is not present.
8. If the card is paired in a protection scheme, delete the protection group:
 1. Click the **Provisioning > Protection** tabs.
 2. Choose the protection group of the reporting card.
 3. Click **Delete**.
9. Right-click the card reporting the alarm.
10. Choose **Delete**.

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

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

MEA (FAN)

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

The MEA alarm is reported against the fan-tray assembly when a newer fan-tray assembly (15454-FTA3) with a 5-A fuse is used with an older shelf assembly or when an older fan-tray assembly with a 2-A fuse is used with a newer 10-Gbps-compatible shelf assembly (15454-SA-ANSI or 15454-SA-HD) that contains cards introduced in Release 3.1 or later. If a 10-Gbps-compatible shelf assembly contains only cards introduced before Release 3.1, then an older fan-tray assembly (15454-FTA-2) can be used and does not report an MEA alarm.

Clear the MEA (FAN) Alarm

1. Determine whether the shelf assembly is a newer 10-Gbps-compatible shelf assembly (15454-SA-ANSI or 15454-SA-HD) or an earlier shelf assembly. In node view, click the **Inventory** tab.

Under the HW Part # column, if the part number is 800-19857-XX or 800-19856-XX, then you have a 15454-SA-ANSI shelf. If the part number is 800-24848-XX, you have a 15454-SA-HD shelf.

Under the HW Part # column, if the number is not one of those listed above, then you are using an earlier shelf assembly.
2. If you have a 10-Gbps-compatible shelf assembly (15454-SA-ANSI or 15454-SA-HD), the alarm indicates that an older incompatible fan-tray assembly is installed in the shelf assembly. Obtain a newer fan-tray assembly (15454-FTA3) with a 5-A fuse and complete the Replace the Fan-Tray Assembly.

ONS_15454_Troubleshooting_Guide_R8.5.x_--_Alarm_Troubleshooting_(M_through_W)

3. If you are using an earlier shelf assembly, the alarm indicates that you are using a newer fan-tray assembly (15454-FTA3), which is incompatible with the earlier version of the shelf assembly. Obtain an earlier version of the fan-tray assembly (15454-FTA2) and complete the [Replace the Fan-Tray Assembly](#).
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.

MEA (PPM)

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

MEA (SHELF)

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

MEM-GONE

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

The Memory Gone alarm occurs when data generated by software operations exceeds the memory capacity of the TCC2/TCC2P. CTC does not function properly until the alarm clears. The alarm clears when additional memory becomes available.

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

MEM-LOW

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

The Free Memory of Card Almost Gone alarm occurs when data generated by software operations is close to exceeding the memory capacity of the TCC2/TCC2P. The alarm clears when additional memory becomes available. If additional memory is not made available and the memory capacity of the card is exceeded, CTC ceases to function.

Note: The 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.

MFGMEM

Default Severity: Critical (CR), Service-Affecting (SA)
SONET Logical Objects: AICI-AEP, AICI-AIE, AIP, BPLANE, FAN
DWDM Logical Object: PPM

The Manufacturing Data Memory Failure alarm occurs when the EEPROM fails on a card or component, or when the TCC2/TCC2P cannot read this memory. EEPROM stores manufacturing data that a system TCC2/TCC2P uses to determine system compatibility and shelf inventory status. Unavailability of this information can cause less-significant problems. The AIP EEPROM also stores the system MAC address. If the MFGMEM alarm indicates EEPROM failure on these panels, IP connectivity could be disrupted and the system icon is grayed out in CTC network view.

Tip: When you lose LAN connectivity with an ONS 15454 due to an MFGMEM alarm on the AIP, you can reestablish node management by disconnecting the Ethernet cable from the panel and connecting it to the active TCC2/TCC2P LAN port.

Clear the MFGMEM Alarm

1. Complete the Reset an Active TCC2/TCC2P Card and Activate the Standby Card.
Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.
2. If the reset card has not rebooted successfully, or the alarm has not cleared, call Cisco TAC 1 800 553-2447. If the Cisco TAC technician tells you to reseat the card, complete the Remove and Reinsert (Reseat) the Standby TCC2/TCC2P Card. If the Cisco TAC technician tells you to remove the card and reinstall a new one, complete the Physically Replace a Traffic Card.
3. If the MFGMEM alarm continues to report after replacing the TCC2/TCC2Ps, the problem lies with the EEPROM.
4. If the MFGMEM is reported from the fan-tray assembly, obtain a fan-tray assembly and complete the Replace the Fan-Tray Assembly.
5. If the MFGMEM is reported from the AIP, the backplane, or the alarm persists after the fan-tray assembly is replaced, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 to report a Service-Affecting (SA) problem.

MS-DEG

The MS-DEG condition is not used in this platform in this release. It is reserved for development.

MS-EXC

The MS-EXC condition is not used in this platform in this release. It is reserved for development.

MT-OCHNC

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

NO-CONFIG

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

The No Startup Configuration condition applies to ML-Series Ethernet cards and occurs when no startup configuration file has been downloaded to the TCC2/TCC2P, whether or not you preprovision the card slot. This alarm can be expected during provisioning. When the startup configuration file is copied to the active TCC2/TCC2P, the alarm clears.

Note: For more information about the ML-Series Ethernet cards, refer to the *Cisco ONS 15454 and Cisco ONS 15454 SDH Ethernet Card Software Feature and Configuration Guide*.

Clear the NO-CONFIG Condition

1. Create a startup configuration for the card in Cisco IOS.
Follow the card provisioning instructions in the *Cisco ONS 15454 and Cisco ONS 15454 SDH Ethernet Card Software Feature and Configuration Guide*.
2. Upload the configuration file to the TCC2/TCC2P:
 1. In node view, right-click the ML-Series card graphic.
 2. Choose **IOS Startup Config** from the shortcut menu.
 3. Click **Local > TCC** and navigate to the file location.
3. Complete the Reset a Traffic Card in CTC.
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.

NON-CISCO-PPM

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)
SONET Logical Object: PPM

The Non-Cisco PPM Inserted condition occurs when a PPM that is plugged into a card's port fails the security code check. The check fails when the PPM used is not a Cisco PPM.

Clear the NON-CISCO-PPM Condition

1. Obtain the correct Cisco PPM and replace the existing PPM with the new one.
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.

NOT-AUTHENTICATED

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

The NOT-AUTHENTICATED alarm is raised by CTC (not by the NE) when CTC fails to log into a node. This alarm only appears in CTC where the login failure occurred. This alarm differs from the "INTRUSION-PSWD" alarm because INTRUSION-PSWD occurs when a user exceeds the login failures threshold.

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

OCHNC-INC

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

OCHTERM-INC

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

ODUK-1-AIS-PM

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

ODUK-2-AIS-PM

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

ODUK-3-AIS-PM

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

ODUK-4-AIS-PM

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

ODUK-AIS-PM

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

ODUK-BDI-PM

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

ODUK-LCK-PM

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

ODUK-OCI-PM

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

ODUK-SD-PM

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

ODUK-SF-PM

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

ODUK-TIM-PM

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

OOU-TPT

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

The Out of Use Transport Failure alarm is a VCAT member alarm. (VCAT member circuits are independent circuits that are concatenated from different time slots into a higher-rate signal.) This condition is raised when a member circuit in a VCAT is unused, such as when it is removed by SW-LCAS. It occurs in conjunction with the "VCG-DEG" condition.

Clear the OOT-TPT Condition

1. Complete the Clear the VCG-DEG Condition. Clearing that condition clears this condition as well.
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.

OPEN-SLOT

Default Severity: Not Alarmed (NA)
Logical Object: EQPT

The Open Slot condition indicates that there is an open slot in the system shelf. Slot covers assist with airflow and cooling.

Clear the OPEN-SLOT Condition

1. To install a slot cover and clear this condition, refer to the procedures located in the "Install Cards and Fiber-Optic Cable" chapter of the *Cisco ONS 15454 Procedure Guide*.
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.

OPTNTWMIS

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

OPWR-HDEG

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

OPWR-HFAIL

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

OPWR-LDEG

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

OPWR-LFAIL

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

OSRION

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

OTUK-AIS

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

OTUK-BDI

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

OTUK-IAE

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

OTUK-LOF

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

OTUK-SD

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

OTUK-SF

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

OTUK-TIM

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

OUT-OF-SYNC

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

PARAM-MISM

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

PDI-P

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)
SONET Logical Objects: STSMON, STSTRM

PDI-P is a set of application-specific codes indicating a signal label mismatch failure (SLMF) in the ONS 15454 STS path overhead. The condition indicates to downstream equipment that there is a defect in one or more of the directly mapped payloads contained in that STS synchronous payload envelope (SPE). For example, the mismatch could occur in the overhead to the path selector in a downstream node configured as part of a path protection. The PDI-P codes appear in the STS Signal Label (C2 byte).

An SLMF often occurs when the payload (for example, ATM) does not match what the signal label is reporting. The "AIS" condition often accompanies a PDI-P condition. If the PDI-P is the only condition reported with the AIS, clearing PDI-P clears the AIS. PDI-P can also occur during an upgrade, but usually clears itself and is not a valid condition.

A PDI-P condition reported on an OC-N port supporting a G1000-4 card circuit could result from the end-to-end Ethernet link integrity feature of the G1000-4 card. If the link integrity is the cause of the path defect, it is typically accompanied by the "TPTFAIL (G1000)" alarm or the "CARLOSS (G1000)" alarm reported against one or both Ethernet ports terminating the circuit. If this is the case, clear the TPTFAIL and CARLOSS alarms to resolve the PDI-P condition.

A PDI-P condition reported on an OC-N port supporting an ML-Series card circuit could result from the end-to-end Ethernet link integrity feature of the ML-Series card. If the link integrity is the cause, it is typically accompanied by the "TPTFAIL (ML100T, ML1000, MLFX)" alarm reported against one or both POS ports terminating the circuit. If TPTFAIL is reported against one or both of the POS ports, troubleshooting the accompanying alarm clears the PDI-P condition. Refer to the *Cisco ONS 15454 and Cisco ONS 15454 SDH Ethernet Card Software Feature and Configuration Guide* for more information about ML-Series cards.

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

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

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

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

Clear the PDI-P Condition

1. Verify that all circuits terminating in the reporting card are DISCOVERED:
 1. Click the **Circuits** tab.
 2. Verify that the **Status** column lists the circuit as active.
 3. If the Status column lists the circuit as PARTIAL, wait 10 minutes for the ONS 15454 to initialize fully. If the PARTIAL status does not change after full initialization, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC to report a Service-Affecting (SA) problem 1 800 553-2447.
2. After determining that the circuit is DISCOVERED, ensure that the signal source to the card reporting the alarm is working.

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

3. If traffic is affected, complete the [Delete a Circuit](#).

Caution! Deleting a circuit can affect existing traffic.

4. Recreate the circuit with the correct circuit size. Refer to the "Create Circuits and VT Tunnels" chapter in the *Cisco ONS 15454 Procedure Guide* for detailed procedures to create circuits.
5. If circuit deletion and re-creation does not clear the condition, verify that there is no problem stemming from the far-end OC-N card providing STS payload to the reporting card.
6. If the condition does not clear, confirm the cross-connect between the OC-N card and the reporting card.
7. If the condition does not clear, clean the far-end optical fiber according to site practice. If no site practice exists, complete the procedure in the "Maintain the Node" chapter of the *Cisco ONS 15454 Procedure Guide*.
8. If the condition does not clear, complete the [Physically Replace a Traffic Card](#) for the optical/electrical cards.
9. If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

PEER-NORESPONSE

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

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

However, for ML-MR-10 cards, a peer card not responding alarm is raised if a CPP card that is active does not receive any heartbeat response from its peer card. This happens under the following conditions:

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

Clear the PEER-NORESPONSE Alarm

1. Complete the [Reset a Traffic Card in CTC](#) for the reporting card. For the LED behavior, see the [Typical Traffic Card LED Activity During Reset](#).
2. Verify that the reset is complete and error-free and that no new related alarms appear in CTC. Verify the LED appearance: A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
3. For ML-MR-10 card, ensure that the CPP peer card has not failed, the correct protection configuration is present on both CPP cards, and protection is not disabled on the CPP peer card.
4. If the alarm does not clear, log into the Cisco Technical Support Website at <http://www.cisco.com/techsupport> for more information or log into <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml> to obtain a directory of toll-free Technical Support numbers for your country.

PLM-P

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

A Payload Label Mismatch Path alarm indicates that signal does not match its label. The condition is indicated by a problematic C2 byte value in the SONET path overhead. The alarm is raised if all of the following conditions are met:

- The received C2 byte is not 0x00 (unequipped).
- The received C2 byte is not a PDI value.
- The received C2 does not match the expected C2.
- The expected C2 byte is not 0x01 (equipped, unspecified).
- The received C2 byte is not 0x01 (equipped, unspecified).

For example, on nodes equipped with CTC Software R4.1 and earlier, this alarm could occur when you have a DS3XM-6 card connected to a DS-3 card instead of a DS-1 card. The DS3XM-6 card expects a C2 label byte value of 01. A DS-1 card transmits this value, but a DS-3 card transmits a value of 04. The mismatch between the sent and expected values causes the PLM-P alarm.

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

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

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

Clear the PLM-P Alarm

1. Complete the [Clear the PDI-P Condition](#).

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

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.

PLM-V

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

SONET Logical Object: VT-TERM, VT-MON

A Payload Label Mismatch VT Layer alarm indicates that the content of the V5 byte in the SONET overhead is inconsistent or invalid. PLM-V occurs when ONS 15454s interoperate with equipment that performs bit-synchronous mapping for DS-1 signal. The ONS 15454 uses asynchronous mapping.

Clear the PLM-V Alarm

1. Verify that your signal source matches the signal allowed by the traffic card. For example, the traffic card does not allow VT6 or VT9 mapping.
2. If the signal source matches the card, verify that the SONET VT path originator is sending the correct VT label value. You can find the SONET VT path originator using circuit provisioning steps.
3. If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.

PMI

For more information about the PMI condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*.

PORT-FAIL

For more information about the PORT-FAIL alarm, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*.

PORT-MISMATCH

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

SONET Logical Object: CEMR, FCMR

The Pluggable Port Mismatch alarm applies to FC_MR-4, ML-MR-10, CE-MR-10 Ethernet card, and TXP card SFP connectors. The alarm indicates that the provisioned payload for the connector does not match the SFP configuration.

The error must be resolved in the Cisco IOS configuration. PORT-MISMATCH cannot be resolved in CTC. For information about provisioning the ML-Series and CE-MR-10 Ethernet cards from the Cisco IOS interface, refer to the *Cisco ONS 15454 and Cisco ONS 15454 SDH Ethernet Card Software Feature and Configuration Guide*.

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

PRC-DUPID

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

The Procedural Error Duplicate Node ID alarm indicates that two identical node IDs exist in the same ring. The ONS 15454 requires each node in the ring to have a unique node ID.

Clear the PRC-DUPID Alarm

1. Log into a node on the ring.
2. Find the node ID by completing the Identify a BLSR Ring Name or Node ID Number.
3. Repeat Step 2 for all the nodes on the ring.
4. If two nodes have an identical node ID number, complete the Change a BLSR Node ID Number so that each node ID is unique.
5. If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.

PROTNA

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

The Protection Unit Not Available alarm is caused by an OOS protection card when a TCC2/TCC2P or XC10G card that has been provisioned as part of a protection group is not available. Unavailable protection can occur when a card is reset, but the alarm clears as soon as the card is back in service. The alarm clears if the device or facility is brought back in service.

Clear the PROTNA Alarm

1. If the PROTNA alarm occurs and does not clear, and if it is raised against a controller or cross-connect card, ensure that there is a redundant TCC2/TCC2P installed and provisioned in the chassis.
2. If the alarm is raised against a line card, verify that the ports have been taken out of service (OOS,MT):
 1. In CTC, double-click the reporting card to open the card view (if the card is not an XC10G card).
 2. Click the **Provisioning** tab.
 3. Click the admin state of any in-service (IS) ports.
 4. Choose OOS,MT to take the ports out of service.
3. Complete the Reset a Traffic Card in CTC for the reporting card. For the LED behavior, see the Typical Traffic Card LED Activity During Reset.
4. Verify that the reset is complete and error-free and that no new related alarms appear in CTC. Verify the LED appearance: A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
5. If the alarm does not clear, complete the Remove and Reinsert (Reseat) Any Card for the reporting card.
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.

PROV-MISMATCH

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

PTIM

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

PWR-FAIL-A

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

The Equipment Power Failure at Connector A alarm occurs when there is no power supply from the main power connector to the equipment. This alarm occurs on the electrical interface assemblies (EIA), cross-connect card, OC-N cards, or TCC2/TCC2P.

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

Clear the PWR-FAIL-A Alarm

1. If a single card has reported the alarm, take the following actions depending on the reporting card:

If the reporting card is an active traffic line port in a 1+1 protection group or part of a path protection, ensure that an APS traffic switch has occurred to move traffic to the protect port. **Note:** Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the Protection Switching, Lock Initiation, and Clearing for commonly used traffic-switching procedures.

- If the alarm is reported against a TCC2/TCC2P, complete the Reset an Active TCC2/TCC2P Card and Activate the Standby Card.
 - If the alarm is reported against an OC-N card, complete the Reset a Traffic Card in CTC.
 - If the alarm is reported against a cross-connect card, complete the Reset a Traffic Card in CTC for the cross-connect card. (The process is similar.)
2. If the alarm does not clear, complete the Remove and Reinsert (Reseat) Any Card.
 3. If the alarm does not clear, complete the Physically Replace a Traffic Card for the *reporting* card.
 4. If the single card replacement does not clear the alarm, or if multiple cards report the alarm, verify the office power. Refer to the "Install the Shelf and Backplane Cable" chapter in the *Cisco ONS 15454 Procedure Guide* for procedures. See the Power Supply Problems as necessary.
 5. If the alarm does not clear, reseat the power cable connection to the connector.
 6. If the alarm does not clear, physically replace the power cable connection to the connector.
 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.

PWR-FAIL-B

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

The Equipment Power Failure at Connector B alarm occurs when there is no power supply from the main power connector to the equipment. This alarm occurs on the electrical interface assemblies (EIA), cross-connect card, OC-N cards, or TCC2/TCC2P.

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

Clear the PWR-FAIL-B Alarm

1. Complete the [Clear the PWR-FAIL-A Alarm](#).
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.

PWR-FAIL-RET-A

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

The Equipment Power Failure at Connector A alarm occurs when there is no power supplied to the backup power connector on the shelf. This alarm occurs on the EIA, cross-connect card, OC-N cards, or TCC2/TCC2P.

Clear the PWR-FAIL-RET-A Alarm

1. Complete the [Clear the PWR-FAIL-A Alarm](#).
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.

PWR-FAIL-RET-B

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

The Equipment Power Failure at Connector B alarm occurs when there is no power supplied to the backup power connector on the shelf. This alarm occurs on the EIA, cross-connect card, OC-N cards, or TCC2/TCC2P.

Clear the PWR-FAIL-RET-A Alarm

1. Complete the [Clear the PWR-FAIL-A Alarm](#).
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.

RAI

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)
SONET Logical Objects: DS1, DS3, E1

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

Clear the RAI Condition

1. Complete the Clear the AIS Condition.
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.

RCVR-MISS

Default Severity: Major (MJ), Service-Affecting (SA)
SONET Logical Objects: DS1, E1

A Facility Termination Equipment Receiver Missing alarm occurs when the facility termination equipment detects an incorrect amount of impedance on its backplane connector. Incorrect impedance usually occurs when a receive cable is missing from a DS-1 port, or a possible mismatch of backplane equipment occurs. For example, an SMB connector or a BNC connector could be misconnected to a DS-1 card.

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

Clear the RCVR-MISS Alarm

1. Ensure that the device attached to the DS-1 port is operational.

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

2. If the attachment is good, verify that the cabling is securely connected.
3. If the cabling is good, verify that the pinouts are correct.
4. If the pinouts are correct, replace the receive cable.
5. If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a service-affecting (SA) problem.

RSV-RT-EXCD-RINGLETO

Default Severity: Major (MJ), Service-Affecting (SA)
SONET Logical Object: RPRIF

The Reserved Bandwidth Exceeds Link Rate on Ringlet Zero alarm is raised by an ML-1000 card if the sum of the reserved bandwidth configured on each station of ringlet 0 is greater than the link rate (circuit bandwidth). The alarm clears when the sum of the reserved bandwidth on each station falls below the link rate. In the case of SW-LCAS or LCAS circuits, the link rate is the working link rate, which will change when members are removed.

RSV-RT-EXCD-RINGLET0 does not suppress any alarms, but it is suppressed by the "RPR-PASSTHR" alarm.

Clear the RSV-RT-EXCD-RINGLET0 Alarm

1. At the CLI command prompt in privileged executive mode, enter the following command:

```
router# show rpr-ieee topology detail
```

This command's output shows the configured reserved bandwidth rate from each station.

2. Reduce the reserved bandwidth on the alarmed station until the error clears. Enter the following CLI command in IEEE 802.17b-based RPR interface configuration mode:

```
router (config-if)# rpr-ieee tx-traffic rate-limit reserved
```

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

RSV-RT-EXCD-RINGLET1

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

SONET Logical Object: RPRIF

The Reserved Bandwidth Exceeds Link Rate on Ringlet One alarm is raised by an ML-1000 card if the sum of reserved bandwidth configured on each station of ringlet 1 is greater than the link rate (circuit bandwidth). The alarm clears when the sum of the reserved bandwidth on each station falls below the link rate. In the case of SW-LCAS or LCAS circuits, the link rate is the working link rate, which will change when members are removed

RSV-RT-EXCD-RINGLET1 does not suppress any alarms, but it is suppressed by the "RPR-PASSTHR" alarm.

Clear the RSV-RT-EXCD-RINGLET1 Alarm

1. At the CLI command prompt in privileged executive mode, enter the following command:

```
router# show rpr-ieee topology detail
```

This command's output shows the configured reserved bandwidth rate from each station.

2. Reduce the reserved bandwidth on the alarmed station until the error clears. Enter the following CLI command in IEEE 802.17b-based RPR interface configuration mode:

```
router (config-if)# rpr-ieee tx-traffic rate-limit reserved
```

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

RFI

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

RFI-L

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)
SONET Logical Objects: EC1, OCN
DWDM Logical Object: TRUNK

A RFI Line condition occurs when the ONS 15454 detects an RFI in OC-N card SONET overhead because of a fault in another node. Resolving the fault in the adjoining node clears the RFI-L condition in the reporting node. RFI-L indicates that the condition is occurring at the line level.

Clear the RFI-L Condition

1. Log into the node at the far-end node of the reporting ONS 15454.
2. Identify and clear any alarms, particularly the "LOS (OCN)" alarm.
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.

RFI-P

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

The RFI Path condition occurs when the ONS 15454 detects an RFI in the an STS-1 signal SONET overhead because of a fault in another node. Resolving the fault in the adjoining node clears the RFI-P condition in the reporting node. RFI-P occurs in the terminating node in that path segment.

Clear the RFI-P Condition

1. Verify that the ports are enabled and in service (IS-NR) on the reporting ONS 15454:
 1. Confirm that the LED is correctly illuminated on the physical card.
A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
 2. To determine whether the OC-N port is in service, double-click the card in CTC to open the card view.
 3. Click the **Provisioning > Line** tabs.
 4. Verify that the Admin State column lists the port as IS.
 5. If the Admin State column lists the port as OOS,MT or OOS,DSBLD, click the column and choose IS. Click **Apply**.
Note: If ports managed into IS admin state are not receiving signals, the LOS alarm is either raised or remains, and the port service state transitions to OOS-AU,FLT.
2. To find the path and node failure, verify the integrity of the SONET STS circuit path at each of the intermediate SONET nodes.
3. Clear alarms in the node with the failure, especially the "UNEQ-P" alarm or the "UNEQ-V" alarm.
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.

RFI-V

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)
SONET Logical Objects: VTMON, VT-TERM

An RFI VT Layer condition occurs when the ONS 15454 detects an RFI in the SONET overhead because of

a fault in another node. Resolving the fault in the adjoining node clears the RFI-V condition in the reporting node. RFI-V indicates that an upstream failure has occurred at the VT layer.

Clear the RFI-V Condition

1. Verify that the connectors are securely fastened and connected to the correct slot. For more information, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 Procedure Guide*.

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

2. If connectors are correctly connected, verify that the DS-N port is active and in service (IS-NR):
 1. Confirm that the LED is correctly illuminated on the physical card. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
 2. To determine whether the OC-N port is in service, double-click the card in CTC to open the card view.
 3. Click the **Provisioning > Line** tabs.
 4. Verify that the Admin State column lists the port as IS. If the Admin State column lists the port as OOS,MT or OOS,DSBLD, click the column and choose IS. Click **Apply**.
Note: If ports managed into IS admin state are not receiving signals, the LOS alarm is either raised or remains, and the port service state transitions to OOS-AU,FLT.
3. If the ports are active and in service, use an optical test set to verify that the signal source does not have errors. For specific procedures to use the test set equipment, consult the manufacturer.
4. If the signal is valid, log into the node at the far-end of the reporting ONS 15454.
5. Clear alarms in the far-end node, especially the "UNEO-P" alarm or the "UNEO-V" alarm.
6. If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

RING-ID-MIS

Default Severity: Major (MJ), Non-Service-Affecting (NSA)
SONET Logical Object: OCN
DWDM Logical Object: OSC-RING

The Ring ID Mismatch condition refers to the ring ID in APC. It occurs when a ring name does not match other detectable node ring names, and can cause problems with applications that require data exchange with APC. This alarm is similar to the "RING-MISMATCH" alarm, but rather than apply to BLSDR ring protection, RING-ID-MIS applies to DWDM node discovery within the same network.

Note: For more information about APC, refer to the *Cisco ONS 15454 DWDM Procedure Guide*.

Clear the RING-ID-MIS Alarm

1. Complete the [Clear the RING-MISMATCH Alarm](#).
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.

RING-MISMATCH

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

A Procedural Error Mismatch Ring alarm occurs when the ring name of the ONS 15454 node that is reporting the alarm does not match the ring name of another node in the BLSR. Nodes connected in a BLSR must have identical ring names to function. This alarm can occur during BLSR provisioning.

RING-MISMATCH is somewhat similar to RING-ID-MIS, but it applies to BLSR protection discovery instead of DWDM node discovery.

Note: For more information about DWDM cards, refer to the *Cisco ONS 15454 DWDM Reference Manual*.

Clear the RING-MISMATCH Alarm

1. In node view, click the **Provisioning** > BLSR tabs.
2. Note the name in the Ring Name field.
3. Log into the next ONS 15454 node in the BLSR.
4. Complete the Identify a BLSR Ring Name or Node ID Number.
5. If the ring name matches the ring name in the reporting node, repeat Step 4 for the next ONS 15454 in the BLSR.
6. Complete the Change a BLSR Ring Name.
7. Verify that the ring map is correct.
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.

RING-SW-EAST

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

The Ring Switch Is Active East Side condition occurs when a ring switch occurs at the east side of a BLSR using a Force Ring command. The condition clears when the switch is cleared. RING-SW-EAST is visible on the network view Alarms, Conditions, and History tabs. The port where the Force Ring was applied shows an "F" on the network view detailed circuit map.

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

RING-SW-WEST

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

The Ring Switch Is Active West Side condition occurs when a ring switch occurs at the west side of a BLSR using a Force Ring command. The condition clears when the switch is cleared. RING-SW-WEST is visible on the network view Alarms, Conditions, and History tabs. The port where the Force Ring was applied shows an "F" on the network view detailed circuit map.

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

ROLL

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)
SONET Logical Objects: STSMON, STSTRM, VT-TERM, VT-MON

The ROLL condition indicates that circuits are being rolled. This is typically carried out to move traffic for a maintenance operation or to perform bandwidth grooming. The condition indicates that a good signal has been received on the roll destination leg, but the roll origination leg has not yet been dropped. The condition clears when the roll origination leg is dropped.

Note: ROLL is an informational condition and does not require troubleshooting.

ROLL-PEND

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)
SONET Logical Objects: STSMON, STSTRM, VT-TERM, VT-MON

ROLL-PEND indicates that a roll process has been started, but a good signal has not been received yet by the roll destination leg. This condition can be raised individually by each path in a bulk circuit roll.

The condition clears when a good signal has been received on the roll destination leg.

Note: ROLL-PEND is an informational condition and does not require troubleshooting.

ROUTE-OVERFLOW

Default Severity: Minor (MN), Non-Service-Affecting (NSA)
SONET Logical Objects: NE
DWDM Logical Object: NE regardless of MSTP or MSPP

The ROUTE-OVERFLOW indicates the condition when the OSPF routing table exceeds 700 routes. The symptoms for this condition are loss of visibility to a node or network, inability to access a node using CTC, CTM, Telnet, Ping, and so on.

Clear the ROUTE-OVERFLOW Condition

1. Reconfigure the OSPF network to less than 700 routes.

RPR-PASSTHR

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

The IEEE 802.17 b-based RPR Interface in Pass-Through Mode condition indicates that an ML card's IEEE 802.17 b-based RPR interface is not participating in a ring. Instead, the card is behaving like a passive device that allows the signal to transit but does not manipulate it. Pass-through mode itself is hitless.

You can manually place an ML card into (or out of) pass-through mode using the Cisco IOS CLI command SHUTDOWN (SHUT) for such reasons as adding, removing, or servicing the node. To do so is hitless.

The ML-1000 automatically enters pass-through mode if either of the following conditions is true:

- Redundant interconnect (RI) is configured and the ML card is in primary mode (that is, single traffic queue mode), standby state.
- RI is configured and the RI interface goes down during a "WTR" alarm, while the ML card is in secondary mode (that is, dual traffic queue mode) on a Cisco proprietary RPR ring.

Note: For GFP and HDLC mode, the ML card shutdown (SHUT) command causes an "AIS-P" alarm to be sent to the peer. But in IEEE 802.17b-based RPR mode, AIS-P is not inserted toward the peer.

The RPR-PASSTHR condition suppresses the following alarms:

- FORCED-REQ
- LINK-KEEPALIVE
- MAN-REQ
- MAX-STATIONS
- RSV-RT-EXCD-RINGLETO
- RSV-RT-EXCD-RINGLETI
- RPR-PROT-ACTIVE
- RPR-PROT-CONFIG-MISM
- RPR-SD
- RPR-SF
- RPR-SPAN-MISMATCH
- WTR

If RPR-PASSTHR is raised-meaning that this RPR-IEEE interface is not available-one or more of its peer nodes might raise the "RPR-PEER-MISS" alarm. RPR-PASSTHR does not suppress the "RPR-PEER-MISS" alarm, or the "RPR-RI-FAIL" alarm.

Clear the RPR-PASSTHR Condition

1. If the ML card was manually configured shut down using the CLI command SHUTDOWN (SHUT), enter the following command at the command prompt:

```
router# no shut
```

2. If the card is in pass-through mode due to being in an RI primary mode standby state, either the IEEE 802.17b-based RPR interface is down or the interconnect interface is down. You must clear the root cause of either problem to clear the pass-through. To trace the root cause problem in the RPR-IEEE interface setup, enter the following CLI command in privileged executive mode:

```
router# show interface rpr-ieee 0
```

3. View the command output and locate the RI information line. It displays the name of the monitored interfaces as "monitoring ring interface," or "monitoring interconnect interface."
4. Locate and clear any trouble on the monitored interface. Trouble might be indicated on that interface through previous alarms that occurred before RPR-PASSTHR was raised.
5. If the card is in pass-through mode while in RI secondary mode when the interconnect fails, pass-through mode should clear automatically in 60 seconds.
6. If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

RPR-PEER-MISS

Default Severity: Major (MJ), Service-Affecting (SA)
SONET Logical Object: RPRIF

The IEEE 802.17-based RPR Peer Node Is Missing condition is raised by an ML card when RI is configured on the card, but this station does not detect its peer station in the topology. The condition clears when the peers detect each other.

Clear the RPR-PEER-MISS Condition

1. Determine whether the peer MAC address is properly configured by completing the following steps:

1. Enter the following CLI command in privileged executive mode:

```
router# show interface rpr-ieee 0
```

This command's output will include information, similar to the following, about the RPR-IEEE interface raising the condition:

```
Hardware is RPR-IEEE Channelized SONET, address is
000e.8312.bcf0 (bia 000e.87312.bfc0)
```

2. Verify that the alarmed interface's configured peer MAC address is the correct MAC address for the peer card. A card in primary mode need to list the peer MAC address of the card operating in secondary mode; the secondary card needs to list the peer MAC address of the primary card. Peer MAC address information is contained in the same "show interface rpr-ieee 0" command output. In the following line example, the RPR-IEEE interface raising the alarm is primary; it is in active mode, and its configured peer, the secondary card, is MAC address 000e.8312.b870:

```
RI: primary, active peer mac 000e.8312.b870
```

Note: The primary and secondary cards do not have to be neighbors on the ring.

Note: If RI is configured, then RI information is displayed in the "show interface rpr 0" output.

To correct the MAC address configuration, refer to the *Cisco ONS 15454 and Cisco ONS 15454 SDH Ethernet Card Software Feature and Configuration Guide* for procedures.

2. If the condition does not clear, enter the following command in privileged executive mode:

```
router# show rpr-ieee protection
```

3. The command output, similar to the following lines, shows whether any protection switches are active:

```
West Span Failures: none
```

```
East Span Failures: none
```

A protection switch can cause an RPR-PEER-MISS condition. You may also see the "RPR-PROT-ACTIVE" alarm raised for a span. Clear any protection issues.

4. If the condition does not clear, correct any issues on the peer node that would cause it to go into pass-through mode, which can cause the peer to raise RPR-PEER-MISS.
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.

RPR-PROT-ACTIVE

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

The IEEE 802.17b-based RPR Protection is Active condition, raised by the ML card, indicates that ring protection is active and that steering protection as defined in IEEE 802.17b is active.

IEEE 802.17b-based RPR provides hitless protection switching for all protected traffic on a ring. Its steering protection mechanism ensures that each station receives span change information (such as fail or restoration) in time to make protection switching decisions within the 50-millisecond time frame.

The condition clears when steering protection is no longer active. For more information about steering, refer to the *Cisco ONS 15454 and Cisco ONS 15454 SDH Ethernet Card Software Feature and Configuration Guide*.

This condition is suppressed by the "RPR-PASSTHR" alarm.

Clear the RPR-PROT-ACTIVE Condition

1. Locate and clear any service-affecting SONET error that might have caused a protection switch, in turn triggering the RPR-PROT-ACTIVE condition. Clearing the SONET condition will clear RPR-PROT-ACTIVE.
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.

RPR-PROT-CONFIG-MISM

Default Severity: Major (MJ), Service-Affecting (SA)
SONET Logical Object: RPRIF

The IEEE 802.17b-based RPR Protection Configuration Mismatched alarm is raised by an ML card when it detects that its steering protection scheme is mismatched with other vendors' equipment configured for wrapping protection. The ONS 15454 does not support IEEE 802.17b's optional wrapping scheme.

The alarm clears when the other vendor's equipment configuration is changed to utilize steering protection.

RPR-PROT-CONFIG-MISM is suppressed by the "RPR-PASSTHR" alarm.

Clear the RPR-PROT-CONFIG-MISM Alarm

1. You cannot clear this alarm from the ONS 15454; rather, it is caused by incompatible vendor equipment configuration. See that equipment's support information to correct the configuration for steering instead of wrapping. This, in turn, will cause RPR-PROT-CONFIG-MISM to clear.
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.

RPR-RI-FAIL

Default Severity: Major (MJ), Service-Affecting (SA)
SONET Logical Object: RPRIF

The IEEE 802.17b-based RPR RI Fail condition is raised by an ML card in primary or secondary mode. If a card is in primary mode, a Gigabit Ethernet interface can cause an interconnect interface (IC) failure. (The IC includes the Gigabit Ethernet interface and possibly a port channel interface.) In primary mode, RPR-RI-FAIL can also be raised in response to a downed ring interface. In secondary mode, the only possible cause of this condition is IC failure.

The alarm clears when the IEEE 802.17b-based RPR interface returns to Init modes and faults, if present, are cleared. RPR-RI-FAIL is suppressed by the "RPR-PASSTHR" alarm.

Clear the RPR-RI-FAIL Condition

1. If the card is in primary mode, enter the following command at the CLI in privileged executive mode:

```
router# show interface rpr-ieee 0
```

2. The RI information line displays the name of the monitored interfaces and says either "monitoring ring interface," or "monitoring interconnect interface."
3. Determine why the monitored interface is down. It can occur because the ring interface has been shut down using the "shutdown" CLI command, or because both SONET circuits are down or OOS.
4. If correcting the previous problem on a primary interface does not clear the condition, or if the condition is raised on a card in secondary mode, the IC failure root cause must be corrected. This can be due to a fiber pull, having link protocol down, or shut down interfaces.
 - ◆ Link state is indicated in the "show interface rpr-ieee 0" output on the following line:
RPR-IEEE0 is up, line protocol is up
 - ◆ A shutdown is indicated if a node is in pass-through mode. The same command output indicates whether or not this is the case:
MAC passthrough not set
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).

RPR-SD

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)
SONET Logical Objects: ML100T, ML1000, MLFX

The IEEE 802.17b-based RPR Signal Degrade condition indicates that a minor signal degradation has occurred on an IEEE- RPR ring that, if not overridden, can deactivate the link. The RPR-SD condition is reported if the SONET "SD-P" alarm, is raised on the circuit which carries the span. The RPR-SD condition clears when the SONET signal degrade clears.

RPR-SD suppresses the "MAN-REQ" alarm and the "WTR" alarm.

It is suppressed by the following alarms:

- FORCED-REQ
- RPR-PASSTHR
- RPR-SF

Clear the RPR-SD Condition

1. Complete the Clear the SD-P Condition to clear this secondary condition.
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.

RPR-SF

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)
SONET Logical Objects: ML100T, ML1000, MLFX

The IEEE 802.17b-based RPR Signal Fail condition indicates a signal loss or major signal degradation that deactivates the RPR-IEEE link. The failure that raises RPR-SF can be attributable to any of the following alarms:

- AIS-P
- GFP-LFD
- LOP-P
- PDI-P
- PLM-P
- RFI-P
- TIM-P
- UNEQ-P
- VCG-DOWN

The RPR-SF condition can also occur if a SONET circuit's state is UNASSIGNED (not provisioned).

This condition clears when these primary cause alarms are cleared. RPR-SF is suppressed by the "RPR-PASSTHR" alarm or the "FORCED-REQ" alarm. RPR-SF itself suppresses the following alarms:

- MAN-REQ
- RPR-SD
- WTR

Clear the RPR-SF Condition

1. Complete the trouble-clearing procedure in this chapter for any primary cause SONET failure condition as previously listed.
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.

RPR-SPAN-MISMATCH

Default Severity: Major (MJ), Service-Affecting (SA)
SONET Logical Objects: ML100T, ML1000, MLFX

The IEEE 802.17b-based RPR-SPAN-MISMATCH alarm is caused by span misprovisioning, span forced switching, physical miscabling, or a circuit loopback.

Miscabling problems between this node's east or west span and its neighboring span in the same direction can also cause this alarm, as will provisioning an XC loopback on a circuit that carries RPR-IEEE traffic.

If a traffic-affecting issue such as the "AIS-P" alarm, the "GFP-LFD" alarm, the "LOP-P" alarm, the "RFI-P" alarm, or the "UNEQ-P" alarm occurs, it in turn suppresses RPR-SPAN-MISMATCH.

Note: Clearing a circuit XC loopback does not always cause the loopback to clear. If this is the case, a FORCE switch is used to clear the RPR-SPAN-MISMATCH alarm. The FORCE might cause a traffic hit.

RPR- SPAN-MISMATCH is suppressed by "RPR-PASSTHR" alarm.

Clear the RPR-SPAN-MISMATCH Alarm

1. Locate and clear any primary cause provisioning errors.
2. If the alarm does not clear, locate and correct any span cabling errors.
3. If the alarm does not clear, look for and clear XC loopbacks on the spans.
4. If the alarm does not clear, configure a FORCE switch on the 802.17b-based RPR span and then clear the switch. To do this, enter the following CLI command in RPR-IEEE interface provisioning mode:

```
router(config)# rpr-ieee protection request forced-switch
{east | west}
```

Clear the switch by entering the following command:

```
router(config)# no rpr-ieee protection request forced-switch
{east | west}
```

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.

RPRW

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)
SONET Logical Objects: ML100T, ML1000, MLFX

The Cisco proprietary RPR Wrapped condition applies to CE100T-8 and ML-Series cards and occurs when the Cisco proprietary RPR protocol initiates a ring wrap due to a fiber cut, node failure, node restoration, new node insertion, or other traffic problem. It can also be raised if the POS port has an Admin down condition. (In this case, you will not see any SONET-level alarms or the "TPTFAIL (ML100T, ML1000, MLFX)" alarm.)

When the wrap occurs, traffic is redirected to the original destination by sending it in the opposite direction around the ring after a link state change or after receiving any SONET path-level alarms.

Note: ML-Series card POS interfaces normally send the "PDI-P" alarm to the far end when the POS link goes down or when Cisco proprietary RPR wraps. ML-Series card POS interfaces do not send a PDI-P alarm to the far end when this alarm is detected, when the alarm is being sent to the far end, or when the only defects being detected are the "GFP-LFD" alarm, the "GFP-CSF" alarm, the VCAT "LOM" alarm, or the VCAT "SQM" alarm.

Note: For more information about ML-Series Ethernet cards, refer to the *Cisco ONS 15454 and Cisco ONS 15454 SDH Ethernet Card Software Feature and Configuration Guide*.

Clear the RPRW Condition

1. Look for and clear any service-affecting SONET path-level alarms on the affected circuit, such as the "LOP-P" alarm, the "LOS-P (TRUNK)" alarm, the "PLM-P" alarm, or the "TIM-P" alarm. Clearing such an alarm can also clear RPRW.
2. If the condition does not clear, look for and clear any service alarms for the ML-Series card itself, such as the "CARLOSS (CEMR, CE1000, CE100T)" alarm, the "CARLOSS (ML1000, ML100T, MLFX)" alarm, the "TPTFAIL (CEMR, CE100T, CE1000)" alarm, or the "TPTFAIL (ML100T, ML1000, MLFX)" alarm.
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).

RUNCFG-SAVENEED

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

The Run Configuration Save Needed condition occurs when you change the running configuration file for ML-Series cards. It is a reminder that you must save the change to the startup configuration file for it to be permanent.

The condition clears after you save the running configuration to the startup configuration, such as by entering the following command in privileged executive mode in the CLI:

```
router# copy run start
```

If you do not save the change, the change is lost after the card reboots. If the command "copy run start" is executed in configuration mode and not privileged executive mode, the running configuration will be saved, but the alarm will not clear.

Note: For more information about the ML-Series Ethernet cards, refer to the *Cisco ONS 15454 and Cisco ONS 15454 SDH Ethernet Card Software Feature and Configuration Guide*.

SD (DS1, DS3)

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

A Signal Degrade (SD) condition for DS-1 or DS-3 occurs when the quality of an electrical signal on a DS3XM-6, DS3XM-12, or DS3/EC1-48 card has exceeded the BER signal degrade threshold. Signal degrade is defined by Telcordia as a soft failure condition. SD and signal fail (SF) both monitor the incoming BER and are similar, but SD is triggered at a lower bit error rate than SF.

The BER threshold is user-provisionable and has a range for SD from 1E-9 dBm to 1E-5 dBm.

SD can be reported on electrical card ports that are In-Service and Normal (IS-NR); Out-of-Service and Autonomous, Automatic In-Service (OOS-AU,AIS); or Out-of-Service and Management, Maintenance (OOS-MA,MT), but not in the Out-of-Service and Management, Disabled (OOS-MA,DSBLD) service state. The BER count increase associated with this alarm does not take an IS-NR port out of service, but if it occurs on an AINS port, the alarm prevents the port from going into service.

The SD condition clears when the BER level falls to one-tenth of the threshold level that triggered the condition. A BER increase is sometimes caused by a physical fiber problem such as a faulty fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice. SD can also be caused by repeated XC10G card switches that in turn can cause switching on the lines or paths.

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

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

Note: Some levels of BER errors (such as 1E-9 dBm) take a long period to raise or clear, about 9,000 seconds, or 150 minutes. If the SD threshold is provisioned at 1E-9 dBm rate, the SD alarm needs at least one and one-half hours to raise and then another period at least as long to clear.

Note: The recommended test set for use on all SONET ONS electrical cards is the Omniber 718. For specific procedures to use the test set equipment, consult the manufacturer.

Clear the SD (DS1, DS3) Condition

1. If the condition applies for a DS-3 line on a DS3XM-6, DS3XM-12, DS3E-12, or DS3/EC1-48 card, complete the Clear a DS3XM-6, DS3XM-12, or DS3E-12 Card Loopback Circuit. If the condition applies to any other DS-N card (DS3i-N-14, DS3-12, DS3i-N-14, or DS1/E1-56) complete the Clear Other Electrical Card or Ethernet Card Loopbacks.

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

2. Ensure that the fiber connector for the card is completely plugged in. For more information about fiber connections and card insertion, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 Procedure Guide*.
3. If the BER threshold is correct and at the expected level, use an optical test set to measure the power level of the line to ensure it is within guidelines. For specific procedures to use the test set equipment, consult the manufacturer.
4. If the optical power level is good, verify that optical receive levels are within the acceptable range.
5. If receive levels are good, clean the fibers at both ends according to site practice. If no site practice exists, complete the procedure in the "Maintain the Node" chapter in the *Cisco ONS 15454 Procedure Guide*.
6. If the condition does not clear, verify that single-mode fiber is used.
7. If the fiber is of the correct type, verify that a single-mode laser is used at the far-end node.
8. Clean the fiber connectors at both ends for a signal degrade according to site practice.
9. Verify that a single-mode laser is used at the far end.
10. If the problem does not clear, the transmitter at the other end of the optical line could be failing and require replacement. Refer to the Physical Card Reseating, Resetting, and Replacement.
11. If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

SD (E1)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)
SONET Logical Object: E1

An SD condition for an E1 occurs on a DS1/E1-56 card in E1 only mode when the quality of an electrical signal has exceeded the BER signal degrade threshold.

SD is triggered at a lower bit error rate than SF. The SD BER threshold is user-provisionable and ranges from 1E-9 dBm to 1E-5 dBm.

SD can be reported on electrical card ports that are In-Service and Normal (IS-NR); Out-of-Service and Autonomous, Automatic In-Service (OOS-AU,AIS); or Out-of-Service and Management, Maintenance (OOS-MA,MT) but not in the Out-of-Service and Management, Disabled (OOS-MA,DSBLD) service state. The BER count increase associated with this alarm does not take an IS-NR port out of service, but if it occurs on an AINS port, the alarm prevents the port from going into service.

The SD condition clears when the BER level falls to one-tenth of the threshold level that triggered the condition. A BER increase is sometimes caused by a physical fiber problem such as a faulty fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice. SD can also be caused by repeated XC10G card switches that in turn can cause switching on the lines or paths.

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

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

Note: Some levels of BER errors (such as 1E-9 dBm) take a long period to raise or clear, about 9,000 seconds, or 150 minutes. If the SD threshold is provisioned at 1E-9 dBm rate, the SD alarm needs at least one and a half hours to raise and then another period at least as long to clear.

Note: The recommended test set for use on all SONET ONS electrical cards is the Omniber 718. For specific procedures to use the test set equipment, consult the manufacturer.

Clear the SD (E1) Condition

1. Complete the Clear Other Electrical Card or Ethernet Card Loopbacks.

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

2. Ensure that the fiber connector for the card is completely plugged in. For more information about fiber connections and card insertion, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 Procedure Guide*.
3. If the BER threshold is correct and at the expected level, use an optical test set to measure the power level of the line to ensure it is within guidelines. For specific procedures to use the test set equipment, consult the manufacturer.
4. If the optical power level is good, verify that optical receive levels are within the acceptable range.
5. If receive levels are good, clean the fibers at both ends according to site practice. If no site practice exists, complete the procedure in the "Maintain the Node" chapter of the *Cisco ONS 15454 Procedure Guide*.
6. If the condition does not clear, verify that single-mode fiber is used.
7. If the fiber is of the correct type, verify that a single-mode laser is used at the far-end node.
8. Clean the fiber connectors at both ends for a signal degrade according to site practice.
9. If the problem does not clear, the transmitter at the other end of the optical line could be failing and require replacement. Refer to the Physical Card Reseating, Resetting, and Replacement.
10. If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

SD (TRUNK)

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

SD-L

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)
SONET Logical Objects: EC1, OCN

An SD Line condition is similar to the "SD (DS1, DS3)" condition. It applies to the line level of the SONET signal and travels on the B2 byte of the SONET overhead.

An SD-L on an Ethernet or OC-N card does not cause a protection switch. If the alarm is reported on a card that has also undergone a protection switch, the SD BER count continues to accumulate. The condition is superseded by higher-priority alarms such as the "LOF (EC1)" alarm, the "LOF (OCN)" alarm, the "LOS (EC1)" alarm, and the "LOS (OCN)" alarm.

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

Clear the SD-L Condition

1. Complete the Clear the SD (DS1, DS3) Condition.
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.

SD-L (TRUNK)

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

SD-P

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)
SONET Logical Objects: STSMON, STSTRM

An SD Path condition is similar to the "SD (DS1, DS3)" condition, but it applies to the path (STS) layer of the SONET overhead. A path or STS-level SD alarm travels on the B3 byte of the SONET overhead.

For path protection protected circuits, the BER threshold is user-provisionable and has a range for SD from 1E-9 dBm to 1E-5 dBm. For BLSR 1+1 and unprotected circuits, the BER threshold value is not user-provisionable and the error rate is hard-coded to 1E-6 dBm.

On path protection configurations, an SD-P condition causes a switch from the working card to the protect card at the path (STS) level. On BLSR, 1+1, and on unprotected circuits, an SD-P condition does not cause switching.

The BER increase that causes the condition is sometimes caused by a physical fiber problem such as a poor fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice.

The SD clears when the BER level falls to one-tenth of the threshold level that triggered the alarm.

Clear the SD-P Condition

1. Complete the Clear the SD (DS1, DS3) Condition.
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.

SD-V

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)
SONET Logical Objects: VT-MON, VT-TERM

An SD-V condition is similar to the "SD (DS1, DS3)" condition, but it applies to the VT layer of the SONET overhead.

For path protection protected circuits, the BER threshold is user-provisionable and has a range for SD from 1E-9 dBm to 1E-5 dBm. For BLSR 1+1 and unprotected circuits, the BER threshold value is not user-provisionable and the error rate is hard-coded to 1E-6 dBm.

On path protection configurations, an SD-V condition does not cause a switch from the working card to the protect card at the path (STS) level. On BLSR, 1+1, and on unprotected circuits, an SD-V condition does not cause switching.

The BER increase that causes the alarm is sometimes caused by a physical fiber problem such as a poor fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice.

The SD alarm clears when the BER level falls to one-tenth of the threshold level that triggered the alarm.

Clear the SD-V Condition

1. Complete the Clear the SD (DS1, DS3) Condition.
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.

SF (DS1, DS3)

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

A Signal Fail (SF) condition occurs when the quality of the signal has exceeded the BER signal failure threshold. Signal failure is defined by Telcordia as a "hard failure" condition. The SD and SF conditions both monitor the incoming BER error rate and are similar conditions, but SF is triggered at a higher BER than SD.

The BER threshold is user-provisionable and has a range for SF from 1E-5 dBm to 1E-3 dBm.

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

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

Clear the SF (DS1, DS3) Condition

1. Complete the Clear the SD (DS1, DS3) Condition.

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

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.

SF (E1)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)
SONET Logical Object: E1

An SF condition for an E1 occurs on a DS1/IE1-56 card in E1 only mode when the quality of the signal has exceeded the BER signal failure threshold.

SF monitors the incoming BER error rate just as SD does, but SF is triggered at a higher BER than SD. The SF BER threshold is user-provisionable and has a range for SF from 1E-5 dBm to 1E-3 dBm.

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

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

Clear the SF (E1) Condition

1. Complete the [Clear the SD \(E1\) Condition](#).

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

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.

SF (TRUNK)

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

SF-L

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)
SONET Logical Objects: EC1, OCN

An SF Line condition is similar to the ["SF \(DS1, DS3\)"](#) condition, but it applies to the line layer B2 overhead byte of the SONET signal. It can trigger a protection switch.

The SF-L condition clears when the BER level falls to one-tenth of the threshold level that triggered the condition. A BER increase is sometimes caused by a physical fiber problem, including a poor fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice.

The condition is superseded by higher-priority alarms such as the "LOF (EC1)" alarm, the "LOS (EC1)" alarm, and the "LOS (OCN)" alarm.

Clear the SF-L Condition

1. Complete the Clear the SD (DS1, DS3) Condition.
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.

SF-L (TRUNK)

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

SF-P

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)
SONET Logical Objects: STSMON, STSTRM

An SF Path condition is similar to the "SF (DS1, DS3)" condition, but it applies to the path (STS) layer B3 byte of the SONET overhead. It can trigger a protection switch.

The SF-P condition clears when the BER level falls to one-tenth of the threshold level that triggered the condition. A BER increase is sometimes caused by a physical fiber problem, including a poor fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice.

Clear the SF-P Condition

1. Complete the Clear the SD (DS1, DS3) Condition.
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.

SFTWDOWN

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

A Software Download in Progress alarm occurs when the TCC2/TCC2P is downloading or transferring software.

If the active and standby TCC2/TCC2Ps have the same versions of software, it takes approximately three minutes for software to be updated on a standby TCC2/TCC2P.

If the active and standby TCC2/TCC2Ps have different software versions, the transfer can take up to 30 minutes. Software transfers occur when different software versions exist on the two cards. After the transfer completes, the active TCC2/TCC2P reboots and goes into standby mode after approximately three minutes.

No action is necessary. Wait for the transfer or the software download to complete. If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

Caution! Updating software on a standby TCC2/TCC2P can take up to 30 minutes. Wait the full time period

before removing the card. Premature removal can cause flash corruption.

Note: When you upgrade a TCC2 to card to a TCC2P, the SFTWDOWN alarm can be raised and cleared more than once before the software download is complete. For example, when you remove the standby TCC2 card in Slot 11 and replace it with a TCC2P card, the SFTWDOWN alarm occurs within moments of this replacement. It can briefly clear and then raise again before it is finally cleared at the end of the upgrade process.

Note: SFTWDOWN is an informational alarm.

SF-V

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)
SONET Logical Objects: VT-MON, VT-TERM

An SF-V condition is similar to the "SF (DS1, DS3)" condition, but it applies to the VT layer of the SONET overhead.

Clear the SF-V Condition

1. Complete the Clear the SD (DS1, DS3) Condition.
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.

SHELF-COMM-FAIL

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

SH-IL-VAR-DEG-HIGH

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

SH-IL-VAR-DEG-LOW

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

SHUTTER-OPEN

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

SIGLOSS

Default Severity: Major (MJ), Service-Affecting (SA)
SONET Logical Object: FCMR
DWDM Logical Objects: ESCON, FC, GE, ISC, TRUNK

The Signal Loss on Data Interface alarm is raised on FC_MR-4 card receive client ports and MXP card FC and ISC client data ports when there is a loss of signal. (Loss of Gigabit Ethernet client signal results in a

"CARLOSS (GE)" alarm, not SIGLOSS.) SIGLOSS can also be raised on the MXP trunk port.

If the "SYNCLOSS" alarm, was previously raised on the port, the SIGLOSS alarm will demote it.

Clear the SIGLOSS Alarm

1. Ensure that the data port connection at the near-end card's port of the SONET link is operational.
2. Verify fiber continuity to the port. To verify fiber continuity, follow site practices.
3. Check the physical port LED on the card. The port LED looks clear (that is, not lit green) if the link is not connected.
4. If the alarm does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.

SNTP-HOST

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

The Simple Network Timing Protocol (SNTP) Host Failure alarm indicates that an ONS 15454 serving as an IP proxy for the other ONS 15454 nodes in the ring is not forwarding SNTP information to the other nodes in the network. The forwarding failure can result from two causes: either the IP network attached to the ONS 15454 proxy node is experiencing problems, or the ONS 15454 proxy node itself is not functioning properly.

Clear the SNTP-HOST Alarm

1. Ping the SNTP host from a workstation in the same subnet to ensure that communication is possible within the subnet by completing the Verify PC Connection to the ONS 15454 (ping).
2. If the ping fails, contact the network administrator who manages the IP network that supplies the SNTP information to the proxy and determine whether the network is experiencing problems, which could affect the SNTP server/router connecting to the proxy ONS 15454 system.
3. If no network problems exist, ensure that the ONS system proxy is provisioned correctly:
 1. In node view for the ONS 15454 serving as the proxy, click the **Provisioning > General** tabs.
 2. Ensure that the Use NTP/SNTP Server check box is checked.
 3. If the Use NTP/SNTP Server check box is not checked, click it.
 4. Ensure that the Use NTP/SNTP Server field contains a valid IP address for the server.
4. If proxy is correctly provisioned, refer to the "Timing" chapter in the *Cisco ONS 15454 Reference Manual* for more information on SNTP Host.
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.

SPANLEN-OUT-OF-RANGE

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

SPAN-SW-EAST

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

The Span Switch Is Active East Side condition occurs when a span switch occurs at the east side of a

four-fiber BLSR span using a Manual Switch, APS switch, or Force Span command. The condition clears when the switch is cleared. SPAN-SW-EAST is visible on the network view Alarms, Conditions, and History tabs. The port where the Force Span was applied shows an "F" on the network view detailed circuit map.

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

SPAN-SW-WEST

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

The Span Switch Is Active West Side condition occurs when a span switch occurs at the west side of a four-fiber BLSR span using a Manual Switch, APS switch, or Force Span command. The condition clears when the switch is cleared. SPAN-SW-WEST is visible on the network view Alarms, Conditions, and History tabs. The port where the Force Span was applied shows an "F" on the network view detailed circuit map.

Note: SPAN-SW-WEST is an informational condition and does not require troubleshooting.

SQUELCH

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

The Ring Squelching Traffic condition occurs in a BLSR when a node that originates or terminates STS circuits fails or is isolated by multiple fiber cuts or maintenance Force Ring commands. The isolation or failure of the node disables circuits that originate or terminate on the failed node. SQUELCH conditions appear on one or both of the nodes on either side of the isolated or failed node. The "AIS-P" condition also appears on all nodes in the ring except the isolated node.

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

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

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

Clear the SQUELCH Condition

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

1. Determine the isolated node:
 1. From the View menu, choose **Go to Network View**.
 2. The grayed out node with red spans is the isolated node.
2. Verify fiber continuity to the ports on the isolated node. To verify cable continuity, follow site practices.
3. If fiber continuity is good, verify that the proper ports are in service:

1. Confirm that the LED is correctly illuminated on the physical card.
A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
2. To determine whether the OC-N port is in service, double-click the card in CTC to open the card view.
3. Click the **Provisioning > Line** tabs.
4. Verify that the Admin State column lists the port as IS.
5. If the Admin State column lists the port as OOS,MT or OOS,DSBLD, click the column and choose IS. Click **Apply**.
Note: If ports managed into IS admin state are not receiving signals, the LOS alarm is either raised or remains, and the port service state transitions to OOS-AU,FLT.
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.
5. If the signal is valid, verify that the power level of the optical signal is within the optical card receiver specifications. Refer to the *Cisco ONS 15454 Reference Manual* for card specifications.
6. If the receiver levels are good, ensure that the optical transmit and receive fibers are connected properly.
7. If the connectors are good, complete the Physically Replace a Traffic Card for the OC-N card.
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.

SQUELCHED

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)
SONET Logical Object: OCN
DWDM Logical Objects: 2R, ESCON, FC, GE, ISC, TRUNK

The Client Signal Squelched condition is raised by a TXP_MR_10G, TXP_MR_10E, TXP_MR_2.5G, TXPP_MR_2.5G, MXP_2.5G_10G, MXP_2.5G_10E, MXP_MR_2.5G, or MXPP_MR_2.5G card.

The condition can be raised in the following situations:

- An MXP or TXP client facility detects that an upstream receive facility has experienced a loss of signal (such as an Ethernet CARLOSS, DWDM SIGLOSS, or optical LOS). In response, the facility's transmit is turned off (SQUELCHED). The upstream receive facilities are the trunk receive on the same card as the client, as well as the client receive on the card at the other end of the trunk span.
- The client will squelch if the upstream trunk receive (on the same card) experiences the "SIGLOSS" alarm, the "CARLOSS (FC)" alarm, the "CARLOSS (GE)" alarm, the "CARLOSS (ISC)" alarm, the "LOS (2R)" alarm, the "LOS (ESCON)" alarm, the "LOS (ISC)" alarm, or the "LOS (TRUNK)" alarm. In some transparent modes, the client is squelched if the trunk detects the "AIS" alarm or the "TIM" alarm.
- The client will squelch if the upstream client receive (on the card at the other end of the DWDM span) experiences the "SIGLOSS" alarm, the "CARLOSS (FC)" alarm, the "CARLOSS (GE)" alarm, the "CARLOSS (ISC)" alarm, the "LOS (2R)" alarm, the "LOS (ESCON)" alarm, the "LOS (ISC)" alarm, or the "LOS (TRUNK)" alarm.

In an example situation, an upstream MXP_2.5G_10G client port receive experiences a "loss of light," and this port raises CARLOSS, SIGLOSS, or LOS (determined by the payload type) locally. The port also sends client signal fail to its downstream card. The downstream card raises a "GFP-CSF" alarm, turns off the client transmit laser, and raises the SQUELCHED condition.

The local client raises SQUELCHED if it also raises one of the following alarms for the client, all of which are signalled by the upstream node:

- GFP-CSF
- GFP-LFD
- GFP-NO-BUFFERS
- GFP-DE-MISMATCH
- GFP-EX-MISMATCH
- ODUK-1-AIS-PM
- ODUK-2-AIS-PM
- ODUK-3-AIS-PM
- ODUK-4-AIS-PM

On the MXP_MR_10G, the local client raises a SQUELCHED condition if the upstream client detects one of the following alarms. Note that no corresponding local alarm is raised to indicate which of these conditions is present upstream.

- LOS for the clients including the "LOS (2R)" alarm, the "LOS (ESCON)" alarm, and the "LOS (ISC)" alarm
- CARLOSS for the clients including the "CARLOSS (FC)" alarm, the "CARLOSS (GE)" alarm, and the "CARLOSS (ISC)" alarm.

The local client raises a SQUELCHED condition if the local trunk raises one of the following alarms:

- OTUK-AIS
- OTUK-LOF
- LOS (TRUNK)
- OTUK-TIM (squelching enabled)
- ODUK-AIS-PM
- ODUK-LCK-PM
- ODUK-TIM-PM (squelching enabled)
- TIM (for the OC-N, squelching enabled)
- LOF (OCN)
- LOS (OCN)
- CARLOSS (TRUNK)
- WVL-MISMATCH (client or trunk)

When troubleshooting the SQUELCHED condition locally, look for failures progressing upstream in the following order. (If you are troubleshooting this alarm remotely, reverse the order of progress.)

- Local client alarms, as above
- Local trunk alarms, as above
- Remote (upstream) client receive alarms, as above

Note: If you see a SQUELCHED condition on the trunk, this can only be caused by a transponder (TXP) card.

Note: For more information about MXP or TXP cards, refer to the *Cisco ONS 15454 DWDM Reference Manual*.

Clear the SQUELCHED Condition

1. If the object is reported against any object besides ESCON, determine whether the remote node and local node reports and LOF or the LOS alarm (for the client trunk, as listed above). If it does, turn to the relevant section in this chapter and complete the troubleshooting procedure.
2. If no LOF or LOS is reported, determine whether any other listed remote node or local node conditions as listed above has occurred. If so, turn to the relevant section of this chapter and complete the troubleshooting procedure.
3. If none of these alarms is reported, determine whether the local port reporting the SQUELCHED condition is in loopback. (You will see LPBKFACILITY or LPBKTERMINAL condition for this particular client type in the Condition window.) If it is in loopback, complete the following steps:
 1. Double-click the client card to open the card view.
 2. Click the **Maintenance > Loopback > Port** tabs.
 3. If the port Admin State column says OOS,MT or OOS,DSBLD, click the cell to highlight it and choose IS from the drop-down list. Changing the state to IS also clears any loopback provisioned on the port.
Note: If ports managed into IS admin state are not receiving signals, the LOS alarm is either raised or remains, and the port service state transitions to OOS-AU,FLT.
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.

SQM

Default Severity: Critical (CR), Service-Affecting (SA) for STSTRM; Major (MJ), Service-Affecting (SA) for VT-TERM
SONET Logical Objects: STSTRM, VT-TERM

The Sequence Mismatch alarm is a virtual concatenated (VCAT) member alarm. (VCAT member circuits are independent circuits that are concatenated from different time slots into a higher-rate signal.) The alarm occurs when the expected sequence numbers of VCAT members do not match the received sequence numbers.

Clear the SQM Alarm

1. For the errored circuit, complete the [Delete a Circuit](#).
2. Recreate the circuit using the "Create Circuits and VT Tunnels" chapter of the *Cisco ONS 15454 Procedure Guide*.
3. If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.

SSM-DUS

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)
SONET Logical Objects: BITS, DS1, E1, OCN
DWDM Logical Object: TRUNK

The Synchronization Status (SSM) Message Quality Changed to Do Not Use (DUS) condition occurs when the synchronization status message (SSM) quality level degrades to DUS or is manually changed to DUS.

The signal is often manually changed to DUS to prevent timing loops from occurring. Sending a DUS prevents the timing from being reused in a loop. The DUS signal can also be sent for line maintenance testing.

Note: SSM-DUS is an informational condition and does not require troubleshooting.

SSM-FAIL

Single Failure Default Severity: Minor (MN), Non-Service-Affecting (NSA); Double Failure ::Default Severity: Major (MJ), Service-Affecting (SA)
SONET Logical Objects: BITS, DS1, E1, OCN
DWDM Logical Object: TRUNK

The SSM Failed alarm occurs when the synchronization status messaging received by the ONS 15454 fails. The problem is external to the ONS 15454. This alarm indicates that although the ONS 15454 is set up to receive SSM, the timing source is not delivering valid SSM messages.

Clear the SSM-FAIL Alarm

1. Verify that SSM is enabled on the external timing source.
2. If timing is enabled, use an optical test set to determine that the external timing source is delivering SSM. For specific procedures to use the test set equipment, consult the manufacturer.
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.

SSM-LNC

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

SONET Logical Objects: BITS, NE-SREF, OCN

DWDM Logical Object: TRUNK

The SSM Local Node Clock (LNC) Traceable condition occurs on MXP trunk ports when the SSM (S1) byte of the SONET overhead multiplexing section has been changed to signify that the line or BITS timing source is the LNC.

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

SSM-OFF

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)
SONET Logical Objects: BITS, DS1, E1, OCN
DWDM Logical Object: TRUNK

The SSM Off condition applies to references used for timing the node. It occurs when the SSM for the reference has been turned off. The node is set up to receive SSM, but the timing source is not delivering SSM messages.

Clear the SSM-OFF Condition

1. Complete the [Clear the SSM-FAIL Alarm](#).
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.

SSM-PRC

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

SONET Logical Objects: BITS, NE-SREF, OCN

DWDM Logical Object: TRUNK

The SSM Primary Reference Clock (PRC) Traceable condition occurs when the SONET transmission level for an MXP trunk port is PRC.

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

SSM-PRS

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

SONET Logical Objects: BITS, DS1, E1, NE-SREF, OCN

DWDM Logical Object: TRUNK

The SSM Primary Reference Source (PRS) Traceable condition occurs when the SSM transmission level is changed to Stratum 1 Traceable.

Note: SSM-PRS is an informational condition and does not require troubleshooting.

SSM-RES

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

SONET Logical Objects: BITS, DS1, E1, NE-SREF, OCN

DWDM Logical Object: TRUNK

The SSM Reserved (RES) For Network Synchronization Use condition occurs when the synchronization message quality level is changed to RES.

Note: SSM-RES is an informational condition and does not require troubleshooting.

SSM-SDH-TN

The SSM-SDH-TN condition is not used in this platform in this release. It is reserved for development.

SSM-SETS

The SSM-SETS condition is not used in this platform in this release. It is reserved for development.

SSM-SMC

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

SONET Logical Objects: BITS, DS1, E1, NE-SREF, OCN

DWDM Logical Object: TRUNK

The SSM SONET Minimum Clock (SMC) Traceable condition occurs when the synchronization message quality level changes to SMC. The login node does not use the clock because the node cannot use any

reference beneath its internal level, which is ST3.

Note: SSM-SMC is an informational condition and does not require troubleshooting.

SSM-ST2

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)
SONET Logical Objects: BITS, DS1, E1, NE-SREF, OCN
DWDM Logical Object: TRUNK

The SSM Stratum 2 (ST2) Traceable condition occurs when the synchronization message quality level is changed to ST2.

Note: SSM-ST2 is an informational condition and does not require troubleshooting.

SSM-ST3

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)
SONET Logical Objects: BITS, DS1, E1, NE-SREF, OCN
DWDM Logical Object: TRUNK

The SSM Stratum 3 (ST3) Traceable condition occurs when the synchronization message quality level is changed to ST3.

Note: SSM-ST3 is an informational condition and does not require troubleshooting.

SSM-ST3E

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)
SONET Logical Objects: BITS, DS1, E1, NE-SREF, OCN
DWDM Logical Object: TRUNK

The SSM Stratum 3E (ST3E) Traceable condition indicates that the synchronization message quality level is changed to ST3E from a lower level of synchronization. SSM-ST3E is a Generation 2 SSM and is used for Generation 1.

Note: SSM-ST3E is an informational condition and does not require troubleshooting.

SSM-ST4

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)
SONET Logical Objects: BITS, DS1, E1, NE-SREF, OCN
DWDM Logical Object: TRUNK

The SSM Stratum 4 (ST4) Traceable condition occurs when the synchronization message quality level is lowered to ST4. The message quality is not used because it is below ST3.

Note: SSM-ST4 is an informational condition and does not require troubleshooting.

SSM-STU

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)
SONET Logical Objects: BITS, DS1, E1, NE-SREF, OCN
DWDM Logical Object: TRUNK

The SSM Synchronization Traceability Unknown (STU) condition occurs when the reporting node is timed to a reference that does not support SSM, but the ONS 15454 has SSM support enabled. SSM-STU can also occur if the timing source is sending out SSM messages but SSM is not enabled on the ONS 15454.

Clear the SSM-STU Condition

1. In node view, click the **Provisioning > Timing > BITS Facilities** tabs.
2. Complete one of the following depending upon the status of the Sync Messaging Enabled check box:
 - ◆ If the **Sync. Messaging Enabled** check box for the BITS source is checked, uncheck the box.
 - ◆ If the **Sync. Messaging Enabled** check box for the BITS source is not checked, check the box.
3. Click **Apply**.
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.

SSM-TNC

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)
SONET Logical Objects: BITS, NE-SREF, OCN
DWDM Logical Object: TRUNK

The SSM Transit Node Clock (TNC) Traceable condition occurs when the synchronization message quality level is changed to TNC.

Note: SSM-TNC is an informational condition and does not require troubleshooting.

STS-SQUELCH-L

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

The Ring is Squelching STS traffic condition is raised on an OC-N facility. If the node failure scenario includes the source or destination node, then switching the nodes will squelch all the STSs that originate from or destinate to the failure node. The condition resolves when the node is no longer failing.

This condition has an NA severity by default. However, the condition indicates that traffic is squelched due to node failure, that is, traffic outage. Traffic outage can be caused by different problems, such as multiple LOS alarms, AIS-L, or node power outage. STS-SQUELCH-L is symptomatic and indicates that the user must investigate which node in a ring is being isolated and what is causing the node isolation.

Note: STS-SQUELCH-L is an informational condition.

SW-MISMATCH

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

The Software Mismatch condition occurs during software upgrade when there is a mismatch between software versions. The card connecting to the TCC2/TCC2P is running an older version than the TCC2/TCC2P is.

Clear the SW-MISMATCH Condition

1. Complete the Reset a Traffic Card in CTC for the errored card.
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.

SWMTXMOD-PROT

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

The Switching Matrix Module Failure on Protect Slot alarm is raised by the Slot 10 cross connect card if this card is active (ACT). Any kind of cross-connect card can raise this alarm. (Two exceptions are given in the following paragraph.) SWMTXMOD-PROT occurs when a logic component internal to the Slot 10 cross connect is out of frame (OOF) with a traffic card in the system. In this case, the alarm is raised against the traffic card slot.

The XC-VXC-10G card can raise this alarm (in Slot 10) whether it is ACT or standby (SBY). The XCVT card can raise SWMTXMOD-PROT against itself if the cross-connect card is OOF with a second logic component on the same cross connect card.

Clear the SWMTXMOD-PROT Alarm

1. Complete the Reset a Traffic Card in CTC for the Slot 10 card. For the LED behavior, see the Typical Traffic Card LED Activity During Reset.
2. Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
3. If the alarm does not clear, complete the Remove and Reinsert (Reseat) Any Card for the Slot 10 cross-connect card.
4. Complete the Side Switch the Active and Standby Cross-Connect Cards.
Note: After the active cross-connect card goes into standby mode, the original standby slot becomes active. The former standby card ACT/SBY LED becomes green.
5. If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.

SWMTXMOD-WORK

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

The Switching Matrix Module Failure on Working Slot alarm is raised by the Slot 8 cross connect card if this card is active (ACT). Any kind of cross-connect card can raise this alarm. (Two exceptions are given in the

following paragraph.) SWMTXMOD-WORK occurs when a logic component internal to the Slot 8 cross connect is OOF with a traffic card in the system. In this case, the alarm is raised against the traffic card slot.

The XC-VXC-10G card can raise this alarm (in Slot 8) whether it is ACT or standby (SBY). The XCVT card can raise SWMTXMOD-WORK against itself if the cross-connect card is OOF with a second logic component on the same cross connect card.

Clear the SWMTXMOD-WORK Alarm

1. Complete the Reset a Traffic Card in CTC for the Slot 8 card. For LED behavior, see the Typical Traffic Card LED Activity During Reset.
2. Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
3. If the alarm does not clear, complete the Remove and Reinsert (Reseat) Any Card for the Slot 8 cross-connect card.
4. Complete the Side Switch the Active and Standby Cross-Connect Cards.
Note: After the active cross-connect card goes into standby mode, the original standby slot becomes active. The former standby card ACT/SBY LED becomes green.
5. If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.

SWTOPRI

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

The Synchronization Switch to Primary Reference condition occurs when the ONS 15454 switches to the primary timing source (reference 1). The ONS 15454 uses three ranked timing references. The timing references are typically two BITS-level or line-level sources and an internal reference.

Note: SWTOPRI is an informational condition and does not require troubleshooting.

SWTOSEC

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

The Synchronization Switch to Secondary Reference condition occurs when the ONS 15454 has switched to a secondary timing source (reference 2).

Clear the SWTOSEC Condition

1. To clear the condition, clear alarms related to failures of the primary source, such as the "SYNCPRI" alarm.
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.

SWTOTHIRD

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

The Synchronization Switch to Third Reference condition occurs when the ONS 15454 has switched to a third timing source (reference 3).

Clear the SWTOTHIRD Condition

1. To clear the condition, clear alarms related to failures of the primary source, such as the "SYNCPRI" alarm or the "SYNCSEC" alarm.
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.

SYNC-FREQ

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)
SONET Logical Objects: BITS, DS1, E1, OCN
DWDM Logical Object: TRUNK

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

Clear the SYNC-FREQ Condition

1. Use an optical test set to verify the timing frequency of the line or BITS timing source and ensure that it falls within the proper frequency. For specific procedures to use the test set equipment, consult the manufacturer.
For BITS, the proper timing frequency range is approximately -15 PPM to 15 PPM. For optical line timing, the proper frequency range is approximately -16 PPM to 16 PPM.
2. If the reference source frequency is not outside of bounds, complete the Physically Replace a Traffic Card for the TCC2/TCC2P.
Note: It takes up to 30 minutes for the TCC2/TCC2P to transfer the system software to the newly installed TCC2/TCC2P. Software transfer occurs in instances where different software versions exist on the two cards. When the transfer completes, the active TCC2/TCC2P reboots and goes into standby mode after approximately three minutes.
3. If the SYNC-FREQ condition continues to report after replacing the TCC2/TCC2P, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447.

SYNCLOSS

Default Severity: Major (MJ), Service-Affecting (SA)
SONET Logical Object: FCMR
DWDM Logical Objects: FC, GE, ISC, TRUNK

The Loss of Synchronization on Data Interface alarm is raised on FC_MR-4 client ports and MXP cards client or trunk ports when there is a loss of signal synchronization on the port. This alarm is demoted by the SIGLOSS alarm.

Clear the SYNCLOSS Alarm

1. Ensure that the data port connection at the near-end card's port of the SONET link is operational.
2. Verify fiber continuity to the port. To do this follow site practices.
3. View the physical port LED to determine whether the alarm has cleared:
 - ◆ If the LED is green, the alarm has cleared.

- ◆ If the port LED is clear (that is, not illuminated green), the link is not connected and the alarm has not cleared.
 - ◆ If the LED is red, this indicates that the fiber is pulled.
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.

SYNCPRI

Default Severity: Minor (MN), Non-Service-Affecting (NSA) for EXT-SREF;Major (MJ), Service-Affecting (SA) for NE-SREF
SONET Logical Objects: EXT-SREF, NE-SREF

A Loss of Timing on Primary Reference alarm occurs when the ONS 15454 loses the primary timing source (reference 1). The ONS 15454 uses three ranked timing references. The timing references are typically two BITS-level or line-level sources and an internal reference. If SYNCPRI occurs, the ONS 15454 should switch to its secondary timing source (reference 2). Switching to the secondary timing source also triggers the "SWTOSEC" alarm.

Note: The SYNCPRI alarm will be escalated to Major (MJ), Service-Affecting if no other valid references (SYNCSEC, SYNCTHIRD) are available. If any other reference are available then SYNCPRI gets raised as Minor (MN), non service affecting.

Clear the SYNCPRI Alarm

1. In node view, click the **Provisioning > Timing > General** tabs.
2. Verify the current configuration for REF-1 of the NE Reference.
3. If the primary timing reference is a BITS input, complete the Clear the LOS (BITS) Alarm.
4. If the primary reference clock is an incoming port on the ONS 15454, complete the Clear the LOS (OCN) Alarm.
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.

SYNCSEC

Default Severity: Minor (MN), Non-Service-Affecting (NSA)
SONET Logical Objects: EXT-SREF, NE-SREF

A Loss of Timing on Secondary Reference alarm occurs when the ONS 15454 loses the secondary timing source (reference 2). If SYNCSEC occurs, the ONS 15454 should switch to a third timing source (reference 3) to obtain valid timing for the ONS 15454. Switching to a third timing source also triggers the "SWTOTHIRD" alarm.

Note: The severity of SYNCSEC alarm is dependent on the alarm profile it is associated with. If the alarm profile it is associated with is Major (MJ), then this condition is raised as MJ, service affecting, even if alternate source of references are available.

Clear the SYNCSEC Alarm

1. In node view, click the **Provisioning > Timing > General** tabs.
2. Verify the current configuration of REF-2 for the NE Reference.
3. If the secondary reference is a BITS input, complete the Clear the LOS (BITS) Alarm.
4. Verify that the BITS clock is operating properly.

5. If the secondary timing source is an incoming port on the ONS 15454, complete the [Clear the LOS \(OCN\) Alarm](#).
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.

SYNCTHIRD

Default Severity: Minor (MN), Non-Service-Affecting (NSA)
SONET Logical Objects: EXT-SREF, NE-SREF

A Loss of Timing on Third Reference alarm occurs when the ONS 15454 loses the third timing source (reference 3). If SYNCTHIRD occurs and the ONS 15454 uses an internal reference for source three, the TCC2/TCC2P could have failed. The ONS 15454 often reports either the "[FRNGSYNC](#)" condition or the "[HLDOVRSYNC](#)" condition after a SYNCTHIRD alarm.

Note: The severity of SYNCTHIRD alarm is dependent on the alarm profile it is associated with. If the alarm profile it is associated with is Major (MJ), then this condition is raised as MJ, service affecting, even if alternate source of references are available.

Clear the SYNCTHIRD Alarm

1. In node view, click the **Provisioning > Timing > General** tabs.
2. Verify that the current configuration of REF-3 for the NE Reference. For more information about references, refer to the "Timing" chapter in the *Cisco ONS 15454 Reference Manual*.
3. If the third timing source is a BITS input, complete the [Clear the LOS \(BITS\) Alarm](#).
4. If the third timing source is an incoming port on the ONS 15454, complete the [Clear the LOS \(OCN\) Alarm](#).

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

5. If the third timing source uses the internal ONS 15454 timing, complete the [Reset an Active TCC2/TCC2P Card and Activate the Standby Card](#).
Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.
6. If the reset card has not rebooted successfully, or the alarm has not cleared, call Cisco TAC 1 800 553-2447. If the Cisco TAC technician tells you to reseal the card, complete the [Remove and Reinsert \(Reseat\) the Standby TCC2/TCC2P Card](#). If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the [Physically Replace a Traffic Card](#).

SYSBOOT

Default Severity: Major (MJ), Service-Affecting (SA)
SONET Logical Object: NE

The System Reboot alarm indicates that new software is booting on the TCC2/TCC2P. No action is required. The alarm clears when all cards finish rebooting the new software. The reboot takes up to 30 minutes. If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.

Note: SYSBOOT is an informational alarm. It only requires troubleshooting if it does not clear.

TEMP-MISM

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

Temperature Reading Mismatch Between Control Cards is raised when the temperature readings on the two TCC2/TCC2Ps are out of range of each other by more than some predefined difference (such as 5 degrees C). A message containing power monitoring and temperature information is exchanged between the two TCC2/TCC2Ps, allowing the values to be compared. The temperature of each TCC2/TCC2P is read from a system variable.

This condition can be caused by a clogged fan filter or by fan tray stoppage.

Clear the TEMP-MISM Condition

1. Complete the Inspect, Clean, and Replace the Reusable Air Filter.
2. If the condition does not clear, complete the Remove and Reinsert a Fan-Tray Assembly.
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.

TIM

Default Severity: Critical (CR), Service-Affecting (SA)
SONET Logical Object: OCN
DWDM Logical Object: TRUNK

The Section TIM alarm occurs when the expected J0 section trace string does not match the received section trace string. This occurs because the data being received is not correct, and the receiving port could not be connected to the correct transmitter port.

If the alarm occurs on a port that has been operating with no alarms, the circuit path has changed due to a fibering misconnection, a TL1 routing change, or to someone entering an incorrect value in the Current Transmit String field.

TIM occurs on a port that has previously been operating without alarms if someone switches optical fibers that connect the ports. TIM is usually accompanied by other alarms, such as the "LOS (OCN)" alarm or the "UNEO-P" alarm. If these alarms accompany a TIM alarm, reattach or replace the original cables/fibers to clear the alarms. If a Transmit or Expected String was changed, restore the original string.

Clear the TIM Alarm

1. Ensure that the physical fibers are correctly configured and attached. To do this, consult site documents. For more information about cabling the ONS 15454, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 Procedure Guide*.
2. If the alarm does not clear, you can compare the J0 expected and transmitted strings and, if necessary, change them:
 1. Log into the circuit source node and click the **Circuits** tab.
 2. Select the circuit reporting the condition, then click **Edit**.
 3. In the Edit Circuit window, check the Show Detailed Circuit Map check box and click Apply.
 4. On the detailed circuit map, right-click the source circuit port and choose **Edit J0 Path Trace** (port) from the shortcut menu.

ONS_15454_Troubleshooting_Guide_R8.5.x_--_Alarm_Troubleshooting_(M_through_W)

5. Compare the Current Transmit String and the Current Expected String entries in the Edit J0 Path Trace dialog box.
6. If the strings differ, correct the Transmit or Expected strings and click **Apply**.
7. Click **Close**.
3. If the alarm does not clear, ensure that the signal has not been incorrectly routed. (Although the ONS 15454 routes circuits automatically, the circuit route could have been changed using TL1.) If necessary, manually correct the routing using TL1. For instructions, refer to the *Cisco ONS SONET TLI Reference Guide* and the *Cisco ONS SONET TLI Command Guide* .
4. If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem if necessary.

TIM-MON

Default Severity: Minor (MN), Non-Service-Affecting (NSA)
SONET Logical Object: OCN
DWDM Logical Object: TRUNK

The TIM Section Monitor TIM alarm is similar to the "**TIM-P**" alarm, but it applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards when they are configured in transparent mode. (In transparent termination mode, all SONET overhead bytes are passed through from client ports to the trunk ports or from trunk ports to client ports.)

Note: For more information about MXP and TXP cards, refer to the *Cisco ONS 15454 DWDM Reference Manual*.

Clear the TIM-MON Alarm

1. Complete the [Clear the TIM-P Alarm](#).
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.

TIM-P

Default Severity: Critical (CR), Service-Affecting (SA) for STSTRM; Default Severity: Minor

MN), Non-Service-Affecting (NSA) for STSMON

SONET Logical Objects: STSMON, STSTRM

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

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

Clear the TIM-P Alarm

1. Complete the Clear the TIM Alarm. (The option will say "Edit J1 Path Trace" rather than "Edit J0 Path Trace.")
2. If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447. If the alarm applies to the STSTRM object, it is Service-Affecting (SA).

TIM-S

Default Severity: Critical (CR), Service-Affecting (SA)
SONET Logical Objects: EC1, OCN

The TIM for Section Overhead alarm occurs when there is a mismatch between the expected and received J0 section overhead strings in either Manual or Auto mode.

In manual mode at the DS3/EC1-48 card Section Trace window, the user enters the expected string into the Current Expected String field for the receiving port. The string must match the string typed into the Transmit String field for the sending port. If these fields do not match, the login node raises the TIM-S alarm.

In Auto mode on the receiving port, the card sets the expected string to the value of the received string. If the alarm occurs on a port that has been operating with no alarms, the circuit path has changed or someone entered a new incorrect value into the Current Transmit String field. Complete the following procedure to clear either problem.

TIM-S also occurs on a port that has previously been operating without alarms if someone switches the cables or optical fibers that connect the ports. If TIM-S is enabled on the port, the "AIS-L" alarm can be raised downstream and the "RFI-L" alarm can be raised upstream.

Note: AIS-L and RFI-L are disabled or enabled in the Provisioning > EC1 > Section Trace tab Disable AIS/RDI on TIM-S? check box.

Clear the TIM-S Alarm

1. Double-click the DS3/EC1-48 card to open the card view.
2. Click the **Provisioning > EC1 > Section Trace** tabs.
3. Choose the port from the Port pull-down.
4. In the Expected area, enter the correct string into the Current Expected String field.
5. Click Apply.
6. If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447. If the alarm applies to the STSTRM object, it is Service-Affecting (SA).

TIM-V

Default Severity: Major (MJ), Service-Affecting (SA)
SONET Logical Object: VT-TERM, VT-MON

The VT Path TIM alarm is raised on VT terminations when the J2 path trace is enabled and is mismatched with the expected trace string.

Clear the TIM-V Alarm

1. Complete the [Clear the TIM Alarm](#).
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.

TPTFAIL (CEMR, CE100T, CE1000)

Default Severity: Major (MJ), Service-Affecting (SA)
SONET Logical Objects: CEMR, CE100T, CE1000

The Transport (TPT) Layer Failure alarm for the CE-Series card indicates a break in the end-to-end Ethernet link integrity feature of the card. TPTFAIL indicates a far-end condition and not a problem with the port reporting TPTFAIL.

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

Clear the TPTFAIL (CEMR, CE100T, CE1000) Alarm

1. Complete the [Clear the TPTFAIL \(G1000\) Alarm](#).
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.

TPTFAIL (FCMR)

Default Severity: Major (MJ), Service-Affecting (SA)
SONET Logical Object: FCMR

The Transport Fail alarm is raised against a local Fibre Channel (FC) port on an FC_MR-4 card when the port receives another SONET error such as the "AIS-P" alarm, the "LOP-P" alarm; "UNEO-P" alarm, the "PLM-P" alarm, the "TIM-P" alarm, the "LOM" alarm (for VCAT only), or the "SQM" alarm (for VCAT only).

This TPTFAIL can be raised against Fibre Channel cards if the remote FC card port is down from SIGLOSS or SYNCLOSS. In that case, the remote FC card port sends a PDI-P error code in the SONET C2 byte and signals the local FC port transmitter to turn off (thus causing the local FC port to raise the TPTFAIL alarm). A TPTFAIL can also be raised when a far-end receive fiber is pulled. This alarm can be demoted when a facility loopback is placed on the FC_MR-4 port.

Clear the TPTFAIL (FCMR) Alarm

1. Find and clear any path alarms applying to the port. Refer to the correct section of this chapter for trouble clearing instructions. Clearing the path alarm also clears the TPTFAIL.
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.

TPTFAIL (G1000)

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

The Transport Layer Failure alarm for the G-Series Ethernet card indicates a break in the end-to-end Ethernet link integrity feature of the ONS 15454 G1000-4 cards. TPTFAIL indicates a far-end condition and not a problem with the port reporting TPTFAIL.

The TPTFAIL alarm indicates a problem on either the SONET path or the remote Ethernet port that prevents the complete end-to-end Ethernet path from working. If any SONET path alarms such as the "AIS-P" alarm, the "LOP-P" alarm, the "PDI-P" alarm, or the "UNEQ-P" alarm exist on the SONET path used by the Ethernet port, the affected port causes a TPTFAIL alarm. Also, if the far-end G1000-4 port Ethernet port is administratively disabled or it is reporting the "CARLOSS (G1000)" alarm, the C2 byte in the SONET path overhead indicates the "PDI-P" alarm, which in turn causes a TPTFAIL to be reported against the near-end port.

When a TPTFAIL alarm occurs, the near-end port is automatically disabled (transmit laser turned off). In turn, the laser shutoff can also cause the external Ethernet device attached at the near end to detect a link down and turn off its transmitter. This also causes a CARLOSS alarm to occur on the reporting port. In all cases, the source problem is either in the SONET path being used by the G1000-4 port or the far-end G1000-4 port to which it is mapped.

An occurrence of TPTFAIL on an ONS 15454 G1000-4 port indicates either a problem with the SONET path that the port is using or with the far-end G1000-4 port that is mapped to the port.

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

Clear the TPTFAIL (G1000) Alarm

1. Clear any alarms being reported by the OC-N card on the G1000-4 circuit.
2. If no alarms are reported by the OC-N card, or if the "PDI-P" condition is reported, the problem could be on the far-end G1000-4 port. Clear any alarms, such as CARLOSS, reported against the far-end port or card.
3. If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.

TPTFAIL (ML100T, ML1000, MLFX)

Default Severity: Major (MJ), Service-Affecting (SA)
SONET Logical Objects: ML100T, ML1000, MLFX

The TPT Layer Failure alarm for the ML-Series Ethernet card indicates a break in the end-to-end packet-over-SONET (POS) link integrity feature of the ML-Series POS cards. TPTFAIL indicates a far-end condition or misconfiguration of the POS port.

The TPTFAIL alarm indicates a problem on the SONET path, a problem on the remote POS port, or a misconfiguration of the POS port that prevents the complete end-to-end POS path from working. If any SONET path alarms such as the "AIS-P" condition, the "LOP-P" alarm, the "PDI-P" condition, or the "UNEQ-P" alarm exist on the circuit used by the POS port, the affected port could report a TPTFAIL alarm. If the far-end ML POS port is administratively disabled, it inserts an "AIS-P" condition that is detected by the

near-end port. The near-end port could report TPTFAIL in this event. If the POS port is misconfigured at the Cisco IOS CLI level, the misconfiguration causes the port to go down and report TPTFAIL.

Note: For more information about the ML-Series Ethernet cards, refer to the *Cisco ONS 15454 and Cisco ONS 15454 SDH Ethernet Card Software Feature and Configuration Guide*.

Clear the TPTFAIL (ML100T, ML1000, MLFX) Alarm

1. If there are no SONET alarms reported against the POS port circuit, verify that both POS ports are properly configured. Refer to the *Cisco ONS 15454 and Cisco ONS 15454 SDH Ethernet Card Software Feature and Configuration Guide* for configuration information.
2. If the "PLM-P" alarm is the only one reported against the POS port circuit, verify that both POS ports are properly configured. Refer to the *Cisco ONS 15454 and Cisco ONS 15454 SDH Ethernet Card Software Feature and Configuration Guide* for configuration information.
3. If the "PDI-P" condition is the only one reported against the POS port circuit and the circuit is terminated by a G-Series card, determine whether a "CARLOSS (G1000)" alarm is reported against the G-Series card, and if so, complete the [Clear the CARLOSS \(G1000\) Alarm](#).
4. If the "AIS-P" alarm, the "LOP-P" alarm, or the "UNEQ-P" alarm is present, clear those alarms using the procedures in those sections.
5. If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.

TRMT

Default Severity: Major (MJ), Service-Affecting (SA)
SONET Logical Objects: DS1, E1

A Missing Transmitter alarm occurs when there is a transmit failure on the ONS 15454 DS-1 card because of an internal hardware failure. The card must be replaced.

Clear the TRMT Alarm

1. Complete the [Physically Replace a Traffic Card](#) for the reporting DS-1 card.
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.

TRMT-MISS

Default Severity: Major (MJ), Service-Affecting (SA)
SONET Logical Objects: DS1, E1

A Facility Termination Equipment Transmitter Missing alarm occurs when the facility termination equipment detects an incorrect amount of impedance on its backplane connector. Incorrect impedance is detected when a transmit cable is missing on the DS-1 port or the backplane does not match the inserted card. For example, an SMB connector or a BNC connector could be connected to a DS-1 card instead of a DS-3 card.

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

Clear the TRMT-MISS Alarm

1. Verify that the device attached to the DS-1 port is operational.
2. If the device is operational, verify that the cabling is securely connected.
3. If the cabling is secure, verify that the pinouts are correct.
4. If the pinouts are correct, replace the transmit cable.
5. If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.

TX-AIS

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)
SONET Logical Objects: DS1, DS3, E1

The (TX) Transmit Direction AIS condition is raised by the ONS 15454 backplane when it receives a far-end DS-1 LOS.

Clear the TX-AIS Condition

1. Determine whether there are alarms on the downstream nodes and equipment, especially the "LOS (OCN)" alarm, or OOS ports.
2. Clear the downstream alarms using the applicable procedures in this chapter.
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.

TX-LOF

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)
SONET Logical Objects: DS1, E1

The Transmit Direction LOF condition is transmitted by the backplane when it receives a DS-1 TX-LOF.

This alarm is raised only at the transmit (egress) side.

Clear the TX-LOF Condition

1. Complete the [Clear the LOF \(DS1\) Alarm](#).
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.

TX-RAI

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)
SONET Logical Objects: DS1, DS3, E1

The Transmit Direction RAI condition is transmitted by the backplane when it receives a DS-1 TX-AIS. This alarm is raised only at the transmit side, but RAI is raised at both ends.

Clear the TX-RAI Condition

1. Complete the [Clear the TX-AIS Condition](#).
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.

UNC-WORD

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

UNEQ-P

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

An SLMF UNEQ Path alarm occurs when the path does not have a valid sender. The UNEQ-P indicator is carried in the C2 signal path byte in the SONET overhead. The source of the problem is the node that is transmitting the signal into the node reporting the UNEQ-P.

The alarm could result from a PARTIAL circuit or an empty VT tunnel. UNEQ-P occurs in the node that terminates a path.

Note: If a newly created circuit has no signal, a UNEQ-P alarm is reported on the OC-N cards and the "[AIS-P](#)" condition is reported on the terminating cards. These alarms clear when the circuit carries a signal.

Caution! Deleting a circuit affects traffic.

Clear the UNEQ-P Alarm

1. In node view, choose **Go to Network View from the View menu**.
2. Right-click the alarm to display the Select Affected Circuits shortcut menu.
3. Click **Select Affected Circuits**.
4. When the affected circuits appear, look in the Type column for VTT, which indicates a VT tunnel circuit. A VT tunnel with no VTs assigned could be the cause of an UNEQ-P alarm.
5. If the Type column does not contain VTT, there are no VT tunnels connected with the alarm. Go to Step 7.
6. If the Type column does contain VTT, attempt to delete these rows:
 - Note:** The node does not allow you to delete a valid VT tunnel or one with a valid VT circuit inside.
 1. Click the VT tunnel circuit row to highlight it. Complete the [Delete a Circuit](#).
 2. If an error message dialog box appears, the VT tunnel is valid and not the cause of the alarm.
 3. If any other rows contain VTT, repeat Step 6.
7. If all nodes in the ring appear in the CTC network view, determine whether the circuits are complete:
 1. Click the **Circuits** tab.
 2. Verify that PARTIAL is not listed in the Status column of any circuits.
8. If you find circuits listed as PARTIAL, use an optical test set to verify that these circuits are not working circuits that continue to pass traffic. For specific procedures to use the test set equipment, consult the manufacturer.
9. If the PARTIAL circuits are not needed or are not passing traffic, delete the PARTIAL circuits.
 - Complete the [Delete a Circuit](#).
10. Recreate the circuit with the correct circuit size. Refer to the "Create Circuits and VT Tunnels" chapter in the *Cisco ONS 15454 Procedure Guide*.

11. Log back in and verify that all circuits terminating in the reporting card are active:
 1. Click the **Circuits** tab.
 2. Verify that the **Status** column lists all circuits as active.
12. If the alarm does not clear, clean the far-end optical fiber according to site practice. If no site practice exists, complete the procedure in the "Maintain the Node" chapter of the *Cisco ONS 15454 Procedure Guide*.

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

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

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

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

13. If the alarm does not clear, complete the Physically Replace a Traffic Card for the OC-N and electrical cards.
14. If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC 1 800 553-2447 in order to report a Service-Affecting (SA) problem.

UNEQ-V

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

An SLMF UNEQ VT alarm indicates that the node is receiving SONET path overhead with Bits 5, 6, and 7 of the V5 overhead byte all set to zeroes. The source of the problem is not the node raising the alarm, but the node transmitting the VT signal to it. The V in UNEQ-V indicates that the failure has occurred at the VT layer.

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

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

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

Clear the UNEQ-V Alarm

1. Complete the [Clear the UNEQ-P Alarm](#).

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

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.

UNQUAL-PPM

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)
SONET Logical Objects: PPM

The Unqualified PPM Inserted condition occurs when a PPM with a nonqualified product ID is plugged into the card's port; that is, the PPM passes the security code check as a Cisco PPM but is not qualified for use on the particular card.

Clear the UNQUAL-PPM Condition

1. Obtain the correct Cisco PPM and replace the existing PPM with the new one.
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.

UT-COMM-FAIL

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

UT-FAIL

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

VCG-DEG

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

The VCAT Group Degraded alarm is a VCAT group alarm. (VCATs are groups of independent circuits that are concatenated from different time slots into higher-rate signals.) The alarm occurs when one member circuit carried by the ML-Series Ethernet card is down. This alarm is accompanied by the "[OOU-TPT](#)" alarm. It only occurs when a Critical (CR) alarm, such as LOS, causes a signal loss.

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

Clear the VCG-DEG Condition

1. Look for and clear any Critical (CR) alarms that apply to the errored card, such as the "LOS (2R)" alarm or "LOS (OTS)" alarm.
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.

VCG-DOWN

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

The VCAT Group Down alarm is a VCAT group alarm. (VCATs are groups of independent circuits that are concatenated from different time slots into higher-rate signals.) The alarm occurs when one or more member circuits carried by an ML-Series or CE-Series Ethernet card are down. This alarm occurs in conjunction with another Critical (CR) alarm, such as the "LOS (2R)" alarm.

Note: If LCAS (Link Capacity Adjustment Scheme) is not enabled, the VCAT group transitions to the down state with even a single member down. If SW-LCAS is enabled on the VCAT group for ML1 cards, or HW LCAS is enabled for CE cards, the VCAT group transitions to the VCG-DOWN state only when all the members are down. The presence of at least one working member causes the VCAT group to remain in VCG-DEG (VCG degraded) state.

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

Clear the VCG-DOWN Condition

1. Complete the Clear the VCG-DEG Condition.
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.

VOA-HDEG

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

VOA-HFAIL

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

VOA-LDEG

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

VOA-LFAIL

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

VOLT-MISM

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

The Power Monitoring Mismatch Between Control Cards alarm is raised against the shelf when the power voltages of both TCC2/TCC2Ps are out of range of each other by more than 5 VDC.

Clear the VOLT-MISM Condition

1. Check the incoming voltage level to the shelf using a voltmeter. Follow site practices or refer to the "Install the Shelf and Backplane Cable" chapter in the *Cisco ONS 15454 Procedure Guide* for power installation procedures.
2. Correct any incoming voltage issues.
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.

VT-SQUELCH-L

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

The Ring is Squelching VT Traffic condition is raised on an OC-N facility. If the node failure scenario includes the source node, the node dropping VT will squelch VT traffic. The condition resolves when the node failure is recovered.

This condition is raised as NA severity by default. However, it indicates that traffic is squelched due to node failure, that is, traffic outage. Traffic outage can be caused by different problems, such as multiple instances of the "LOS (OCN)" alarm, the "AIS-L" condition, or node power outage. VT-SQUELCH-L is symptomatic and indicates that the user must investigate which node in a ring is being isolated and what causes node isolation.

Note: VT-SQUELCH-L is an informational condition.

WKSWPR

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)
SONET Logical Objects: EQPT, OCN, STSMON, VT-MON
DWDM Logical Objects: 2R, ESCON, FC, GE, ISC

The Working Switched To Protection condition occurs when a line experiences the "LOS (OCN)" alarm, the "SD (DS1, DS3)" condition, or the "SD (TRUNK)" condition.

This condition is also raised when you use the Manual Switch, APS Switch, FORCE SPAN, FORCE RING or MANUAL SPAN command at the network level. WKSWPR is visible on the network view Alarms, Conditions, and History tabs.

Clear the WKSWPR Condition

1. Complete the [Clear the LOS \(OCN\) Alarm](#).
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.

WORK-QUEUE-FULL

Default Severity: Not Alarmed (NA)
 Logical Object: EQPT

The Work Queue Full condition occurs when the netTask Queue in VxWorks has filled up and task operations for the card is postponed.

WTR

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)
 SONET Logical Objects: EC1, EQPT, ML1000, ML100T, MLFX, OCN, STSMON, VT-MON
 DWDM Logical Objects: 2R, ESCON, FC, GE, ISC, TRUNK

The Wait To Restore condition for SONET and DWDM objects occurs when the "WKSWPR" condition is raised, but the wait-to-restore time has not expired, meaning that the active protect path cannot revert to the working path. The condition clears when the timer expires and traffic switches back to the working path.

If the condition is raised on an IEEE 802.17b-based RPR span, it indicates that the wait-to-restore timer is active after a span failure has cleared.

Caution! DS-1 traffic loss can occur on a DS-1 with 1:N protection if a DS-1 card is reset with the protect card in the WTR state.

Note: Generally, WTR is an informational condition and does not require troubleshooting.

Clear the WTR Condition on an IEEE 802.17b-Based RPR Span

1. Determine the setting for the IEEE 802.17b-based RPR interface's WTR timer setting. In privileged executive mode, enter the following command:

```
router#show interface rpr protection
View the WTR timer setting.
```

2. If the timer is set to "never," clear the WTR condition by requesting a forced switch on the span. Enter the following command at the RPR-IEEE interface configuration mode command prompt:

```
router(config-if)#rpr-ieee protection request force-switch
{east | west}
```

3. If you configured a FORCE on the span, clear the switch with the following command:

```
router(config-if)#no rpr-ieee protection request force-switch
{east | west}
```

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.

WVL-MISMATCH

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

Traffic Card LED Activity

ONS 15454 traffic card LED behavior patterns are listed in the following sections. These sections give behavior for card insertion, reset, and side-switch.

Typical Traffic Card LED Activity After Insertion

When a card is inserted, the following LED activities occur:

1. The red FAIL LED turns on and remains illuminated for 20 to 30 seconds.
2. The red FAIL LED blinks for 35 to 45 seconds.
3. All LEDs blink once and turn off for 5 to 10 seconds.
4. The ACT or ACT/SBY LED turns on. The SF LED can persist until all card ports connect to their far-end counterparts and a signal is present.

Typical Traffic Card LED Activity During Reset

While a card resets, the following LED activities occur:

1. The FAIL LED on the physical card blinks and turns off.
2. The white LED with the letters "LDG" appears on the reset card in CTC.
3. The green ACT LED appears in CTC.

Typical Card LED State After Successful Reset

When a card successfully resets, the following LED states are present:

- ◇ If you are looking at the physical ONS 15454, the ACT/SBY LED is illuminated.
- ◇ If you are looking at node view of the ONS 15454, the current standby card has an amber LED depiction with the initials "SBY," and this has replaced the white "LDG" depiction on the card in CTC.
- ◇ If you are looking at node view of the ONS 15454, the current active card has a green LED depiction with the initials "ACT," and this has replaced the white "LDG" depiction on the card in CTC.

Typical Cross-Connect LED Activity During Side Switch

When a XC10G card is switched in CTC from active (ACT) to standby (SBY) or from SBY to ACT, the following LED activities occur:

1. The FAIL LED on the physical card blinks and turns off.
2. The standby card yellow SBY LED becomes a green ACT LED, indicating it is now active.
3. The active card green ACT LED becomes a yellow SBY LED, indicating it is now standby.

Frequently Used Alarm Troubleshooting Procedures

This section gives common procedures that are frequently used when troubleshooting alarms. Most of these procedures are summarized versions of fuller procedures existing elsewhere in the ONS 15454 documentation. They are included in this chapter for the user's convenience. For further information, please refer to the *Cisco ONS 15454 Procedure Guide*.

Node and Ring Identification, Change, Visibility, and Termination

The following procedures relate how to identify or change BLSR names and node IDs, and how to verify visibility from other nodes.

Identify a BLSR Ring Name or Node ID Number

1. Log into a node on the network.
2. In node view, choose **Go to Network View from the View menu**.
3. Click the **Provisioning > BLSR** tabs.
4. From the Ring Name column, record the ring name, or in the Nodes column, record the Node IDs in the BLSR. The Node IDs are the numbers in parentheses next to the node name.

Change a BLSR Ring Name

1. Log into a node on the network.
2. In node view, choose **Go to Network View from the View menu**.
3. Click the **Provisioning > BLSR** tabs.
4. Highlight the ring and click **Edit**.
5. In the BLSR window, enter the new name in the Ring Name field.
6. Click **Apply**.
7. Click **Yes** in the Changing Ring Name dialog box.

Change a BLSR Node ID Number

1. Log into a node on the network.
2. In node view, choose **Go to Network View from the View menu**.
3. Click the **Provisioning > BLSR** tabs.
4. Highlight the ring and click **Edit**.
5. In the BLSR window, right-click the node on the ring map.
6. Select **Set Node ID** from the shortcut menu.
7. In the Edit Node ID dialog box, enter the new ID. The Node ID is the number in parentheses after the Node Name.
8. Click **OK**.

Verify Node Visibility for Other Nodes

1. Log into a node on the network.
2. In node view, click the **Provisioning > BLSR** tabs.
3. Highlight a BLSR.
4. Click **Ring Map**.
5. In the BLSR Ring Map window, verify that each node in the ring appears on the ring map with a node ID and IP address.
6. Click **Close**.

Protection Switching, Lock Initiation, and Clearing

The following sections give instructions for port, ring, and span switching and switch-clearing commands, as well as lock-ons and lockouts.

Initiate a 1+1 Force Switch Command

This procedure switches 1+1 protection group traffic from one port in the group to the other using a Force switch.

Caution! The Force command overrides normal protective switching mechanisms. Applying this command incorrectly can cause traffic outages.

Caution! Traffic is not protected during a Force protection switch.

Note: A Force command switches traffic on a working path even if the path has signal degrade (SD) or signal fail (SF) conditions. A Force switch does not switch traffic on a protect path. A Force switch preempts a Manual switch.

1. In node view, click the **Maintenance > Protection** tabs.
2. In the Protection Groups area, select the protection group with the port you want to switch.
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.
4. In the Switch Commands area, click **Force**.
5. Click Yes in the Confirm Force Operation dialog box.
6. If the switch is successful, the group says "Force to working" in the Selected Groups area.

Initiate a 1+1 Manual Switch Command

This procedure switches 1+1 protection group traffic from one port in the group to the other using a Manual switch.

Note: A Manual command switches traffic if the path has an error rate less than the signal degrade. A Manual switch is preempted by a Force switch.

1. In node view, click the **Maintenance > Protection** tabs.
2. In the Protection Groups area, select the protection group with the port you want to switch.
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.
4. In the Switch Commands area, click **Manual**.
5. Click Yes in the Confirm Force Operation dialog box.
6. If the switch is successful, the group now says "Manual to working" in the Selected Groups area.

Clear a 1+1 Force or Manual Switch Command

Note: If the 1+1 protection group is configured as revertive, clearing a Force switch to protect (or working) moves traffic back to the working port. In revertive operation, the traffic always switches back to working. There is no revert to the protect. If ports are not configured as revertive, clearing a Force switch to protect does not move traffic back.

Note: If the Force Switch was user-initiated, the reversion occurs immediately when the clear command is issued. The five-minute WTR period is not needed in this case. If the Force was system-initiated, allow the five-minute waiting period (during WTR) before the reversion occurs.

1. In node view, click the **Maintenance > Protection** tabs.
2. In the Protection Groups area, choose the protection group containing the port you want to clear.

3. In the Selected Group area, choose the port you want to clear.
4. In the Switching Commands area, click **Clear**.
5. Click **Yes** in the Confirmation Dialog box.

The Force switch is cleared. Traffic immediately reverts to the working port if the group was configured for revertive switching.

Initiate a Lock-On Command

Note: For 1:1 and 1:N electrical protection groups, working or protect cards can be placed in the Lock On state. For a 1+1 optical protection group, only the working port can be placed in the Lock On state.

1. In node view, click the **Maintenance > Protection** tabs.
2. In the Protection Groups list, click the protection group where you want to apply a lock-on.
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:
 1. In the Selected Group list, click the protect card.
 2. In the Switch Commands area, click **Force**.
4. In the Selected Group list, click the active card where you want to lock traffic.
5. In the Inhibit Switching area, click **Lock On**.
6. Click **Yes** in the confirmation dialog box.

Initiate a Card or Port Lockout Command

Note: For 1:1 or 1:N electrical protection groups, working or protect cards can be placed in the Lock Out state. For a 1+1 optical protection group, only the protect port can be placed in the Lock Out state.

1. In node view, click the **Maintenance > Protection** tabs.
2. In the Protection Groups list, click the protection group that contains the card you want to lockout.
3. In the Selected Group list, click the card where you want to lock out traffic.
4. In the Inhibit Switching area, click **Lock Out**.
5. Click **Yes** in the confirmation dialog box.

The lockout has been applied and traffic is switched to the opposite card.

Clear a Lock-On or Lockout Command

1. In node view, click the **Maintenance > Protection** tabs.
2. In the Protection Groups list, click the protection group that contains the card you want to clear.
3. In the Selected Group list, click the card you want to clear.
4. In the Inhibit Switching area, click **Unlock**.
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.

1. In node view, click the **Maintenance > Protection** tabs.
2. Click the protection group that contains the card you want to switch.
3. Under Selected Group, click the active card.
4. Next to Switch Commands, click **Switch**.

The working slot should change to Working/Active and the protect slot should change to Protect/Standby.

Initiate a Force Switch for All Circuits on a Path Protection Span

This procedure forces all circuits in a path protection configuration from the working span to the protect. It is used to remove traffic from a card that originates or terminates path protection circuits.

Caution! The Force command overrides normal protective switching mechanisms. Applying this command incorrectly can cause traffic outages.

Caution! Traffic is not protected during a Force protection switch.

1. Log into a node on the network.
2. In node view, choose **Go to Network View from the View menu**.
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.
4. Click the **Perform Path Protection span switching** field.
5. Choose **Force Switch Away** from the drop-down list.
6. Click **Apply**.
7. In the Confirm Path Protection Switch dialog box, click **Yes**.
8. In the Protection Switch Result dialog box, click **OK**.
In the Circuits on Span dialog box, the switch state for all circuits is FORCE. Unprotected circuits do not switch.

Initiate a Manual Switch for All Circuits on a Path Protection Span

This procedure manually switches all circuits in a path protection configuration from the working span to the protect. It is used to remove traffic from a card that originates or terminates path protection circuits.

Caution! The Manual command does not override normal protective switching mechanisms.

1. Log into a node on the network.
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.
3. Click the **Perform Path Protection span switching** field.
4. Choose **Manual** from the drop-down list.
5. Click **Apply**.
6. In the Confirm Path Protection Switch dialog box, click **Yes**.
7. In the Protection Switch Result dialog box, click **OK**.
In the Circuits on Span dialog box, the switch state for all circuits is Manual. Unprotected circuits do not switch.

Initiate a Lockout for All Circuits on a Protect Path Protection Span

This procedure prevents all circuits in a path protection working span from switching to the protect span. It is used to keep traffic off cards that originate or terminate path protection circuits.

Caution! The Lock Out of Protect command overrides normal protective switching mechanisms.

1. Log into a node on the network. If you are already logged in, continue with Step 2.
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.

3. Click the **Perform Path Protection span switching** field.
4. Choose **Lock Out of Protect** from the drop-down list.
5. Click **Apply**.
6. In the Confirm Path Protection Switch dialog box, click **Yes**.
7. In the Protection Switch Result dialog box, click **OK**.
In the Circuits on Span dialog box, the switch state for all circuits is LOCKOUT.
Unprotected circuits do not switch.

Clear an External Switching Command on a Path Protection Span

Note: If the ports terminating a span are configured as revertive, clearing a Force or Manual switch to protect moves traffic back to the working port. If ports are not configured as nonrevertive, clearing a Force switch to protect does not move traffic back.

1. Log into a node on the network. If you are already logged in, continue with Step 2.
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.
3. Initiate a Force switch for all circuits on the span:
 1. Click the **Perform Path Protection span switching** field.
 2. Choose **Clear** from the drop-down list.
 3. Click **Apply**.
 4. In the Confirm Path Protection Switch dialog box, click **Yes**.
 5. 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

1. Log into a node on the network. If you are already logged in, continue with Step 2.
2. From the View menu choose **Go to Network View**.
3. In network view, click the **Provisioning > BLSR** tabs.
4. Click the row of the BLSR you are switching, then click **Edit**.
5. Right-click a BLSR node west port and choose **Set West Protection Operation**.
6. In the Set West Protection Operation dialog box, choose **Force Ring** from the drop-down list.
7. Click **OK**.
8. Click **Yes** in the two Confirm BLSR Operation dialog boxes that appear.

Initiate a Force Span Switch on a Four-Fiber BLSR

1. Log into a node on the network.
2. From the View menu choose **Go to Network View**.
3. In network view, click the **Provisioning > BLSR** tabs.
4. Click the row of the BLSR you are switching, then click **Edit**.
5. Right-click a BLSR node west port and choose **Set West Protection Operation**.
6. In the Set West Protection Operation dialog box, choose **Force Span** from the drop-down list.
7. Click **OK**.
8. Click **Yes** in the two Confirm BLSR Operation dialog boxes that appear.

Initiate a Manual Span Switch on a BLSR

1. From the View menu, choose **Go to Network View**.
2. Click the **Provisioning > BLSR** tabs.

3. Choose the BLSR and click **Edit**.
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).
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.
6. Click **OK**.
7. Click **Yes** in the two Confirm BLSR Operation dialog boxes.

Initiate a Manual Ring Switch on a BLSR

1. From the View menu, choose **Go to Network View**.
2. Click the **Provisioning > BLSR** tabs.
3. Choose the BLSR and click **Edit**.
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).
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.
6. Click **OK**.
7. Click **Yes** in the two Confirm BLSR Operation dialog boxes.

Initiate a Lockout on a BLSR Protect Span

1. From the View menu choose **Go to Network View**.
2. Click the **Provisioning > BLSR** tabs.
3. Choose the BLSR and click **Edit**.
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).
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.
6. Click **OK**.
7. Click **Yes** in the two Confirm BLSR Operation dialog boxes.

Initiate an Exercise Ring Switch on a BLSR

1. Log into a node on the network.
2. Click **View > Go to Network View**.
3. Click the **Provisioning > BLSR** tabs.
4. Click the row of the BLSR you are exercising, then click **Edit**.
5. Right-click the west port of a node and choose **Set West Protection Operation**.
6. In the Set West Protection Operation dialog box, choose **Exercise Ring** from the drop-down list.
7. Click **OK**.
8. Click **Yes** in the Confirm BLSR Operation dialog box.

Initiate an Exercise Ring Switch on a Four Fiber BLSR

1. Log into a node on the network.
2. From the View menu, choose **Go to Network View**.
3. Click the **Provisioning > BLSR** tabs.
4. Click the row of the BLSR you are exercising, then click **Edit**.
5. Right-click the west port of a node and choose **Set West Protection Operation**.
6. In the Set West Protection Operation dialog box, choose **Exercise Span** from the drop-down list.
7. Click **OK**.
8. Click **Yes** in the Confirm BLSR Operation dialog box.

Clear a BLSR External Switching Command

1. Log into a node on the network.
2. From the View menu, choose **Go to Network View**.
3. Click the **Provisioning > BLSR** tabs.
4. Click the BLSR you want to clear.
5. Right-click the west port of the BLSR node where you invoked the switch and choose **Set West Protection Operation**.
6. In the Set West Protection Operation dialog box, choose **Clear** from the drop-down list.
7. Click **OK**.
8. Click **Yes** in the Confirm BLSR Operation dialog box.

CTC Card Resetting and Switching

This section gives instructions for resetting traffic cards, TCC2/TCC2Ps, and cross-connect cards.

Caution! For TXP and MXP cards placed in a Y-cable protection group, do not perform a software reset on both cards simultaneously. Doing so will cause a traffic hit of more than one minute. For more information about Y-cable protection groups, refer to the *Cisco ONS 15454 DWDM Procedure Guide*.

Caution! Resetting the active card in a Y-cable group will cause a traffic outage if the standby card is down for any reason.

Note: When an AIC-I card is reset in CTC, any subsequent user client operations (such as CTC or TL1 activity) is paused for approximately 5-10 seconds. The reset does not cause any conditions to be raised.

Note: For more information about MXP and TXP cards, refer to the *Cisco ONS 15454 DWDM Reference Manual*.

Reset a Traffic Card in CTC

1. Log into a node on the network. If you are already logged in, continue with Step 2.
2. In node view, position the cursor over the optical or electrical traffic card slot reporting the alarm.
3. Right-click the card. Choose **Reset Card** from the shortcut menu.
4. Click **Yes** in the Resetting Card dialog box.

Reset an Active TCC2/TCC2P Card and Activate the Standby Card

Caution! Resetting an active TCC2/TCC2P can be service-affecting.

Note: Before you reset the TCC2/TCC2P, you should wait at least 60 seconds after the last provisioning change you made to avoid losing any changes to the database.

1. Log into a node on the network. If you are already logged in, continue with Step 2.
2. Identify the active TCC2/TCC2P:
If you are looking at the physical ONS 15454 shelf, the ACT/SBY LED of the active card is green. The ACT/STBLY LED of the standby card is amber.
3. Right-click the active TCC2/TCC2P in CTC.
4. Choose **Reset Card** from the shortcut menu.
5. Click **Yes** in the Confirmation Dialog box.
The card resets, the FAIL LED blinks on the physical card, and connection to the node is lost. CTC switches to network view.

6. Verify that the reset is complete and error-free and that no new related alarms appear in CTC. For LED appearance, see the [Typical Card LED State After Successful Reset](#).
7. Double-click the node and ensure that the reset TCC2/TCC2P is in standby mode and that the other TCC2/TCC2P is active. Verify the following:
 - ◆ If you are looking at the physical ONS 15454 shelf, the ACT/SBY LED of the active card is green. The ACT/STBLY LED of the standby card is amber.
 - ◆ No new alarms appear in the Alarms window in CTC.

Side Switch the Active and Standby Cross-Connect Cards

Caution! The cross-connect card side switch is usually service-affecting.

1. Log into a node on the network. For instructions regarding how to log into a node, refer *Cisco ONS 15454 Procedure Guide, Release 8.0*. If you are already logged in, continue with Step 2.
2. Display node view.
3. Determine the active or standby XC10G card.

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

Note: You can also position the cursor over the card graphic to display a popup identifying the card as active or standby.
4. In node view, click the **Maintenance > Cross-Connect > Cards** tabs.
5. Click **Switch**.
6. Click **Yes** in the Confirm Switch dialog box. See the [Typical Cross-Connect LED Activity During Side Switch](#) for LED information.

Note: During a maintenance side switch or soft reset of an active XC10G card, the 1+1 protection group might display a protection switch. To disallow the protection switch from being displayed, the protection group should be locked at the node where XC switch or soft reset of an active XC switch is in progress.

Caution! Active cross connect (XC10G/XCVT) cards should not be physically removed.

The following rules must be followed for removing an Active Cross Connect Card (XC10G/XCVT):

If the active cross connect has to be removed, perform an XCVT/XC10G side switch to change the status of the card from active to standby and then remove the cross connect card once it goes back to standby.

OR

Perform a lockout on all circuits that originate from the node whose active cross connect card has to be removed (performing a lockout on all spans will also accomplish the same goal).

Physical Card Reseating, Resetting, and Replacement

This section gives instructions for physically reseating and replacing TCC2/TCC2P, cross-connect, and traffic cards.

Caution! Do not physically replace a card without first making provisions to switch or move traffic to a different card or circuit. General procedures for this are located in the [Protection Switching, Lock Initiation, and Clearing](#). In-depth traffic switching procedures and information can be found in the "Maintain the Node" chapter of the *Cisco ONS 15454 Procedure Guide*.

Remove and Reinsert (Reseat) the Standby TCC2/TCC2P Card

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

Caution! Do not perform this action without the supervision and direction of Cisco TAC 1 800 553-2447.

Caution! The TCC2/TCC2P reseat could be service-affecting. Refer to the [Protection Switching, Lock Initiation, and Clearing](#) for traffic-switching procedures.

Note: Before you reset the TCC2/TCC2P, you should wait at least 60 seconds after the last provisioning change you made to avoid losing any changes to the database.

Note: When a standby TCC2/TCC2P card is removed and reinserted (reseated), all three fan lights could momentarily turn on, indicating that the fans have also reset.

1. Log into a node on the network.

Ensure that the TCC2/TCC2P you want to reseat is in standby mode. A standby card has an amber ACT/SBY (Active/Standby) LED illuminated.

2. When the TCC2/TCC2P is in standby mode, unlatch both the top and bottom ejectors on the TCC2/TCC2P.
3. Physically pull the card at least partly out of the slot until the lighted LEDs turn off.
4. Wait 30 seconds. Reinsert the card and close the ejectors.

Note: The TCC2/TCC2P requires several minutes to reboot and display the amber standby LED after rebooting. Refer to the *Cisco ONS 15454 Reference Manual* for more information about LED behavior during a card reboot.

Remove and Reinsert (Reseat) Any Card

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

1. Open the card ejectors.
2. Slide the card halfway out of the slot along the guide rails.
3. Slide the card all the way back into the slot along the guide rails.
4. Close the ejectors.

Physically Replace a Traffic Card

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

Caution! Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. refer to the procedures in the [Protection Switching, Lock Initiation, and Clearing](#). For more information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 Procedure Guide*.

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

1. Open the card ejectors.
2. Slide the card out of the slot.
3. Open the ejectors on the replacement card.

4. Slide the replacement card into the slot along the guide rails.
5. Close the ejectors.

Physically Replace an In-Service Cross-Connect Card

Caution! The cross-connect reseal could be service-affecting. Refer to the [Protection Switching, Lock Initiation, and Clearing](#) for traffic-switching procedures prior to completing this procedure.

Note: This procedure is placed in the chapter as a quick guide for the user's convenience. A more detailed procedure is located in the "Maintain the Node" chapter of the *Cisco ONS 15454 Procedure Guide*.

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

1. Determine the active cross-connect card (XCVT/XC10G/XC-VXC-10G). The ACT/SBY LED of the active card is green. The ACT/SBY LED of the standby card is amber.
Note: You can also place the cursor over the card graphic to display a popup identifying the card as active or standby.
2. Switch the active cross-connect card to standby:
 1. In the node view, click the **Maintenance > Cross-Connect** tabs.
 2. Under Cross Connect Cards, choose **Switch**.
 3. Click **Yes** in the Confirm Switch dialog box.
Note: After the active cross-connect card becomes standby, the original standby slot becomes active. This causes the ACT/SBY LED to become green on the former standby card.
3. Physically remove the new standby cross-connect card from the ONS 15454.
Note: An improper removal (IMPROPRMVL) alarm is raised when a card reseal is performed, unless the card is first deleted in Cisco Transport Controller (CTC). The alarm clears after the card is replaced.
4. Insert the replacement cross-connect card into the empty slot.
The replacement card boots up and becomes ready for service after approximately one minute.

Generic Signal and Circuit Procedures

This section gives instructions for verify BER thresholds, deleting circuits, provisioning SDCC terminations, and clearing loopbacks.

Verify the Signal BER Threshold Level

1. Log into a node on the network.
2. In node view, double-click the card reporting the alarm to open the card view.
3. Click the **Provisioning > Line** tabs.
4. Under the **SD BER** (or **SF BER**) column in the Provisioning window, verify that the cell entry is consistent with the originally provisioned threshold. The default setting is 1E-7.
5. If the entry is consistent with the original provisioning, go back to your original procedure.
6. If the entry is not consistent with what the system was originally provisioned for, click the cell to reveal the range of choices and click the original entry.
7. Click **Apply**.

Delete a Circuit

1. Log into a node on the network.
2. In node view, click the **Circuits** tab.
3. Click the circuit row to highlight it and click **Delete**.
4. Click **Yes** in the Delete Circuits dialog box.

Verify or Create Node Section DCC Terminations

Note: Portions of this procedure are different for ONS 15454 DWDM nodes.

1. Log into a node on the network.
2. In node view, click the **Provisioning > Comm Channels > SDCC** tab.
3. View the Port column entries to see where terminations are present for a node. If terminations are missing, proceed to Step 4.
4. If necessary, create a DCC termination:
 1. Click **Create**.
 2. 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.
 3. In the port state area, click the **Set to IS** radio button.
 4. Verify that the Disable OSPF on Link check box is unchecked.
 5. Click **OK**.

Clear an OC-N Card Facility or Terminal Loopback Circuit

1. Log into a node on the network.
2. Double-click the reporting card in CTC to open the card view.
3. Click the **Maintenance > Loopback > Port** tabs.
4. In the Loopback Type column, determine whether any port row shows a state other than None.
5. If a row contains another state besides None, click in the column cell to display the drop-down list and select None.
6. In the Admin State column, determine whether any port row shows a state other than IS.
7. If a row shows a state other than IS, click in the column cell to display the drop-down list and select IS.
8. Click **Apply**.

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

Clear an OC-N Card Cross-Connect (XC) Loopback Circuit

1. Log into a node on the network.
2. Double-click the reporting card in CTC to open the card view.
3. Click the **Maintenance > Loopback > SONET STS** tabs.
4. Uncheck the XC Loopback check box.
5. Click **Apply**.

Clear a DS3XM-6, DS3XM-12, or DS3E-12 Card Loopback Circuit

1. Log into a node on the network.
2. Double-click the reporting card in CTC to open the card view.
3. Click the **Maintenance > DS3** tabs or the **Maintenance > DS1** tabs.
4. In the Loopback Type column, determine whether any port row shows a state other than None.

5. If a row contains another state besides None, click in the column cell to display the drop-down list and select None.
6. In the Admin State column, determine whether any port row shows a state other than IS.
7. If a row shows a state other than IS, click in the column cell to display the drop-down list and select IS.
8. Click **Apply**.

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

Clear Other Electrical Card or Ethernet Card Loopbacks

Note: This procedure does not apply to DS3XM-6 or DS3XM-12 cards.

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

1. Log into a node on the network.
2. Double-click the reporting card in CTC to open the card view.
3. Click the **Maintenance > Loopback** tabs.
4. In the Loopback Type column, determine whether any port row shows a state other than None.
5. If a row contains another state besides None, click in the column cell to display the drop-down list and select **None**.
6. In the Admin State column, determine whether any port row shows a state other than IS.
7. If a row shows a state other than IS, click in the column cell to display the drop-down list and select IS.
8. Click **Apply**.

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

Clear an MXP, TXP, or FC_MR-4 Card Loopback Circuit

1. Log into a node on the network.
2. Double-click the reporting card in CTC to open the card view.
3. Click the **Maintenance > Loopback** tabs.
4. In the Loopback Type column, determine whether any port row shows a state other than None.
5. If a row contains another state besides None, click in the column cell to display the drop-down list and select None.
6. In the Admin State column, determine whether any port row shows an admin state other than IS, for example, OOS,MT.
7. If a row shows an admin state other than IS, click in the column cell to display the drop-down list and select IS.

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

8. Click **Apply**.

Air Filter and Fan Procedures

This section gives instructions for cleaning or replacing the air filter and reseating or replacing the fan tray assembly.

Inspect, Clean, and Replace the Reusable Air Filter

To complete this task, you need a vacuum cleaner or detergent and water faucet, a spare filter, and a pinned hex key.

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

Although the filter works if it is installed with either side facing up, Cisco recommends that you install it with the metal bracing facing up to preserve the surface of the filter.

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

1. Verify that you are replacing a reusable air filter. The reusable filter is made of a gray, open-cell, polyurethane foam that is specially coated to provide fire and fungi resistance. NEBS 3E and later versions of the ONS 15454 use a reusable air filter.
2. If the air filter is installed in the external filter brackets, slide the filter out of the brackets while being careful not to dislodge any dust that could have collected on the filter. If the filter is installed beneath the fan tray and not in the external filter brackets, open and remove the front door assembly by completing the following steps:
 1. Open the front door of the shelf assembly by completing the following substeps. (If it is already open or if the shelf assembly does not have a front door, continue with Step 3.)
 - Open the front door lock.
 - Press the door button to release the latch.
 - Swing the door open.
 2. Remove the front door by completing the following substeps (optional):
 - Detach the ground strap from either the door or the chassis by removing one of the Kepnuts.
 - Place the Kepnut back on the stud after the ground strap is removed to avoid misplacement.
 - Secure the dangling end of the ground strap to the door or chassis with tape.
3. Push the outer side of the handles on the fan-tray assembly to expose the handles.
4. Pull the handles and slide the fan-tray assembly one inch (25.4 mm) out of the shelf assembly and wait until the fans stop.
5. When the fans have stopped, pull the fan-tray assembly completely out of the shelf assembly.
6. Gently remove the air filter from the shelf assembly. Be careful not to dislodge any dust that could have collected on the filter.
7. Visually inspect the air filter material for dirt and dust.
8. If the reusable air filter has a concentration of dirt and dust, either vacuum or wash the air filter. Prior to washing the air filter, replace the dirty air filter with a clean air filter and also reinsert the fan-tray assembly. Wash the dirty air filter under a faucet with a light detergent.

Spare ONS 15454 filters should be kept in stock for this purpose.

Note: Cleaning should take place outside the operating environment to avoid releasing dirt and dust near the equipment.

9. If you washed the filter, allow it to completely air dry for at least eight hours.

Caution! Do not put a damp filter back in the ONS 15454.

10. If the air filter should be installed in the external filter brackets, slide the air filter all the way to the back of the brackets to complete the procedure.

11. If the filter should be installed beneath the fan-tray assembly, remove the fan-tray assembly and slide the air filter into the recessed compartment at the bottom of the shelf assembly. Put the front edge of the air filter flush against the front edge of the recessed compartment. Push the fan tray back into the shelf assembly.

Caution! If the fan tray does not slide all the way to the back of the shelf assembly, pull the fan tray out and readjust the position of the reusable filter until the fan tray fits correctly.

Note: On a powered-up ONS 15454, the fans start immediately after the fan-tray assembly is correctly inserted.

12. To verify that the tray is plugged into the backplane, ensure that the LCD on the front of the fan-tray assembly is activated and displays node information.
13. Rotate the retractable handles back into their compartments.
14. Replace the door and reattach the ground strap.

Remove and Reinsert a Fan-Tray Assembly

1. Use the retractable handles embedded in the front of the fan-tray assembly to pull it forward several inches.
2. Push the fan-tray assembly firmly back into the ONS 15454.
3. Close the retractable handles.

Replace the Fan-Tray Assembly

Caution! The 15454-FTA3 fan-tray assembly can only be installed in ONS 15454 R3.1 and later shelf assemblies (15454-SA-ANSI, P/N: 800-19857; 15454-SA-HD, P/N: 800-24848). It includes a pin that does not allow it to be installed in ONS 15454 shelf assemblies released before ONS 15454 R3.1 (15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1, P/N: 800-07149). Equipment damage can result from attempting to install the 15454-FTA3 in a incompatible shelf assembly.

Caution! Do not force a fan-tray assembly into place. Doing so can damage the connectors on the fan tray and/or the connectors on the backplane.

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

To replace the fan-tray assembly, it is not necessary to move any of the cable management facilities.

1. Open the front door of the shelf assembly by completing the following steps. If the shelf assembly does not have a front door, continue with Step 3.
 1. Open the front door lock.
 2. Press the door button to release the latch.
 3. Swing the door open.
2. Remove the front door (optional):
 1. Detach the ground strap from either the door or the chassis by removing one of the Kepnuts.
 2. Place the Kepnut back on the stud after the ground strap is removed to avoid misplacement.
 3. Secure the dangling end of the ground strap to the door or chassis with tape.
3. Push the outer side of the handles on the fan-tray assembly to expose the handles.
4. Fold out the retractable handles at the outside edges of the fan tray.
5. Pull the handles and slide the fan-tray assembly one inch (25.4 mm) out of the shelf assembly and wait until the fans stop.
6. When the fans have stopped, pull the fan-tray assembly completely out of the shelf assembly.

7. If you are replacing the fan-tray air filter and it is installed beneath the fan-tray assembly, slide the existing air filter out of the shelf assembly and replace it before replacing the fan-tray assembly.
If you are replacing the fan-tray air filter and it is installed in the external bottom bracket, you can slide the existing air filter out of the bracket and replace it at anytime. For more information on the fan-tray air filter, see the [Inspect, Clean, and Replace the Reusable Air Filter](#).
8. Slide the new fan tray into the shelf assembly until the electrical plug at the rear of the tray plugs into the corresponding receptacle on the backplane.
9. To verify that the tray has plugged into the backplane, check that the LCD on the front of the fan tray is activated.
10. If you replace the door, be sure to reattach the ground strap.

Interface Procedures

This section includes instructions for replacing an EIA and an AIP.

Replace the Electrical Interface Assembly

Note: You need a #2 Phillips screwdriver. If you use high-density BNC EIAs, you also need a BNC insertion and removal tool.

1. To remove the lower backplane cover, loosen the five screws that secure it to the ONS 15454 and pull it away from the shelf assembly.
2. Loosen the nine perimeter screws that hold the backplane sheet metal cover or EIA in place. Do not remove the interior screws.
If you are removing an AMP Champ EIA, remove the fastening plate before proceeding. To remove the fastening plate, loosen the two thumbscrews.
3. If a backplane cover is attached to the ONS 15454, lift the panel by the bottom to remove it from the shelf assembly and store the panel for later use.
4. If an EIA is attached to the ONS 15454, lift the EIA handles and gently pull it away from the backplane.
Note: Attach backplane sheet metal covers whenever EIAs are not installed.
5. Line up the connectors on the new EIA with the mating connectors on the backplane.
6. Gently push the EIA until both sets of connectors fit together snugly.
7. Replace the nine perimeter screws that you removed while removing the backplane cover.
8. If you are installing an AMP Champ EIA, attach the fastening plate with the two thumbscrews.
9. Reattach the lower backplane cover.

Replace the Alarm Interface Panel

Caution! Do not use a 2A AIP with a 5A fan-tray assembly; doing so causes a blown fuse on the AIP.

Caution! If any nodes in an Ethernet circuit are not using Software R4.0 or later, there is a risk of Ethernet traffic disruptions. Contact Cisco TAC at 1 800 553-2447 when prompted to do so in the procedure.

Note: Perform this procedure during a maintenance window. Resetting the active TCC2/TCC2P can cause a service disruption of less than 50 ms to OC-N or DS-N traffic. Resetting the active TCC2/TCC2P can cause a service disruption of 3 to 5 minutes on all Ethernet traffic due to spanning tree reconvergence if any nodes in the Ethernet circuit are not using Software R4.0 or later.

Caution! Do not perform this procedure on a node with live traffic. Hot-swapping the AIP can affect traffic and result in a loss of data. For assistance with AIP replacement contact Cisco TAC 1 800 553-2447.

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

This procedure replaces an existing AIP with a new AIP on an in-service node without affecting traffic. Ethernet circuits that traverse nodes with a software release prior to R4.0 is affected.

You need a #2 Phillips screwdriver.

1. Ensure that all nodes in the affected network are running the same software version before replacing the AIP and repairing circuits:
 1. In network view, click the **Maintenance > Software** tabs. The working software version for each node is listed in the Working Version column.
 2. If you need to upgrade the software on a node, refer to the release-specific software upgrade document for procedures. No hardware should be changed or circuit repair performed until after the software upgrade is complete. If you do not need to upgrade software or have completed the software upgrade, proceed to Step 2.
2. Record the MAC address of the old AIP:
 1. Log into the node where you are replacing the AIP. For login procedures, refer to the "Connect the PC and Log into the GUI" chapter in the *Cisco ONS 15454 Procedure Guide*.
 2. In node view, click the **Provisioning > Network > General** tabs.
 3. Record the MAC address.
3. Call Cisco TAC 1 800 553-2447 for assistance in replacing the AIP and maintaining the original MAC address.
4. Unscrew the five screws that hold the lower backplane cover in place.
5. Grip the lower backplane cover and gently pull it away from the backplane.
6. Unscrew the two screws that hold the AIP cover in place.
7. Grip the cover and gently pull away from the backplane.

Note: On the 15454-SA-HD (P/N: 800-24848), 15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1 (P/N: 800-07149) shelves the AIP cover is clear plastic. On the 15454-SA-ANSI shelf (P/N: 800-19857), the AIP cover is metal.
8. Grip the AIP and gently pull it away from the backplane.
9. Disconnect the fan-tray assembly power cable from the AIP.
10. Set the old AIP aside for return to Cisco.

Caution! The type of shelf the AIP resides in determines the version of AIP that should replace the failed AIP. The 15454-SA-ANSI shelf (P/N: 800-19857) and 15454-SA-HD (P/N: 800-24848) currently use the 5A AIP, (P/N: 73-7665-01). The 15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1 (P/N: 800-07149) shelves and earlier use the 2A AIP (P/N: 73-5262-01).

Caution! Do not put a 2A AIP (P/N: 73-5262-01) into a 15454-SA-ANSI (P/N: 800-19857) or 15454-SA-HD (P/N: 800-24848) shelf; doing so causes a blown fuse on the AIP.

11. Attach the fan-tray assembly power cable to the new AIP.
12. Place the new AIP on the backplane by plugging the panel into the backplane using the DIN connector.
13. Replace the AIP cover over the AIP and secure the cover with the two screws.
14. Replace the lower backplane cover and secure the cover with the five screws.
15. In node view, click the **Provisioning > Network** tabs.

Caution! Cisco recommends TCC2/TCC2P resets be performed in a maintenance window to avoid any potential service disruptions.

16. Reset the standby TCC2/TCC2P:

1. Right-click the standby TCC2/TCC2P and choose **Reset Card**.
 2. Click **Yes** in the Resetting Card dialog box. As the card resets, a loading (Ldg) indication appears on the card in CTC. The reset takes approximately five minutes. Do not perform any other steps until the reset is complete.
17. Reset the active TCC2/TCC2P:
1. Right click the active TCC2/TCC2P and choose **Reset Card**.
 2. Click **Yes** in the Resetting Card dialog box. As the card resets, a Ldg indication appears on the card in CTC. The reset takes approximately five minutes and CTC loses its connection with the node.
18. From the **File** drop-down list, choose **Exit** to exit the CTC session.
19. Log back into the node. At the Login dialog box, choose **(None)** from the Additional Nodes drop-down list.
20. Record the new MAC address:
1. In node view, click the **Provisioning > Network > General** tabs.
 2. Record the MAC address.
21. In node view, click the **Circuits** tab. Note that all circuits listed are PARTIAL.
22. In node view, choose **Repair Circuits** from the **Tools** drop-down list. The Circuit Repair dialog box appears.
23. Read the instructions in the Circuit Repair dialog box. If all the steps in the dialog box have been completed, click **Next**. Ensure that you have the old and new MAC addresses.
24. The Node MAC Addresses dialog box appears. Complete the following steps:
1. From the Node drop-down list, choose the name of the node where you replaced the AIP.
 2. In the Old MAC Address field, enter the old MAC address that was recorded in Step 2.
 3. Click **Next**.
25. The Repair Circuits dialog box appears. Read the information in the dialog box and click **Finish**.
- The CTC session freezes until all circuits are repaired. Circuit repair can take up to five minutes or more depending on the number of circuits provisioned on it.
When the circuit repair is complete, the Circuits Repaired dialog box appears.
26. Click **OK**.
27. In the node view of the new node, click the **Circuits** tab. Note that all circuits listed are DISCOVERED. If all circuits listed do not have a DISCOVERED status, call the Cisco TAC 1 800 553-2447 to open a Return Material Authorization (RMA).