Alarm Troubleshooting

This chapter gives a description, severity, and troubleshooting procedure for each commonly encountered Cisco DWDM alarm and condition. Table 1: Alarm Logical Object Type Definitions, on page 12 gives definitions of all DWDM alarm logical objects. For a comprehensive list of all conditions and instructions for using TL1 commands, refer to the TL1 Command Guide. An alarm troubleshooting procedure applies to both the Cisco Transport Controller (CTC) and TL1 version of that alarm.

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

For more information about alarm profiles, see the Manage Alarms chapter in the *Cisco ONS 15454 DWDM Procedure Guide*see the Alarm and TCA Monitoring and Management document.

Alarm Indexes

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

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

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

Logical Objects

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

Alarm profile list objects are defined in Table 1: Alarm Logical Object Type Definitions, on page 12.

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

Alarm Logical Objects

The table below lists all logical alarm objects used in this chapter.

Table 1: Alarm Logical Object Type Definitions

Logical Object	Definition
2R	Reshape and retransmit (used for transponder [TXP] cards).
AICI-AEP	Alarm Interface ControllerInternational/alarm expansion panel. A combination term that refers to this platform AIC-I card.
AICI-AIE	Alarm Interface Controller-International/Alarm Interface Extension. A combination term that refers to this platform's AIC-I card.
AIP	Alarm Interface Panel.
AOTS	Amplified optical transport section.
BITS	Building integrated timing supply incoming references (BITS-1, BITS-2).
BPLANE	The backplane.
ENVALRM	An environmental alarm port.
EQPT	A card, its physical objects, and its logical objects as they are located in any of the eight noncommon card slots. The EQPT object is used for alarms that refer to the card itself and all other objects on the card including ports, lines, synchronous transport signals (STS), and virtual tributaries (VT).
ESCON	Enterprise System Connection fiber optic technology, referring to the following TXP cards: TXP_MR_2.5G, TXPP_MR_2.5G, MXP_MR_2.5G, MXPP_MR_2.5G, AR-XP, AR-MXP, AR-XPE.

Logical Object	Definition
EXT-SREF	BITS outgoing references (SYNC-BITS1, SYNC-BITS2).
FAN	Fan-tray assembly.
FC	Fibre channel data transfer architecture, referring to the following muxponder (MXP) or TXP cards: MXP_MR_2.5G, MXPP_MR_2.5G, MXP_MR_10DME_C, MXP_MR_10DME_L, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, TXP_MR_10E_C, TXP_MR_10E_L, GE_XP, 10GE_XP, ADM-10G, and OTU2_XP, 40G-MXP-C, 40E-MXP, 10x10G-LC, WSE, 400G-XP-LC.
GE	Gigabit Ethernet, referring to the following MXP or TXP cards: MXP_MR_2.5G, MXPP_MR_2.5G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10G, TXP_MR_10E,TXP_MR_10E_C, TXP_MR_10E_L, MXP_MR_10DME_C, MXP_MR_10DME_L, GE-XP, 10GE-XP, ADM-10G, and OTU2_XP, 40G-MXP, 40E-MXP, 40G-TXP-C, 40G-TXP-E, 40E-TAR-XP, AR-MXP, AR-XPE, 10x10G, WSE, 100G-LC-C, 100G-CK-C, CFP-LC, MR-MXP, 100GS-CK-LC-C, 200G-CK-C, 400G-XP-LC.
ISC	Inter-service channel, referring to TXPP_MR_2.5G or TXP_MR_2.5G cards.
NE	The entire network element.
NE-SREF	The timing status of the NE.
OCH	The optical channel, referring to dense wavelength division multiplexing (DWDM) cards.
OCH-TERM	The optical channel termination node, referring to DWDM cards.
OCHNC-CONN	The optical channel network connection, referring to DWDM cards.
OMS	Optical multiplex section.
OSC-RING	Optical service channel ring.
OTS	Optical transport section.
PPM	Pluggable port module (PPM, also called SFP), referring to MXP and TXP cards.
PWR	Power equipment.
SHELF	The shelf assembly.
TRUNK	The card carrying the high-speed signal; referring to MXP or TXP cards.

Trouble Characterizations

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

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

Note For a description of CTC-view terminology, refer to the Cisco Transport Controller Operation chapter in the *Cisco ONS 15454 DWDM Reference Manual*CTC Enhancements, Operations, and Shortcuts.

Alarm Characteristics

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

Condition Characteristics

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

For a comprehensive list of all conditions, refer to the TL1 Command Guide. For information about transients, see Transient Conditions.

Note When an entity is put in the OOS,MT administrative state, the NCS suppresses all standing alarms on that entity. You can retrieve alarms and events on the Conditions tab. You can change this behavior for the LPBKFACILITY and LPBKTERMINAL alarms. To display these alarms on the Alarms tab, set the NODE.general.ReportLoopbackConditionsOnPortsInOOS-MT to TRUE on the NE Defaults tab.

Severity

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

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

alarm occurs upstream. These conditions do not in themselves require troubleshooting, but are to be expected in the presence of primary alarms.

Severities can be customized for an entire network or for single nodes, from the network level down to the port level by changing or downloading customized alarm profiles. These custom severities are subject to the standard severity-demoting rules given in Telcordia GR-474-CORE. Procedures for customizing alarm severities are located in the Manage Alarms chapter in the *Cisco ONS 15454 DWDM Procedure Guide*Alarm and TCA Monitoring and Management document.

Service Effect

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

State

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

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

Safety Summary

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

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

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

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

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

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

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

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

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

Trouble-Clearing Procedures

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

Note When you check the status of alarms for cards, ensure that the alarm filter icon in the lower right corner of the GUI is not indented. If it is, click it to turn it off. When you are done checking for alarms, you can click the alarm filter icon again to turn filtering back on.

Note When checking alarms, ensure that alarm suppression is not enabled on the card or port.

Note When an entity is put in the OOS,MT administrative state, the system suppresses all standing alarms on that entity. All alarms and events appear on the Conditions tab. You can change this behavior for the LPBKFACILITY and LPBKTERMINAL alarms. To display these alarms on the Alarms tab, set the NODE.general.ReportLoopbackConditionsOnPortsInOOS-MT to TRUE on the NE Defaults tab.

ACT-SOFT-VERIF-FAIL

On the Active Controller card, the Alarm severity is Critical (CR) and Service Affecting (SA).

On the Standby Controller card, the Alarm severity is Minor (MN) and Non-Service affecting (NSA).

Logical Object: EQPT

The Active Volume Software Signature Verification Failed (ACT-SOFT-VERIF-FAIL) alarm occurs under the following conditions:

- The working software running on the control card in the NCS system is tampered with or the working software running on the system did not originate from Cisco.
- Problem present in the software stored in the protect or standby card.

Clear the ACT-SOFT-VERIF-FAIL Alarm

Procedure

Step 1 To clear the ACT-SOFT-VERIF-FAIL alarm, download the software on the protect (standby) flash.

Step 2 Activate the protect (standby) flash.

Step 3 After the control card is activated, download the software on the standby partition or the standby code volume on the protect flash.

If the troubleshooting procedure does not clear the alarm, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html or call the Cisco Technical Assistance Center (1 800 553-2447) to report the problem.

AIS

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

Logical Objects: BITS, FUDC, MSUDC

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

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

Clear the AIS Condition

Procedure

Step 1 Determine whether there are alarms such as LOS on the upstream nodes and equipment or if there are OOS,MT (or Locked,maintenance), or OOS,DSBLD (or Locked,disabled) ports.

Step 2 Clear the upstream alarms using the applicable procedures in this chapter.

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

AIS-L

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

logical Objects: OCN, TRUNK

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

This condition can also be raised in conjunction with the TIM-S alarm if AIS-L is enabled.

Clear the AIS-L Condition

Procedure

Complete the Clear the AIS Condition, on page 18 procedure.

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

AIS-P

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

Logical Object: STSMON, STSTRM

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

Clear the AIS-P Condition

Procedure

Complete the Clear the AIS Condition, on page 18 procedure.

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

ALS

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

Logical Objects: 2R, AOTS, ESCON, FC, GE, ISC, OCN, TRUNK

The Automatic Laser Shutdown (ALS) condition on the amplifier cards indicate that the ALS safety feature on the card port is switched ON. This condition is accompanied by a corresponding LOS alarm in the reverse direction of the same port.

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

ALS-DISABLED

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

Logical Object: EQPT

The Automatic Laser Shutdown (ALS) condition occurs when Amplifier card ALS is changed to Disabled from any other state (such as Enabled) by user command.

Clear the ALS-DISABLED Condition

Procedure

Step 1 In node view (single-shelf mode) or shelf view (multishelf mode), double-click the OPT-BST, or OPT-PRE, OPT-AMP-C, or OMP-AMP-17-C card to display the card view.

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

Step 3 In the ALS Mode column, change the entry from Disabled to your required state.

AMPLI-INIT

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

Logical Object: AOTS

The Amplifier Initialized condition occurs when an amplifier card is not able to calculate gain. This condition typically accompanies the APC-DISABLED , on page 20 alarm.

Clear the AMPLI-INIT Condition

Procedure

Step 1 Complete the Delete a Circuit, on page 314 procedure on the most recently created circuit.

Step 2 Recreate this circuit using the procedures in the Configuration guide.

APC-CORR-SKIPPED

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

Logical Objects: AOTS, OCH, OMS, OTS

The Automatic Power Control (APC) Correction Skipped condition occurs when the actual power level of a channel exceeds the expected setting by 3 dBm or more. APC compares actual power levels with previous power levels every hour or after any channel allocation is performed. If the power difference to be compensated by APC exceeds the range of + 3 dBm or 3 dBm compared with the previous value set, APC is designed not to correct the level and the APC-CORR-SKIPPED condition is raised.

The APC Correction Skipped alarm strongly limits network management (for example, a new circuit cannot be turned into IS). The Force APC Correction button helps to restore normal conditions by clearing the APC Correction Skipped alarm.

APC-DISABLED

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

Logical Objects: NE, SHELF, AOTS, OTS, OMS, OCH, EQPT

The APC Disabled alarm occurs when the information related to the number of channels is not reliable. The condition can occur when any of the following related alarms also occur: the EQPT alarm, the IMPROPRMVL alarm, or the MEA (EQPT)alarm. If the condition occurs with the creation of the first circuit, delete and recreate the circuit.

APC Disabled alarm is raised under the following conditions:

- When APC is manually disabled in a domain to prevent unexpected power regulations during maintenance or troubleshooting.
- When an abnormal event impacting optical regulation occurs.
- When an EQPT, MEA or IMPROPRMVL alarm is raised by any unit in a network.
- When gain or power degrade occurs or when the Power Fail alarm is raised by the output port of any amplifier in the network.
- When a VOA degrade or a VOA Fail alarm is raised by any unit in a network.
- When signalling protocol detects that one of the APC instances in a network is no longer reachable.
- When all nodes in a network do not belong to metro core.

Note The MEA and IMPROPRMVL alarms does not disable APC when raised on MXP/TXP cards.

Clear the APC-DISABLED Alarm

Procedure

Step 1 Complete the appropriate procedure to clear the main alarm:

- Clear the EQPT Alarm
- Clear the IMPROPRMVL Alarm
- Clear the MEA (EQPT) Alarm

Step 2 If the condition does not clear, .

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

APC-END

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

Logical Object: NE

The APC Terminated on Manual Request condition is raised when APC terminates after it is manually launched. APC-END is an informational condition that is raised and cleared spontaneously by the system. It is visible only by retrieving it in the Conditions or History tabs.

Note APC-END is an informational condition and does not require troubleshooting.

APC-OUT-OF-RANGE

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

Logical Objects: AOTS, OCH, OMS, OTS

The APC-OUT-OF-RANGE condition is raised on amplifier cards when the requested gain or attenuation setpoint cannot be set because it exceeds the port parameter range. For example, this condition is raised when APC attempts to set the OPT-BST gain higher than 20 dBm (the card maximum setpoint) or to set the attenuation on the express VOA lower than 0 dBm (its minimum setpoint).

Note A common cause of an amplifier trying to attain a value higher than the maximum setpoint or an attenuator trying to attain a value lower than the minimum setpoint is the low input power.

Clear the APC-OUT-OF-RANGE Alarm

Procedure

There are various root causes for the APC-OUT-OF-RANGE condition. To determine the correct root cause, complete the network-level troubleshooting procedures and node level problems.

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

APC-WRONG-GAIN

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

Logical Object: AOTS

The APC-WRONG-GAIN condition is raised on the amplifier card, when the actual gain of the card (17dB) does not match the expected gain calculated by APC. There is a margin of +1 or -1 dB before the condition is raised.

Note The APC-WRONG-GAIN condition indicates a system issue and not the card problem.

Clear the APC-WRONG-GAIN Alarm

The condition can be cleared by recovering the power at the input port:

Procedure

Step 1 Check the incoming fiber connection and clean them.

Step 2 Check the regulation points (VOA and amplifiers) along the optical path upstream of the card.

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

APSB

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

Logical Object: OCN, STMN

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

Clear the APSB Alarm

Procedure

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

Step 2 If the alarm does not clear and the overhead shows inconsistent or invalid K bytes, you could need to replace the upstream cards for protection switching to operate properly. Complete the Physically Replace a Card, on page 313 procedure.

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

APSCM

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

Logical Object: OCN, STMN

The APS Channel Mismatch alarm occurs when the NCS expects a working channel but receives a protect channel. In many cases, the working and protect channels are crossed and the protect channel is active. If the fibers are crossed and the working line is active, the alarm does not occur. The APSCM alarm occurs only on the NCS when bidirectional protection is used on OC-N cards in a 1+1 protection group configuration. The APSCM alarm does not occur in an optimized 1+1 protection configuration.

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

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

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

Clear the APSCM Alarm

Before you begin

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

Procedure

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

Step 2 If the fibers are correctly connected, verify that the protection-card channel fibers are physically connected directly to the adjoining node protection-card channel fibers.

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

APSIMP

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

Logical Object: OCN, STMN

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

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

Clear the APSIMP Alarm

Procedure

Step 1 Check the configuration of the other node in the 1+1 protection group. If the far end is not configured for 1+1 protection, create the group.

Step 2 If the other end of the group is properly configured or the alarm does not clear after you have provisioned the group correctly, verify that the working ports and protect ports are cabled correctly.

Step 3 Ensure that both protect ports are configured for SONET.

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

APSMM

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

SONET Logical Object: STMN

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

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

Clear the APSMM Alarm

Procedure

Step 1 For the reporting NCS, display node view and verify the protection scheme provisioning:

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

b) Click the 1+1 protection group configured for the OC-N cards.

The chosen protection group is the protection group optically connected (with data communications channel, or DCC, connectivity) to the far end.

c) Click **Edit**.

d) Record whether the Bidirectional Switching check box is checked.

Step 2 Click **OK** in the Edit Protection Group dialog box.

Step 3 Log into the far-end node and verify that the OC-N 1+1 protection group is provisioned.

Step 4 Verify that the Bidirectional Switching check box matches the checked or unchecked condition of the box recorded in Step 1, on page 26. If not, change it to match.

Step 5 Click **Apply.**

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

APS-NO-RESPONSE

Default Severity: Minor (MN), Service Affecting (SA)

Logical Object: ODU

The APS-NO-RESPONSE alarm is raised when the requested or bridge signals of a SNC protection do not match.

Clear the APS-NO-RESPONSE Alarm

Procedure

Verify that the requested and bridge signals of SNC protection match.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

APS-PROV-MISM

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

Logical Object: ODU

The APS-PROV-MISM alarm is raised when the SNC protection types on the near end and far end near are incompatible.

Clear the APS-PROV-MISM Alarm

Procedure

Verify that the near end and far end SNC protection types match.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

AS-CMD

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

Logical Objects: 2R, AOTS, BPLANE, EQPT, ESCON, FC, GE, ISC, NE, OCH, OCN/STMN, OMS, OTS, PPM, PWR, SHELF, TRUNK

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

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

Note For more information about suppressing alarms, refer to the Alarm and TCA Monitoring and Management document.

Note This condition is not raised for multiservice transport platform (MSTP) cards such as amplifiers, multiplexers, or demultiplexers.

Clear the AS-CMD Condition

Procedure

Step 1 For all nodes, in node view (single-shelf mode) or shelf view (multishelf mode),,click the **Conditions** tab.

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

- If the condition is reported against a slot and card, alarms were either suppressed for the entire card or for one of the ports. Note the slot number and continue with Step 3, on page 28.
- If the condition is reported against the backplane, go to Step 7, on page 28.
- If the condition is reported against the NE object, go to Step 8, on page 28.

Step 3 Determine whether alarms are suppressed for a port and if so, raise the suppressed alarms:

a) Double-click the card to open the card view.

b) Click the **Provisioning** > **Alarm Profiles** > **Alarm Behavior** tabs and complete one of the following substeps:

- If the Suppress Alarms column check box is checked for a port row, deselect it and click **Apply.**
- If the Suppress Alarms column check box is not checked for a port row, from the View menu choose **Go to Previous View**.

Step 4 If the AS-CMD condition is reported for a card and not an individual port, in node view (single-shelf mode) or shelf view (multishelf mode), click the **Provisioning** > **Alarm Profiles** > **Alarm Behavior** tabs.

Step 5 Locate the row number for the reported card slot.

Step 6 Click the **Suppress Alarms** column check box to deselect the option for the card row.

Step 7 If the condition is reported for the backplane, the alarms are suppressed for cards that are not in the optical or electrical slots. To clear the alarm, complete the following steps:

a) Click the **Provisioning** > **Alarm Profiles** > **Alarm Behavior** tabs.

b) In the backplane row, uncheck the **Suppress Alarms** column check box.

c) Click **Apply.**

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

a) In node view (single-shelf mode) or shelf view (multishelf mode), click the **Provisioning** > **Alarm Profiles** > **Alarm Behavior** tabs if you have not already done so.

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

c) Click **Apply.**

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

AS-MT

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

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

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

While provisioning traffic between two MXP-MR-10DME, MXP-MR-2.5G, or MXPP-MR-2.5G cards, putting the trunk port (09) of the card OOS-MT (initially IS) results in the AS-MT alarm being reported on both trunk and client port. This is because all the GFP interfaces derive their state from the trunk state if the trunk is not IS-NR. If the Trunk port state is IS-NR, then all the GFP interfaces derive their state from the corresponding client port. When the trunk is moved to AS-MT, which is not IS, the GFP of the client port also moves to the AS-MT state. The FAC of the client does not change state.

Clear the AS-MT Condition

Procedure

Complete the Clear an MXP, TXP, GE-XP, 10GE-XP, and ADM-10G Card Loopback Circuit, on page 315 procedure.

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

AU-AIS

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

Logical Object: VCMON-HP, VCTRM-HP

An AU AIS condition applies to the administration unit, which consists of the virtual container (VC) capacity and pointer bytes (H1, H2, and H3) in the SDH frame.

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

Clear the AU-AIS Condition

Procedure

Step 1 Complete the Clear the AIS Condition, on page 18 procedure.

Step 2 If the condition does not clear, complete the Clear the APSB Alarm, on page 23 procedure.

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

AU-LOP

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

Logical Objects: VCMON-HP, VCTRM-HP

An AU-LOP alarm indicates that the administration unit's SDH high-order path overhead section has detected a path loss. AU-LOP occurs when there is a mismatch between the expected and provisioned circuit size. An AU-LOP is raised for the TXP card if a port is configured for an SDH signal but does not receive an SDH signal. (This information is contained in the H1 byte bits 5 and 6.)

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 AU-LOP Alarm

Procedure

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

Step 2 Verify that the correct circuit size is listed in the Size column. If the size is different from what is expected, such as a VC4-4c instead of a VC4, this causes the alarm.

Step 3 If you have been monitoring the circuit with optical test equipment, a mismatch between the provisioned circuit size and the size expected by the test set can cause this alarm. Ensure that the test set monitoring is set up for the same size as the circuit provisioning. For specific procedures to use the test set equipment, consult the manufacturer.

Step 4 If you have not been using a test set, or if the test set is correctly set up, the error is in the provisioned CTC circuit size. Complete the Delete a Circuit, on page 314 procedure.

Step 5 Recreate the circuit for the correct size.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

AUTH-EC

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

Logical Objects: OTU

The Authentication Error Count (AUTH-EC) alarm is raised when the authentication error count crosses the authentication threshold.

Clear the AUTH-EC Alarm

Procedure

This alarm is cleared automatically when the authentication error count becomes less then authentication error threshold.

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

AUTO-SENSE

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

Logical Object: PPM

The AUTO-SENSE alarm is raised when the port detects an incoming signal on the port. The alarm clears automatically after detecting the signal.

AUTO-SENSE-DSBLD

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

Logical Object: PPM

The AUTO-SENSE-DSBLD alarm is raised when the port is configured as an AUTO port, but auto-sensing is disabled.

Clear the AUTO-SENSE-DSBLD Alarm

Procedure

Clear the AUTO-SENSE-DSBLD alarm with either of these procedures:

a) Enable auto-sensing.

1. Login to CTC.
2. In node view (single-shelf mode) or shelf view (multishelf view), double-click the AR_MXP or AR_XP card where you want to enable auto-sensing.
3. Click the **Provisioning** > **Line** > **Auto Ports** tabs.
4. Check the **Auto Sensing** check box.

b) Delete the auto port.

1. Login to CTC.
2. In node view (single-shelf mode) or shelf view (multishelf view), double-click the AR_MXP or AR_XP card where you want to delete the auto port.
3. Click the **Provisioning** > **Pluggable Port Modules** tabs.
4. In the Pluggable Port Modules area, select the auto PPM that you want to delete and click **Delete**.
5. Click **Yes**. The auto port is deleted.

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

AUTORESET

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

Logical Object: EQPT

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

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

Clear the AUTORESET Alarm

Procedure

Step 1 Determine whether there are additional alarms that could have triggered an automatic reset. If there are, troubleshoot these alarms using the applicable section of this chapter.

Step 2 If the card automatically resets more than once a month with no apparent cause, complete the Physically Replace a Card, on page 313 procedure.

Warning **High-performance devices on this card can get hot during operation. To remove the card, hold it by the faceplate and bottom edge. Allow the card to cool before touching any other part of it or before placing it in an antistatic bag.** Statement 201

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

AUTOSW-AIS

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

Logical Object: STSMON, VT-MON

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

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

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

Clear the AUTOSW-AIS Condition

Procedure

Complete the Clear the AIS Condition, on page 18 procedure.

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

AUTOSW-AIS-SNCP

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

Logical Object: VCMON-HP, VCMON-LP

The Automatic UPSR Switch Caused by an AIS condition indicates that automatic UPSR protection switching occurred because of the TU-AIS condition. If the UPSR ring is configured for revertive switching, it switches back to the working path after the fault clears. The AUTOSW-AIS-UPSR clears when you clear the primary alarm on the upstream node.

Note This condition is only reported if the SNCP is set up for revertive switching.

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

Clear the AUTOSW-AIS-UPSR Condition

Procedure

Complete the Clear the AIS Condition, on page 18 procedure.

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

AUTOSW-LOP (STSMON)

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

Logical Object: STSMON

The Automatic Path Protection Switch Caused by LOP condition for the STS monitor (STSMON) indicates that automatic path protection switching occurred because of the LOP-P , on page 155 alarm. If the path protection is configured for revertive switching, it reverts to the working path after the fault clears.

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

Clear the AUTOSW-LOP (STSMON) Condition

Procedure

Complete the Clear the LOP-P Alarm, on page 156 procedure.

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

AUTOSW-LOP-SNCP

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

Logical Object: VCMON-HP, VCMON-LP

An Automatic UPSR Switch Caused by LOP alarm indicates that an automatic UPSR protection switching occurred because of the AU-LOP , on page 30. If the UPSR ring is configured for revertive switching, it switches back to the working path after the fault clears.

Note This condition is only reported if the SNCP is set up for revertive switching.

Clear the AUTOSW-LOP-SNCP Alarm

Procedure

Complete the Clear the AU-LOP Alarm , on page 30 procedure.

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

AUTOSW-PDI

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

Logical Object: STSMON, VT-MON

The Automatic Path Protection Switch Caused by Payload Defect Indication (PDI) condition indicates that automatic path protection switching occurred because of a PDI-P , on page 230 alarm. If the path protection is configured for revertive switching, it reverts to the working path after the fault clears.

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

Clear the AUTOSW-PDI Condition

Procedure

Complete the Clear the PDI-P Condition, on page 231 procedure.

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

AUTOSW-PDI-SNCP

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

Logical Object: VCMON-HP, VCMON-LP

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

Note This condition is only reported if the SNCP is set up for revertive switching.

Clear the AUTOSW-PDI-SNCP Condition

Procedure

Complete the Clear the PDI-P Condition, on page 231 procedure.

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

AUTOSW-SDBER

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

Logical Object: STSMON, VT-MON

The Automatic Path Protection Switch Caused by Signal Degrade Bit Error Rate (SDBER) condition indicates that a SD-P , on page 259 condition caused automatic path protection switching to occur. If the path protection is configured for revertive switching, the path protection reverts to the working path when the SD-P is resolved.

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

Clear the AUTOSW-SDBER Condition

Procedure

Complete the Clear the SD-P Condition, on page 259 procedure.

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

AUTOSW-SDBER-SNCP

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

Logical Object: VCMON-HP, VCMON-LP

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

Note This condition is only reported if the SNCP is set up for revertive switching.

Clear the AUTOSW-SDBER-SNCP Condition

Procedure

Complete the Clear the SD (TRUNK) Condition, on page 257 procedure.

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

AUTOSW-SFBER

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

Logical Object: STSMON, VT-MON

The Automatic USPR Switch Caused by Signal Fail Bit Error Rate (SFBER) condition indicates that a SF-P , on page 263 condition caused automatic path protection switching to occur. If the path protection is configured for revertive switching, the path protection reverts to the working path when the SF-P is resolved.

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

Clear the AUTOSW-SFBER Condition

Procedure

Complete the Clear the SF-P Condition, on page 263 procedure.

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

AUTOSW-SFBER-SNCP

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

Logical Object: VCMON-HP, VCMON-LP

The Automatic UPSR Switch Caused by Signal Fail Bit Error Rate (SFBER) condition indicates that a signal fail caused automatic UPSR protection switching to occur. If the UPSR ring is configured for revertive switching, it reverts to the working path when the SF is resolved.

Note This condition is only reported if the SNCP is set up for revertive switching.

Clear the AUTOSW-SFBER-SNCP Condition

Procedure

Complete the Clear the SF (TRUNK) Condition, on page 262 procedure.

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

AUTOSW-UNEQ (STSMON)

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

Logical Object: STSMON

The Automatic Path Protection Switch Caused by Unequipped condition indicates that an UNEQ-P , on page 290, caused automatic path protection switching to occur. If the path protection is configured for revertive switching, it reverts to the working path after the fault clears.

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

Clear the AUTOSW-UNEQ (STSMON) Condition

Procedure

Complete the Clear the UNEQ-P Alarm, on page 290 procedure.

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

AUTOSW-UNEQ-SNCP (VCMON-HP)

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

Logical Object: VCMON-HP

The Automatic UPSR Switch Caused by an Unequipped condition indicates that an HP-UNEQ alarm caused automatic UPSR protection switching to occur (see the HP-UNEQ , on page 121). If the UPSR ring is configured for revertive switching, it reverts to the working path after the fault clears.

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

Warning **Class 1M laser radiation when open. Do not view directly with optical instruments.** Statement 1053

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

Clear the AUTOSW-UNEQ-SNCP (VCMON-HP) Condition

Procedure

Complete the Clear the HP-UNEQ Alarm, on page 121 procedure.

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

AWG-DEG

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

Logical Object: OTS

The Arrayed Waveguide Gratings (AWG) Degrade alarm occurs when a card heater-control circuit degrades. The heat variance can cause slight wavelength drift.

Clear the AWG-DEG Alarm

Procedure

For the alarmed card, complete the Physically Replace a Card, on page 313 procedure during the next maintenance period.

Warning **High-performance devices on this card can get hot during operation. To remove the card, hold it by the faceplate and bottom edge. Allow the card to cool before touching any other part of it or before placing it in an antistatic bag.** Statement 201

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

AWG-FAIL

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

Logical Object: OTS

The AWG Failure alarm occurs when a card heater-control circuit completely fails. The circuit failure disables wavelength transmission. The card must be replaced to restore traffic.

Clear the AWG-FAIL Alarm

Procedure

For the alarmed card, complete the Physically Replace a Card, on page 313 procedure during the next maintenance period.

Warning **High-performance devices on this card can get hot during operation. To remove the card, hold it by the faceplate and bottom edge. Allow the card to cool before touching any other part of it or before placing it in an antistatic bag.** Statement 201

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

AWG-OVERTEMP

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

Logical Object: OTS

The AWG Over Temperature alarm is raised if a card having an AWG-FAIL alarm is not replaced and its heater-control circuit temperature exceeds 212 degrees F (100 degrees C). The card goes into protect mode and the heater is disabled.

Clear the AWG-OVERTEMP Alarm

Procedure

Complete the Clear the AWG-FAIL Alarm, on page 41 procedure.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

AWG-WARM-UP

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

Logical Object: OTS

The AWG Warm-Up condition occurs when a card heater-control circuit is attaining its operating temperature during startup. The condition lasts approximately 10 minutes but can vary somewhat from this period due to environmental temperature.

Note AWG-WARM-UP is an informational condition and does not require troubleshooting.

BAD-DB-DETECTED

Default Severity: Critical (CR)

Logical Object: NE

The Bad Database Detected alarm is raised when the database load fails due to the following:

- Soft-reset of Active Controller
- Software Upgrade
- Database Restore

A pop-up error message might appear while navigating to card view and shelf view.

Note Do not use the reboot command in the console when the BAD-DB-DETECTED alarm is raised.

Clear the BAD-DB-DETECTED Alarm

Procedure

Restore any known good database.

(or)

Reset NE to the factory default settings.

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

BAT-FAIL

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

Logical Object: PWR

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

Note FAN-FAIL alarm is not raised if BAT-FAIL alarm appears on the power module.

Clear the BAT-FAIL Alarm

Procedure

Step 1 At the site, determine which battery is not present or operational.

Step 2 Remove the power cable from the faulty supply. Reverse the power cable installation procedure.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

BP-LPBKFACILITY

Default Severity: Not alarmed (NA)

Logical Object: EQPT

The BP-LPBKFACILITY alarm is raised when the backplane facility loopback is configured on the 100G-LC-C or 10x10G-LC card.

Clear the BP-LPBKFACILTIY Alarm

Remove the backplane facility loopback on the 100G-LC-C or 10x10G-LC card.

Procedure

Step 1 Log in to a node on the network.

Step 2 In node view (single-shelf mode) or shelf view (multishelf mode), double-click the 100G-LC-C or 10x10G-LC card in CTC to open the card view.

Step 3 Click the **Maintenance** > **Card** tabs.

Step 4 Click on the card port that is in IS (or Unlocked) state in the Admin State column, and change the state to OOS,MT.

Step 5 Click **Apply**.

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

BP-LPBKTERMINAL

Default Severity: Not alarmed (NA)

Logical Object: EQPT

The BP-LPBKTERMINAL alarm is raised when the backplane terminal loopback is configured on the 100G-LC-C or 10x10G-LC card.

Clear the BP-LPBKTERMINAL Alarm

Remove the backplane terminal loopback on the 100G-LC-C or 10x10G-LC card.

Procedure

Step 1 Log in to a node on the network.

Step 2 In node view (single-shelf mode) or shelf view (multishelf mode), double-click the 100G-LC-C or 10x10G-LC card in CTC to open the card view.

Step 3 Click the **Maintenance** > **Card** tabs.

Step 4 Click on the card port that is in IS (or Unlocked) state in the Admin State column, and change the state to OOS,MT.

Step 5 Click **Apply**.

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

CARLOSS (EQPT)

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

Logical Object: EQPT

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

On MXP_2.5G_10G cards, CARLOSS is also raised against trunk ports when ITU-T G.709 encapsulation is turned off.

Note The multishelf management (MSM) port is turning Yellow even when Carloss alarm is not present on external connection unit (ECU) of M6 Chassis, this is a known behaviour.

The CARLOSS alarm is also raised against multishelf management (MSM) ports of the external connection unit (ECU) when the connection to the shelf subtending the node is improper.

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 CARLOSS alarms are not reported on M15-ECU for ONS-SI-100-LX10 and ONS-SE-100-LX1 pluggables under the following conditions.

- When the pluggables are plugged-in for the first time and there is no fiber connection on their ports.
- When the controller switch-over happens or when the cable connects or disconnects.

Clear the CARLOSS (EQPT) Alarm

Procedure

Step 1 If the reporting card is an MXP or TXP card in an NCS node, verify the data rate configured on the PPM (also called SFP):

a) In node view (single-shelf mode) or shelf view (multishelf mode), double-click the reporting MXP or TXP card.
b) Click the **Provisioning** > **Pluggable Port Modules** tabs.
c) View the Pluggable Port Modules area port listing in the **Actual Equipment Type** column and compare this with the contents of the Selected PPM area Rate column for the MXP or TXP multirate port.
d) If the rate does not match the actual equipment, you must delete and recreate the selected PPM. Select the PPM (SFP), click **Delete**, then click **Create** and choose the correct rate for the port rate.

Note For more information about provisioning PPMs (SFPs) and their specifications, refer to the Installing the GBIC, SFP, SFP+, and XFP Optical Modules in Cisco ONS Platforms document.

Step 2 If the reporting card is an OC-N/STM-N card, verify connectivity by pinging the system that is reporting the alarm.

Step 3 If the ping is successful, it demonstrates that an active TCP/IP connection exists. Restart CTC:

a) Exit from CTC.
b) Reopen the browser.
c) Log into CTC.

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

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

Step 5 Verify that the optical LAN cable is properly connected and attached to the correct port.

Step 6 If the fiber cable is properly connected and attached to the port, verify that the cable connects the card to another Ethernet device and is not misconnected to an OC-N/STM-N card.

Step 7 If you are unable to establish connectivity, replace the fiber cable with a new known-good cable.

Step 8 If you are unable to establish connectivity, perform standard network or LAN diagnostics. For example, trace the IP route, verify cable continuity, and troubleshoot any routers between the node and CTC. To verify cable continuity, follow site practices.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

CARLOSS (FC)

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

Logical Object: FC

The Carrier Loss for Fibre Channel (FC) alarm occurs on the client port of MXP_MR_2.5G, MXPP_MR_2.5G, MXP_MR_10DME_C, MXP_MR_10DME_L, supporting 1-Gb Fibre Channel (FC1G), 2-Gb FC (FC2G), or 10Gb Fiber Channel (10G Fiber Channel) traffic. The loss can be due to a misconfiguration, fiber cut, or client equipment problem.

Clear the CARLOSS (FC) Alarm

Procedure

Complete the Clear the CARLOSS (GE) Alarm, on page 48 procedure.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

CARLOSS (GE)

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

Logical Object: GE

The Carrier Loss for Gigabit Ethernet (GE) alarm occurs on the client port of MXP_MR_2.5G, MXPP_MR_2.5G, MXP_MR_10DME_C, MXP_MR_10DME_L, GE-XP, 10GE-XP, or ADM-10G cards supporting 1-Gbps or 10-Gbps traffic. The loss can be due to a misconfiguration, fiber cut, or client equipment problem.

Clear the CARLOSS (GE) Alarm

Procedure

Step 1 Ensure that the GE client is correctly configured:

a) Click the **Provisioning** > **Pluggable Port Modules** tabs.

b) View the Pluggable Port Modules area port listing in the **Actual Equipment Type** column and compare this with the client equipment. If no PPM (SFP) is provisioned, refer to the Turn Up a Node chapter. PPM (SFP) specifications are listed in the Installing the GBIC, SFP, SFP+, and XFP Optical Modules in Cisco ONS Platforms document.

c) If a PPM (SFP) has been created, view the contents of the Selected PPM area Rate column for the MXP or TXP MR card and compare this rate with the client equipment data rate. In this case, the rate should be ONE_GE or 10G Ethernet. If the PPM (SFP) rate is differently provisioned, select the PPM (SFP), click **Delete**, then click **Create** and choose the correct rate for the equipment type.

Note For information about installing and provisioning PPMs (SFPs), refer to the Installing the GBIC, SFP, SFP+, and XFP Optical Modules in Cisco ONS Platforms document.

Step 2 If there is no PPM (SFP) misprovisioning, check for a fiber cut. An LOS alarm would also be present. If there is an alarm, complete the Clear the LOS (OCN/STMN) Alarm procedure located in Chapter 2, Alarm Troubleshooting, of the Troubleshooting guide.

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

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

CARLOSS (ISC)

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

Logical Object: ISC

The Carrier Loss for Inter-Service Channel (ISC) alarm occurs on:

- The client port of MXP_MR_2.5G, or MXPP_MR_2.5G card supporting ISC traffic.
- MSM ports of an NCS NC shelf.
- MSM ports of an NCS SS shelf.

The loss can be due to a misconfiguration, fiber cut, or client equipment problem.

Clear the CARLOSS (ISC) Alarm

Procedure

Perform the following to clear the CARLOSS (ISC) alarm:

- For TXP/MXP cards—Complete the Clear the CARLOSS (GE) Alarm, on page 48 procedure.
- For MS-ISC cards—Suppress the alarm.
  - Check the **Suppress Alarms** check box and click **Apply** in the **Provisioning > Alarm Profiles > Alarm Behavior** tab in the card view of CTC.
- For NCS NC shelf or NCS SS shelf—Suppress the alarm.
  - Check the **Suppress Alarms** check box and click **Apply** in the **Provisioning > Alarm Profiles > ECU MS Ports Alarm Suppression** tab in the shelf view of CTC.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

CARLOSS (TRUNK)

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

Logical Object: TRUNK

A Carrier Loss alarm is raised on the optical Trunk-RX port of MXP_MR_2.5G, and MXPP_MR_2.5G when the Ethernet payload is lost. This alarm only occurs when ITU-T G.709 encapsulation is disabled.

Clear the CARLOSS (TRUNK) Alarm

Procedure

Step 1 Check for any upstream equipment failures:

- Verify that the far-end TXP or MXP is generating the signal to be received by the alarmed card.
- Verify that the Trunk-Tx port is not reporting any performance monitoring (PM) problems.
- Verify that the Client-Rx port is not reporting any PM problems that could cause the CARLOSS in this card.

Step 2 If there is no cause upstream, verify cabling continuity from the transmitting port of the DWDM card ( ) connected to the TXP receiving port reporting this alarm.

Step 3 If a patch panel is used, ensure that the LC-LC adapter managing the connection is in good working order.

Step 4 If the continuity is good, clean the fiber according to site practice. If none exists, complete the fiber cleaning procedure in the Maintain the Node chapter in the *Cisco ONS 15454 DWDM Procedure Guide*Manage the Node document.

Step 5 If the signal is valid, ensure that the transmit and receive outputs from the patch panel to your equipment are properly connected (that is, the correct wavelength is coming from the patch panel). For more information about fiber connections and terminations, refer to the Turn Up a Node chapter.

Step 6 If the correct port is in service but the alarm has not cleared, use an optical test set to confirm that a valid signal exists on the input port of the alarmed TXP. For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving card as possible.

Step 7 If the alarm does not clear, complete the Physically Replace a Card, on page 313 procedure for the reporting card.

Warning **High-performance devices on this card can get hot during operation. To remove the card, hold it by the faceplate and bottom edge. Allow the card to cool before touching any other part of it or before placing it in an antistatic bag.** Statement 201

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

CASETEMP-DEG

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

Logical Object: AOTS

Note For specific temperature and environmental information about each DWDM card, refer to the Hardware Specifications appendix in the *Cisco ONS 15454 DWDM Reference Manual*Hardware Specifications document.

Clear the CASETEMP-DEG Alarm

Procedure

Step 1 Determine whether the air filter needs replacement. Complete the Inspect, Clean, and Replace the Air Filter, on page 316 procedure.

Step 2 If the filter is clean, complete the Remove and Reinsert a Fan-Tray Assembly, on page 318 procedure.

Step 3 If the fan does not run or the alarm persists, complete the Replace the Fan-Tray Assembly, on page 318 procedure. The fan should run immediately when correctly inserted.

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

CD

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

Logical Object: Trunk port (dir RX)

The Chromatic Dispersion value alarm is raised when the device experiences CD in excess.

Clear the CD Alarm

Procedure

Switch the traffic on a lower CD link.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of toll-free Technical Support numbers for your country in order to report a Service-Affecting (SA) problem.

CFM-CONFIG-ERROR

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

Logical Objects: ETH

The Connectivity Fault Management Configuration Error (CFM-CONFIG-ERROR) alarm is raised on GE_XP or 10GE_XP cards under the following scenarios:

- A mismatch is present in the continuity check (CC) timer between two maintenance end points.
- A mismatch exists between the maintenance association and domain name.
- A similar maintenance point (MP) ID exists on both the maintenance end points.

Clear the CFM-CONFIG-ERROR Condition

Procedure

Step 1 In node view, double-click the GE_XP or 10GE_XP card to open the card view.

Step 2 Verify if the CC Timer settings on both the maintenance end points of the card are the same. To set or view the CC timer values do the following:

a) In card view, click the Provisioning > CFM > Configuration > Global Settings tabs.
b) Select or note down the CC Timer value.
c) Repeat step a and b on the other end of the maintenance end point.
d) Set the CC Timer value that is same as the value set at the other maintenance end point.

Step 3 Verify the maintenance association and the domain name are the same. Do the following:

a) In card view, click the **Provisioning** > **CFM** > **Configuration** > **MA Profiles** tabs.
b) Enter or note down the maintenance profile name.
c) In card view, click the **Provisioning** > **CFM** > **Configuration** > **Domain Profiles** tabs.
d) Enter or note down the domain profile name.
e) Repeat step a and d on the other end of the maintenance end point.
f) The maintenance profile name and the domain profile name should be the same on both the maintenance end points.

Step 4 Verify the maintenance point (MP) ID on both the sides are the same. Do the following:

a) In card view, click the **Provisioning** > **CFM** > **Configuration** > **MEP** tabs.
b) Note down the MPID value.
c) MPID should not be the same.
d) Repeat step a and d on the other end of the maintenance end point.
e) The MPID values must not be the same on both the maintenance end points.

CFM-LOOP

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

Logical Objects: ETH

The Connectivity Fault Management Loop (CFM-LOOP) alarm occurs on GE_XP or 10GE_XP cards when a continuity check (CC) packet is reused in a loop and consequently the same packet is returned to the source.

Clear the CFM-LOOP Condition

Procedure

Ensure that there are no loops in the L2-over-DWDM mode for VLANs in the network.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

CFM-MEP-DOWN

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

Logical Objects: ETH

The Connectivity Fault Management Maintenance End-Point Down (CFM-MEP-DOWN) alarm occurs in GE_XP, 10GE_XP, GE_XPE or 10GE_XPE cards when two maintenance end points cannot communicate with each other.

Clear the CFM-MEP-DOWN Condition

Procedure

Step 1 Make sure that there are no fiber cuts or other CFM alarms present.

Step 2 In card view, click the **Provisioning** > **CFM** > **CCDB** > **Counters** tabs.

Step 3 Ensure that the counter values in the CCM Received field is equivalent to the counter values in the CCM Transmitted field and that the counter is incrementing appropriately.

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

CFM-XCON-SERVICE

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

Logical Objects: ETH

The Connectivity Fault Management Cross-Connect Service (CFM-XCON-SERVICE) occurs in GE_XP, 10GE_XP, GE_XPE and 10GE_XPE cards when the domain are configured incorrectly, and a packet meant for a one domain goes to the other.

Clear the CFM-XCON-SERVICE Condition

Procedure

Step 1 In card view, click the **Provisioning** > **CFM** > **Configuration** > **MEP** tabs.

Step 2 Do the following to ensure that the maintenance association and the domain names are the same.

a) In card view, click the **Provisioning** > **CFM** > **Configuration** > **MA Profiles** tabs.
b) Enter or note down the maintenance profile name.
c) In card view, click the **Provisioning** > **CFM** > **Configuration** > **Domain Profiles** tabs.
d) Enter or note down the domain profile name.

e) Repeat steps a to d on the other end of the maintenance end point.

The maintenance profile name and the domain profile name must be the same on both the maintenance end points.

Step 3 Verify that the MA-Domain Mapping is correct. Click **Provisioning** > **CFM** > **Configuration** > **MA-Domain Mapping**

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

CHANLOSS

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

Logical Object: OCN

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

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

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

Clear the CHANLOSS Condition

Procedure

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

Step 2 If alternate vendor equipment is not the cause of the alarm, complete the Reset a Card in CTC, on page 310 procedure for the traffic card.

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

Step 3 If the alarm does not clear, complete the Physically Replace a Card, on page 313 procedure.

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

CHAN-PWR-THRESHOLD-CHECK

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

Logical Objects: OTS

The Channel Power Threshold Check (CHAN-PWR-THRESHOLD-CHECK) alarm is raised againstd OPT-EDFA cards. This alarm is raised when deleting or restoring a channel results in channel power drop below the fail thresholds. The alarm is raised even if the power of one channel drops below the fail threshold. The check for channel power is run every hour.

Clear the CHAN-PWR-THRESHOLD-CHECK Alarm

Procedure

CHAN-PWR-THRESHOLD-CHECK alarm is cleared in one of the these scenarios:

a) The alarm clears automatically when the periodic check determines that the total channel power does not cross failure thresholds. This scenario occurs when channels are deleted or restored. This increases the total channel power.
b) The alarm must be cleared manually by changing the failure threshold limits.

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

CLDRESTART

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

Logical Object: EQPT

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

Clear the CLDRESTART Condition

Procedure

Step 1 Remove and reinsert (reseat) the standby control card.

Step 2 If the condition fails to clear after the card reboots, complete the Remove and Reinsert (Reseat) Any Card , on page 313 procedure.

Step 3 If the condition does not clear, complete the Physically Replace a Card, on page 313 procedure for the card.

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

COMP-CARD-MISSING

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

Logical Object: EQPT

When the 100G-LC-C and CFP-LC cards work in a combination, the COMP-CARD-MISSING alarm is raised under any of the following conditions:

- When the 100G-LC-C or CFP-LC card is removed from the slot.
- When the 100G-LC-C or CFP-LC card is reset.
- When any one of these alarms is raised on the 100G-LC-C or CFP-LC card:
  - AUTORESET , on page 32
  - MANRESET , on page 181
  - CLDRESTART , on page 55
  - PROV-MISMATCH, on page 240

Clear the COMP-Card-Missing Alarm

Procedure

Step 1 Add the missing 100G-LC-C or CFP-LC card. If the card is reset, wait for it to boot up. To add a card, see the "Turn Up a Node" chapter.

Step 2 Complete the appropriate procedure to clear the following alarms:

- Clear the AUTORESET Alarm, on page 33
- Clear the CLDRESTART Condition, on page 55

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

COMM-FAIL

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

Logical Object: EQPT

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

Clear the COMM-FAIL Alarm

Procedure

Step 1 Complete the Remove and Reinsert (Reseat) Any Card , on page 313 procedure for the reporting card.

Step 2 If the alarm does not clear, complete the Physically Replace a Card, on page 313 procedure for the card.

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

CONTBUS-IO-A

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

Logical Object: EQPT

The *TCCA to Shelf A Slot Communication Failure*(CONTBUS-IO-A) alarm is raised when:

- The active Slot 7 TCC2/TCC2P/TCC3 (TCC A) has lost communication with another card in the shelf.
- NCS switches to the protection switch TCC2/TCC2P/TCC3 and clears after the other cards establish communication with the newly active TCC2/TCC2P/TCC3.
- The physical path of communication from the TCC2/TCC2P/TCC3 to the reporting card is not correct.

Clear the CONTBUS-IO-A Alarm

To clear this alarm, perform these steps:

Procedure

Step 1 Click the **Inventory** tab and expand the **Eqpt Type** column to view the provisioned type.

Verifies that the card on which the alarm is reported is physically present in the shelf.

If the actual and provisioned card types do not match, see the MEA (EQPT) , on page 184 alarm for the reporting card.

Step 2 If the alarm is raised on a single card slot that is not the standby Slot 11 TCC2/TCC2P/TCC3, or if it is the standby Slot 11 TCC2/TCC2P/TCC3, reset the card using the steps mentioned in the Reset a Card in CTC, on page 310 procedure.

Wait ten minutes to confirm that the card has fully rebooted and has returned to standby status.

Step 3 If the alarm is raised on multiple cards, perform the steps outlined in the Reset an Active Control Card and Activate the Standby Card, on page 311 procedure.

Step 4 Confirm that the reset is complete without errors and no new card related alarms appear in CTC.

Step 5 Verify that the physical path of communication from the TCC2/TCC2P/TCC3 to the reporting card is correct.

Step 6 If resetting the card using CTC does not clear the alarm, perform the steps outlined in the Remove and Reinsert (Reseat) Any Card , on page 313 procedure.

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

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447)

CONTBUS-IO-B

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

Logical Object: EQPT

The *TCC B to Shelf Communication Failure*(CONTBUS-IO-B) alarm is raised when:

- The active Slot 7 TCC2/TCC2P/TCC3 (TCC B) has lost communication with another card in the shelf.
- NCS switches to the protection switch TCC2/TCC2P/TCC3 and clears after the other cards establish communication with the newly active TCC2/TCC2P/TCC3.
- The physical path of communication from the TCC2/TCC2P/TCC3 to the reporting card is not correct.

Clear the CONTBUS-IO-B Alarm

To clear this alarm, perform these steps:

Procedure

Step 1 Click the **Inventory** tab and expand the **Eqpt Type** column to view the provisioned type.

Verifies that the card on which the alarm is reported is physically present in the shelf.

If the actual and provisioned card types do not match, see the MEA (EQPT) , on page 184 alarm for the reporting card.

Step 2 If the alarm is raised on a single card slot that is not the standby Slot 11 TCC2/TCC2P/TCC3, or if it is the standby Slot 11 TCC2/TCC2P/TCC3, reset the card using the steps mentioned in the Reset a Card in CTC, on page 310 procedure.

Wait ten minutes to confirm that the card has fully rebooted and has returned to standby status.

Step 3 If the alarm is raised on multiple cards, perform the steps outlined in the Reset an Active Control Card and Activate the Standby Card, on page 311 procedure.

Step 4 Confirm that the reset is complete without errors and no new card related alarms appear in CTC.

Step 5 Verify that the physical path of communication from the TCC2/TCC2P/TCC3 to the reporting card is correct.

Step 6 If resetting the card using CTC does not clear the alarm, perform the steps outlined in the Remove and Reinsert (Reseat) Any Card , on page 313 procedure.

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

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447)

COOL-MISM

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

Logical Object: FAN

The Cool Mismatch (COOL-MISM) condition is raised when an incorrect cooling profile is chosen for the NCS shelf. To determine the cooling profile values for the cards, see the "Cooling Profile" section in the "Installing the NCS Shelf" chapter of the *Hardware Installation Guide*.

Clear the COOL-MISM Alarm

Set the correct cooling profile for the NCS shelf depending on the cards used.

Procedure

Step 1 Log in to a node on the network.

Step 2 Navigate to **Shelf view** > **Provisioning** > **General** > **Voltage/Temperature** tabs.

Step 3 From the Cooling Profile drop-down list, choose the correct cooling profile value for the shelf.

Step 4 Click **Apply**.

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

CP-UNVER-CLEARED Alarm

Default Severity: Minor (MN)

Logical Object: NE

The CP-UNVER-CLEARED alarm is raised under the following conditions:

- When there is a failure in the original path and it is not fixed.
- After all the circuits are moved to the restored path, the port on the original path moves to OOS,DSBLD (ANSI) or Locked,disabled (ETSI) state. These alarms disappear on the original path and unverified alarms appear in **Maintenance** > **DWDM** > **WSON** tabs.

The CP-UNVER-CLEARED alarm is automatically cleared after acknowledging the unverified alarms in the WSON tab.

CTNEQPT-MISMATCH

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

Logical Object: EQPT

The Connection Equipment Mismatch condition is raised when there is a mismatch between the cross-connect card preprovisioned in the slot and the card actually present in the shelf. For example, an XC-VXL card could be preprovisioned in Slot 10, but another card could be physically installed.

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

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

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

Clear the CTNEQPT-MISMATCH Condition

Procedure

Step 1 Determine what kind of card is preprovisioned in the slot by completing the following steps:

a) In node view, click the **Inventory** tab.

b) View the slot row contents in the Eqpt Type and Actual Eqpt Type columns.

The Eqpt Type column contains the equipment that is provisioned in the slot. The Actual Eqpt Type contains the equipment that is physically present in the slot.

Step 2 Complete the Physically Replace a Card, on page 313 procedure for the mismatched card.

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

DATA-CRC

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

Logical Object: OCH, MSISC

A data cyclic redundancy check (CRC) bad packet count condition occurs when excessive CRC errors are received on the trunk ports of the GE-XP, GE-XPE, 10GE-XP, and 10GE-XPE cards.

The CRC error rate is measured and compared against a configured threshold. The system can be configured to perform an automatic FAPS switch when the DATA-CRC alarm occurs.

Clear the DATA-CRC Alarm

Procedure

For GE-XP, GE-XPE, 10GE-XP, and 10GE-XPE cards, perform the following:

a) Ensure that the fiber connector for the card is completely plugged in.
b) 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.
c) If the optical power level is good, verify that optical receive levels are within the acceptable range.
d) If the receive levels are good, clean the fibers at both the ends according to site practise. If no site practice exists, complete the procedure in the Maintain the Node chapter.
e) Clear the CRC alarm in CTC.
f) Wait for a time equivalent to (polling period * soak count).

DBOSYNC

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

Logical Object: NE

The Standby Database Out Of Synchronization alarm occurs when the standby controller card database does not synchronize with the active database on the active controller card.

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

Clear the DBOSYNC Alarm

Procedure

Step 1 Save a backup copy of the active controller card database.

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

a) In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **General** > **General** tabs.

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

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

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

DCU-LOSS-FAIL

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

Logical Object: OTS

The DCU-LOSS-FAIL condition occurs when the DCU loss monitored value exceeds the maximum acceptable DCU loss of the board .

Clear the DCU-LOSS-FAIL Condition

Procedure

Step 1 Verify that the optical fibers connecting the board (OPT-PRE, OPT-PRE-L, 40-SMR1-C, or 40-SMR2-C) and the DCU unit are clean, correctly plugged in, and not damaged.

Step 2 If the condition does not clear, verify that appropriate DCU unit, according to the installation requirements, is connected to the board and is correctly working.

Step 3 If the condition still does not clear, verify that the optical power signal is present on the DCU-TX port.

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

DISCONNECTED

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

Logical Object: SYSTEM

The Disconnected alarm is raised when CTC has been disconnected from the node. The alarm is cleared when CTC is reconnected to the node.

Clear the DISCONNECTED Alarm

Procedure

Restart the CTC application.

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

DSP-COMM-FAIL

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

Logical Object: TRUNK

The Digital Signal Processor (DSP) Communication Failure alarm indicates that there is a communication failure between an MXP or TXP card microprocessor and the on-board DSP chip that controls the trunk (or DWDM) port. This alarm typically occurs after a DSP code upgrade.

The alarm is temporary and does not require user action. The MXP or TXP card microprocessor attempts to restore communication with the DSP chip until the alarm is cleared.

If the alarm is raised for an extended period, the MXP or TXP card raises the DUP-IPADDR , on page 64 condition and could affect traffic.

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

DSP-FAIL

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

Logical Object: TRUNK

The DSP Failure alarm indicates that a DSP-COMM-FAIL , on page 63, has persisted for an extended period on an MXP or TXP card. It indicates that the card is faulty.

Clear the DSP-FAIL Alarm

Procedure

Complete the Physically Replace a Card, on page 313 procedure for the reporting MXP or TXP card.

Warning **High-performance devices on this card can get hot during operation. To remove the card, hold it by the faceplate and bottom edge. Allow the card to cool before touching any other part of it or before placing it in an antistatic bag.** Statement 201

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

DUP-IPADDR

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

Logical Object: NE

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

Clear the DUP-IPADDR Alarm

Procedure

Step 1 Isolate the alarmed node from the other node having the same address:
a) Connect to the alarmed node using the Craft port on the control card.
b) Begin a CTC session.
c) In the login dialog box, uncheck the **Network Discovery** check box.

Step 2 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **Network** > **General** tabs.

Step 3 In the IP Address field, change the IP address to a unique number.

Step 4 Click **Apply.**

Step 5 Restart any CTC sessions that are logged into either of the duplicate IP addresses. (For procedures to log in or log out, refer to the Connect the PC and Log Into the GUI chapter in the *Cisco ONS 15454 DWDM Procedure Guide*Connect the PC and Log into the GUI document.

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

DUP-NC

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

Logical Object: Shelf

(In R10.0) The DUP-NC (Duplicate Node Controller) alarm is raised in multishelf environment on both the node controllers, when two node controllers are connected to the same switch.

(In R10.1), The DUP-NC alarm is raised in multishelf environment on the NCS 2006 duplicate node controller, when two node controllers are connected to the same switch.

Clear the DUP-NC Alarm

Procedure

Step 1 (In R10.0) Pull the LAN cables out from both the node controllers connected to the switch.

Step 2 (In R10.1)

a. Disconnect the duplicate node controller's cable from switch. The DUP-NC alarm clears.

b. Perform soft reset of the control card to recover the MSM ASIC interface.

Step 3 (In R10.6.2)

a. Disconnect the duplicate node controller's cable from switch.

b. Perform soft reset of the active control card on both the node controllers. The DUP-NC alarm clears.

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

DUP-NODENAME

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

Logical Object: NE

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

Clear the DUP-NODENAME Alarm

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **General** > **General** tabs.

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

Step 3 Click **Apply.**

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

DUP-SHELF-ID

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

Logical Object: SHELF

The Duplicated Shelf Identifier alarm applies to a shelf that has multishelf management enabled when the control card detects that you have programmed an ID already in use by another shelf.

Clear the DUP-SHELF-ID Alarm

Procedure

Unprovision the shelf ID of the duplicate shelf by completing the following steps:

a) In shelf view (multishelf mode) or multishelf view (multishelf mode), click the node controller **Provisioning** > **General** > **Multishelf Config** tabs.
b) Enter a new value in the **Shelf ID** field.
c) Click **Apply**

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

EPROM-SUDI-SN-MISMATCH

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

Logical Object: EQPT

The EPROM SUDI Serial Number Mismatch alarm is raised when the card serial number mismatches with certificate serial number.

Clear the EPROM-SUDI-SN-MISMATCH Alarm

Procedure

This alarm is cleared when the card serial number matches with certificate serial number.

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

EFM-PEER-MISSING

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

Logical Objects: GE

The EFM Peer Missing (EFM-PEER-MISSING) alarm occurs in GE_XP or 10GE_XP cards under the following conditions:

- When an EFM session is established between two ports and EFM is disabled on one of the ports, the alarm is raised on the peer port.
- When an EFM session is established between two ports and one of the ports is moved to OOS-DSBLD state, the alarm is raised on the peer port.

Clear the EFM-PEER-MISSING Condition

Procedure

To clear the EFM PEER MISSING alarm, do the following:

a) In card view, click the Provisioning > EFM > Configuration tabs.
b) From the EFM State drop-down list, choose Enabled.
c) Click Apply to enable EFM for that port.

Peer port is in IS state.

EFM-RFI-CE

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

Logical Object: GE

The EFM Remote Failure Indication Critical Event (EFM-RFI-CE) alarm is raised if the peer interface defines the RFI CE.

Clear the EFM-RFI-CE Alarm

Procedure

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

EFM-RFI-DG

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

Logical Object: GE

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

- The peer interface is administratively shut down.
- The EFM is not configured on the peer interface.
- The peer card is reloading.

Clear the EFM-RFI-DG Alarm

Procedure

To clear the EFM-RFI-DG alarm, check if the peer is administratively disabled. If it is, move the port to IS state.

Note If the peer device is not an GE-XP or 10GE-XP card, consult the peer device manual to find the scenarios under which the EFM-RFI-DG alarm is raised.

EFM-RFI-LF

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

Logical Object: GE

The EFM Remote Failure Indication Link Fault (EFM-RFI-LF) alarm indicates that the peer interface has a carrier loss.

Clear the EFM-RFI-LF Alarm

Procedure

Clear the EHIBATVG and CARLOSS alarms on the peer Ethernet interface.

Note If the peer device is not a GE_XP or 10GE_XP card, consult the user documentation of the peer device to understand scenarios under which the alarm is raised.

EFM-RLBK

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

Logical Objects: GE

TThe EFM Remote Loopback (EFM-RLBK) alarm indicates that the EFM port is participating in an EFM remote loopback.

Clear the EFM-RLBK Condition

Procedure

To clear the EFM-LPBK alarm, ensure that the EFM loopback is not configured on the port and the peer port.

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

EHIBATVG

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

Logical Object: PWR

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

Clear the EHIBATVG Alarm

Procedure

The problem is external to the ONS system. Troubleshoot the power source supplying the battery leads.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

ELWBATVG

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

Logical Object: PWR

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

Clear the ELWBATVG Alarm

Procedure

The problem is external to the ONS system. Troubleshoot the power source supplying the battery leads.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

ENCAP-MISMATCH-P

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

Logical Object: STSTRM

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

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

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

For an ENCAP-MISMATCH-P to be raised, there is a mismatch between the received and expected C2 byte, with either the expected byte or received byte value being 0x01.

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

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

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

This alarm is demoted by a PLM-P condition or a PLM-V condition.

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

Clear the ENCAP-MISMATCH-P Alarm

Procedure

Step 1 Ensure that the correct framing mode is in use on the receive card:

a) In node view, double-click the receive ML-Series or CE-1000 card to open the card view.
b) Click the **Provisioning** > **Card** tabs.
c) In the Mode drop-down list, ensure that the same mode (GFP or HDLC) is selected. If it is not, choose it and click **Apply**.

Step 2 Ensure that the correct framing mode is in use on the transmit card, and that it is identical to the receiving card:

a) In node view, double-click the transmit ML-Series or CE-1000 card to open the card view.
b) Click the **Provisioning** > **Card** tabs.
c) In the Mode drop-down list, ensure that the same mode (GFP or HDLC) is selected. If it is not, choose it and click **Apply**.

Step 3 If the alarm does not clear, use the CLI to ensure that the remaining settings are correctly configured on the ML-Series or CE-1000 card:

- Encapsulation
- CRC size
- Scrambling state

To open the interface, click the **IOS** tab and click **Open IOS Command Line Interface (CLI)**.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

ENC-CERT-EXP

Default Severity: Minor (MN), Service-Affecting (SA)

Logical Objects: EQPT

The SUDI 2029 MIC encryption certicate is expired on line cards like 400G-XP-LC, WSE, and MR-MXP.

Clear the ENC-CERT-EXP Alarm

Procedure

The alarm is cleared under the following conditions:

- Change the encryption certificate type to LSC (or)
- Disable the encryption (or)
- Both near-end and far-end line cards must have SUDI 2099 certificates and software package release 11.12 and above.

If the alarm is not cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

EMBEDDED-AMPLIFIER-SATURATED

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

Logical Object: OTS

The Embedded Amplifer Saturated condition is raised by the embedded EDFA in the AS-16-CCOFS cards. It means the incoming signal on the ADD or COM Rx port is saturating the internal amplifier.

Clear the EMBEDDED-AMPLIFIER-SATURATED Alarm

Procedure

Add an attenuator or decrease the power on the port if the alarm is raised on COM-Tx. Decrease the SMR-20 setpoint if the alarm is raised on COM-Rx.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

EOC-E

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

Logical Objects: OCN, STMN, FE, GE

The SONET DCC Termination Failure alarm occurs when the system loses its DCC. Although this alarm is primarily SONET, it can apply to DWDM. EOC-E is supported only on TNC/TNC-E with GE or FE OSC ports.

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

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

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

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

Note The EOC alarm is raised on the DWDM trunk in MSTP systems. Its SDH (ETSI) counterpart, MS-EOC, is not raised against the trunk port.

Clear the EOC-E Alarm

Procedure

Step 1 If the LOS (DS1) alarm or SF-L alarm is reported, complete the appropriate troubleshooting procedure in the "Alarm Troubleshooting" chapter of the troubleshooting guide.

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

Step 2 If the alarm does not clear on the reporting node, verify the physical connections between the cards and that the fiber-optic cables are configured to carry SDCC traffic.

Step 3 If the physical connections are correct and configured to carry DCC traffic, ensure that both ends of the fiber span have in-service (IS) ports. Verify that the ACT/SBY LED on each card is green.

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

Step 5 Repeat Step 4 procedure at the adjacent nodes.

Step 6 If DCC is provisioned for the ends of the span, verify that the port is active and in service by completing the following steps:

a) Confirm that the card shows a green LED in CTC or on the physical card. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
b) To determine whether the port is in service, in node view (single-shelf mode) or shelf view (multishelf mode), double-click the card in CTC to open the card view.
c) In card view, click the **Provisioning** > **Line** tabs.
d) Verify that the Admin State column lists the port as IS (or Unlocked).
e) If the Admin State column lists the port as OOS,MT (or Locked,maintenance) or OOS,DSBLD (or Locked,disabled), click the column and choose IS, or Unlocked. Click **Apply**.

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

Caution Using an optical test set disrupts service on a card. It could be necessary to manually switch traffic carrying circuits over to a protection path. Refer to the "2.8.2 Protection Switching, Lock Initiation, and Clearing" section for commonly used switching procedures.

Step 8 If no signal failures exist on terminations, measure power levels to verify that the budget loss is within the parameters of the receiver. Refer to the Configuration guide for card power levels.

Step 9 If budget loss is within parameters, ensure that fiber connectors are securely fastened and properly terminated.

Step 10 If fiber connectors are properly fastened and terminated, complete the "Reset an Active Control Card and Activate the Standby Card" procedure.

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

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

Step 11 If the control card reset does not clear the alarm, delete the problematic SDCC termination:

a) From the View menu in card view, choose **Go to Previous View** if you have not already done so.

b) In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **Comm Channels** > **SDCC** tabs.
c) Highlight the problematic DCC termination.
d) Click **Delete.**
e) Click **Yes** in the Confirmation Dialog box.

Step 12 Recreate the SDCC termination.

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

If the alarm has not cleared, call Cisco TAC (1 800 553-2447). If the Cisco TAC technician tells you to reseat the card,

If the Cisco TAC technician tells you to reseat the card, complete the "Reset an Active Control Card and Activate the Standby Card" procedure. If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Card" procedure.

Warning **High-performance devices on this card can get hot during operation. To remove the card, hold it by the faceplate and bottom edge. Allow the card to cool before touching any other part of it or before placing it in an antistatic bag. Statement 201**

OSC ports in TNCP and TNCS cards might have the EOC-E alarm. Follow this procedure to clear the EOC-E alarm.

a. If you want to connect SFP ports with far end OTDR ports, use 1518 nm OSC SFP. For example, use the ONS-SC-OSC-18.0 SFP. Otherwise, OSC might not work as expected.

b. If you want to connect SFP OSC to SFP OSC ports, set proper Rx/Tx power values in both ends using optical attenuators. If SFP GREEN LED in both ends glow and EOC-E alarm is not still cleared, adjust the power values using attenuators until the EOC-E alarm clears.

c. Ensure to use same wavelength SFPs in both near end and far end. 1518 nm OSC SFP will not work with other wavelength SFPs.

EOC-L

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

Logical Object: TRUNK

The Line DCC (LDCC) Termination Failure alarm occurs when the ONS system loses its line data communications channel (LDCC) termination. EOC-L is not supported on OSCM or TNC/TNC-E cards.

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

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

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

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

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

Clear the EOC-L Alarm

Procedure

Complete the "Clear the EOC Alarm" procedure.

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

Warning **High-performance devices on this card can get hot during operation. To remove the card, hold it by the faceplate and bottom edge. Allow the card to cool before touching any other part of it or before placing it in an antistatic bag.** Statement 201

EQPT

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

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

An Equipment Failure alarm indicates that a hardware failure has occurred on the reporting card. If the EQPT alarm occurs with a BKUPMEMP, refer to the procedure to clear the alarm. (Clearing a BKUPMEMP alarm also clears an EQPT alarm.)

This alarm is also invoked if a diagnostic circuit detects a card application-specific integrated circuit (ASIC) failure. In this case, if the card is part of a protection group, an APS switch occurs. If the card is the protect card, switching is inhibited and a PROTNA , on page 239, is raised. The standby path generates a path-type alarm. For more information about provisioning PPMs (SFPs), refer to the Installing the GBIC, SFP, SFP+, and XFP Optical Modules in Cisco ONS Platforms document.

Clear the EQPT Alarm

Procedure

Step 1 If traffic is active on the alarmed port, you could need to switch traffic away from it. See the Protection Switching, Lock Initiation, and Clearing, on page 306 procedure for commonly used traffic-switching procedures.

Step 2 Complete the Reset a Card in CTC, on page 310 procedure for the reporting card.

Step 3 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. Verify the LED status. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

Step 4 If the CTC reset does not clear the alarm, complete the Remove and Reinsert (Reseat) Any Card , on page 313 procedure for the reporting card.

Warning **High-performance devices on this card can get hot during operation. To remove the card, hold it by the faceplate and bottom edge. Allow the card to cool before touching any other part of it or before placing it in an antistatic bag.** Statement 201

Step 5 If the physical reseat of the card fails to clear the alarm, complete the Physically Replace a Card, on page 313 procedure for the reporting card.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

EQPT-DEGRADE

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

Logical Objects: EQPT

The Equipment Degrade condition is raised when a permanent failure that limits or compromises the normal behavior of the card (without impact on traffic) is detected.

Clear the EQPT-DEGRADE Condition

Procedure

Remove and reinsert the card where the EQPT-DEGRADE condition is raised. If the reinsertion does not clear the alarm, replace the card. Complete the Physically Replace a Card, on page 313 procedure to replace the card.

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

EQPT-DIAG

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

Logical Object: EQPT

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

Clear the EQPT-DIAG Alarm

Procedure

Step 1 Complete the Remove and Reinsert (Reseat) Any Card , on page 313 procedure for the alarmed card

Step 2 If the alarm does not clear, complete the Physically Replace a Card, on page 313 procedure if it is raised against a traffic card, or complete the Generic Signal and Circuit Procedures, on page 314 procedure if the alarm is raised against the cross-connect card.

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

EQPT-FAIL

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

Logical Object: EQPT

An Equipment Failure (EQPT-FAIL) alarm is raised when diagnostic circuit detects a card ASIC failure. This alarm indicates that a hardware or communication failure has occurred on the reporting card.

Clear the EQPT-FAIL Alarm

Procedure

Step 1 Complete the procedure for the reporting card.

Step 2 Verify that the reset is complete and error-free and that no new related alarms appear in . Verify the LED status. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

Step 3 If reset does not clear the alarm, complete the Remove and Reinsert (Reseat) Any Card , on page 313 procedure for the reporting card.

Warning **High-performance devices on this card can get hot during operation. To remove the card, hold it by the faceplate and bottom edge. Allow the card to cool before touching any other part of it or before placing it in an antistatic bag.** Statement 201

Step 4 If the physical reseat of the card fails to clear the alarm, complete the Physically Replace a Card, on page 313 procedure for the reporting card.

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

EQPT-FPGA-IMAGE-AVAILABLE

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

Logical Object: EQPT

The EQPT-FPGA-IMAGE-AVAILABLE condition occurs when there is a mismatch between the running trunk FPGA version and the package version.

Clear the EQPT-FPGA-IMAGE-AVAILABLE Condition

Procedure

Perform a manual FPGA upgrade.

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

EQPT-MISS

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

Logical Object: FAN

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

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

Clear the EQPT-MISS Alarm

Procedure

Step 1 If the alarm is reported against the fan, verify that the fan-tray assembly is present.

Step 2 If the fan-tray assembly is present, complete the Replace the Fan-Tray Assembly, on page 318 procedure.

Step 3 If no fan-tray assembly is present, obtain a fan-tray assembly and refer to the Install the Fan-Tray Assembly procedure in the Hardware Installation Guide.

Step 4 If the alarm does not clear, replace the ribbon cable from the AIP to the system board with a known-good ribbon cable.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

ERFI-P-SRVR

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

Logical Object: STSMON, STSTRM

The Three-Bit ERFI Path Server condition is triggered on DS-1, DS-3, or VT circuits when the AIS-P , on page 18 or the LOP-P , on page 155 is raised on the transmission signal.

Clear the ERFI-P-SRVR Condition

Procedure

Complete the Clear the LOP-P Alarm, on page 156 procedure. This should clear the ERFI condition.

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

ESMC-FAIL

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

Logical Object: GE, TRUNK

An Ethernet Synchronization Messaging Channel Fail (ESMC-FAIL) alarm is raised when a SyncE port fails to receive the ESMC protocol data units (PDU) for 5 seconds.

Clear the ESMC-FAIL Alarm

Procedure

Step 1 Verify if the far end port is enabled for SyncE and is sending ESMC PDUs.

Step 2 Verify if the Ethernet link is up on the client and SA alarms are not present on it.

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

ETH-LINKLOSS

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

Logical Object: NE

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

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

Clear the ETH-LINKLOSS Alarm

Procedure

Step 1 To clear this condition, reconnect the backplane LAN cable. Refer to the Hardware Installation Guide for procedures to install this cable.

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

EVAL-LIC

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

Logical Object: EQPT

The Evaluation License (EVAL-LIC) alarm is raised to indicate that an valid evaluation license is in use.

Clear the EVAL-LIC Alarm

The EVAL-LIC alarm clears in one of the following scenarios:

- When the user discontinues or disables the associated feature that raised the evaluation license alarm. After this alarm clears, the line card resumes normal operation. The line card tracks the remaining validity period of the evaluation license that was disabled by the user.
- When the validity period of the evaluation license is expired. After the validity period, the card raises an LICENSE-EXPIRED.
- When a permanent license is installed.

Procedure

Procure and install a permanent license. For more information on installing a license, see the Licensing Configuration Guide.

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

EXC-BP

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

Logical Objects: OTS

The Excessive Back Propagation condition occurs due to excessive backscattered Raman pump power at the LINE-RX connector. This condition is caused either due to a dirty connector, bad optical patch panel connection, or disconnected LINE-RX connector. When the EXC-BP alarm is raised, the level of backscattered power is at a hazardous level, with the risk of possible damage to the unit and/or the external equipment.

Clear the EXC-BP Condition

Procedure

Step 1 Verify all the fibers between the LINE RX and patch-panel are connected.

Step 2 Clean the connectors using site practices or, if none exists, complete the procedure in the Maintain the Node chapter of the Procedure Guide.

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

EXCCOL

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

Logical Object: EQPT

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

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

Clear the EXCCOL Alarm

Procedure

Step 1 Verify that the network device port connected to the control card has a flow rate set to 10 Mb, half-duplex.

Step 2 If the port has the correct flow rate and duplex setting, troubleshoot the network device connected to the control card and the network management LAN.

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

EXT

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

Logical Object: ENVALRM

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

Clear the EXT Alarm

Procedure

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

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

FAILTOSW (2R, EQPT, ESCON, FC, GE, ISC, OCN/STMN, TRUNK, OTS)

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

Logical Objects: 2R, EQPT, ESCON, FC, GE, ISC, OCN, STMN, TRUNK, OTS

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

Note For more information about protection schemes, refer to the Manage the Node chapter of the *Cisco ONS 15454 DWDM Procedure Guide*Manage the Node document.

Clear the FAILTOSW (2R, EQPT, ESCON, FC, GE, ISC, OCN/STMN, TRUNK, OTS) Condition

Procedure

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

Step 2 If the condition does not clear, replace the working card that is reporting the higher-priority alarm by following the Physically Replace a Card, on page 313 procedure. This card is the working facility using the protect facility and not reporting FAILTOSW.

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

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

FAILTOSW (TRUNK)

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

Logical Object: TRUNK

The Failure to Switch to Protection Facility condition applies to MXP and TXP trunk ports in splitter protection groups and occurs when a working or protect trunk port switches to its companion port by using a MANUAL command.

Note For more information about protection schemes, refer to the Manage the Node chapter of the *Cisco ONS 15454 DWDM Procedure Guide*Manage the Node document.

Clear the FAILTOSW (TRUNK) Condition

Procedure

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

Step 2 If the condition does not clear, replace the working card that is reporting the higher-priority alarm by following the Physically Replace a Card, on page 313 procedure. This card is the working facility using the protect facility and not reporting FAILTOSW.

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

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

FAILTOSW-HO

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

Logical Object: VCMON-HP

The High-Order Path Failure to Switch to Protection condition occurs when a high-order path circuit fails to switch to the working or protect electrical circuit using the MANUAL command.

Clear the FAILTOSW-HO Condition

Procedure

Complete the Clear the FAILTOSW (2R, EQPT, ESCON, FC, GE, ISC, OCN/STMN, TRUNK, OTS) Condition, on page 84 procedure.

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

FAILTOSW-PATH

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

Logical Object: STSMON, VT-MON

The Fail to Switch to Protection Path condition occurs when the working circuit does not switch to the protection circuit on a path protection configuration. Common causes of the FAILTOSW-PATH alarm include a missing or defective protect port, a lockout set on one of the path protection nodes, or path-level alarms that would cause a path protection switch to fail.

Clear the FAILTOSW-PATH Condition in a Path Protection Configuration

Procedure

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

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

Step 2 If the condition does not clear, replace the active OC-N card that is reporting the higher-priority alarm. Complete the Physically Replace a Card, on page 313 procedure. Replacing the active OC-N card that is reporting the higher-priority alarm allows traffic to revert to the active slot. Reverting frees the standby card, which can then take over traffic from the card reporting the lower-priority alarm and the FAILTOSW-PATH condition.

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

FAN

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

Logical Object: FAN

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

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

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

Note FAN-FAIL alarm is not raised if BAT-FAIL alarm appears on the power module.

Clear the FAN Alarm

Procedure

Step 1 Determine whether the air filter needs replacement. Complete the Inspect, Clean, and Replace the Air Filter, on page 316 procedure.

Step 2 If the filter is clean, complete the Remove and Reinsert a Fan-Tray Assembly, on page 318 procedure.

Step 3 If the fan does not run or the alarm persists, complete the Replace the Fan-Tray Assembly, on page 318 procedure. The fan should run immediately when correctly inserted.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

FAPS

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

Logical Objects: TRUNK

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

Clear the FAPS Alarm

Procedure

When the cause of switching disappears, the protection port switches from the forwarding to the blocking state, and the FAPS alarm clears.

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

FAPS-CONFIG-MISMATCH

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

Logical Object: EQPT

The Fast Automatic Protection Switching (FAPS) Config Mismatch condition is raised when a GE-XP or 10GE-XP card that is provisioned as a primary card in a FAPS ring, resets or when one of the primary card's trunk port is not set to Blocking.

Clear the FAPS-CONFIG-MISMATCH Condition

Procedure

Check the configuration of the primary card. Ensure that at least one of the trunk ports of the primary card is in the blocking state and the FAPS ring is complete.

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

FC-NO-CREDITS

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

Logical Objects: Client port

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

FC-NO-CREDITS is raised only if transmission is completely prevented. (If traffic is slowed but still passing, this alarm is not raised.)

Clear the FC-NO-CREDITS Alarm

Procedure

Step 1 If the port is connected to a Fibre Channel/FICON switch, make sure it is configured for interoperation mode using the manufacturer's instructions.

Step 2 If the port is not connected to a switch, turn off Autodetect Credits by completing the following steps:

a) Double-click the card.

b) Click the **Provisioning** > **Port** > **General** tabs.

c) Under Admin State, click the cell and choose OOS,MT (or Locked,maintenance).
d) Click **Apply**.
e) Click the **Provisioning** > **Port** > **Distance Extension** tabs.
f) Uncheck the Autodetect Credits column check box.
g) Click **Apply**.
h) Click the **Provisioning** > **Port** > **General** tabs.
i) Under Admin State, click the cell and choose **IS** (or **Unlocked**).
j) Click **Apply**.

Step 3 Program the Credits Available value based on the buffers available on the connected equipment by completing the following steps:

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

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

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

FDI

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

Logical Objects: OCH, OCH-TERM, OMS, OTS, EQPT

The Forward Defect Indication (FDI) condition is part of network-level alarm correlation. It is raised at the far end when the OCH optical payload is missing due to an optical channel signal (LOS), light (LOS-P), or optical power (OPWR-LFAIL) alarm root cause.

An LOS, LOS-P, or OPWR-LFAIL alarm on a circuit causes multiple alarms for each channel. Correlation simplifies troubleshooting by reporting a single alarm for multiple alarms having one root cause, then demoting the root alarms so that they are only visible in the Conditions window (showing their original severity.)

FDI clears when the optical channel is working on the aggregated or single-channel optical port.

Note Network-level alarm correlation is only supported for communication alarms. It is not supported for equipment alarms.

Clear the FDI Condition

Procedure

Clear the root-cause service-affecting alarm by using one of the following procedures, as appropriate:

- Clear the LOS (OTS) Alarm, on page 161
- Clear the LOS (TRUNK) Alarm, on page 163
- Clear the LOS-P (OCH) Alarm, on page 167
- Clear the LOS-P (AOTS, OMS, OTS) Alarm, on page 165
- Clear the LOS-P (TRUNK) Alarm, on page 170
- Clear the OPWR-LFAIL Alarm, on page 207

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

FE-FRCDWKSWBK-SPAN

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

Logical Object: STMN

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

Note WKSWBK-type conditions apply only to nonrevertive circuits.

Clear the FE-FRCDWKSWBK-SPAN Condition

Procedure

Complete the Clear a 1+1 Force or Manual Switch Command, on page 308 procedure for the far-end port.

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

FE-FRCDWKSWPR-SPAN

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

Logical Object: STMN

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

Clear the FE-FRCDWKSWPR-SPAN Condition

Procedure

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

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

Step 3 Clear the main alarm.

Step 4 If the FE-FRCDWKSWPR-SPAN condition does not clear, complete the Clear a BLSR External Switching Command, on page 310procedure.

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

FE-MANWKSWBK-SPAN

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

Logical Object: STMN

The Far End Manual Switch Back to WorkingSpan condition occurs when a far-end span is Manual switches back to working.

Note WKSWBK-type conditions apply only to nonrevertive circuits.

Clear the FE-MANWKSWBK-SPAN Condition

Procedure

Step 1 To troubleshoot the FE condition, determine which node and card is linked directly to the card reporting the FE condition. For example, an FE condition on a card in Slot 12 of Node 1 could relate to a main alarm from a card in Slot 6 of Node 2.

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

Step 3 Complete the Clear a BLSR External Switching Command, on page 310 procedure.

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

FE-MANWKSWPR-SPAN

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

Logical Object: STMN

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

Clear the FE-MANWKSWPR-SPAN Condition

Procedure

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

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

Step 3 Complete the Clear a BLSR External Switching Command, on page 310 procedure.

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

FEC-MISM

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

Logical Object: TRUNK

The Forward Error Correction (FEC) Mismatch alarm applies to all cards featuring FEC/E-FEC capability: TXP_MR_10G, TXP_MR_10E, TXP_MR_10E_C, TXP_MR_10E_L, TXP_MR_2.5G, TXPP_MR_2.5G, MXP_10G, MXP_MR_10E, ADM-10G, and OTU2_XP. FEC-MISMATCH is reported only on the card configured in Standard FEC mode or with FEC disabled. A card configured in enhanced FEC mode will report an OTUK-LOF , on page 223 alarm.

The alarm is related to ITU-T G.709 encapsulation and is only raised against a trunk port.

When the OUT2 client is directly connected with another OTU2 client with standard FEC and Disabled FEC on either side, the FEC-MISM alarm is not raised on the 400G-XP-LC card. The Uncorrected FEC Word condition is raised on the standard FEC side.

Clear the FEC-MISM Alarm

Procedure

Step 1 In node view (single-shelf mode) or shelf view (multishelf mode), double-click the TXP_MR_10G, TXP_MR_10E, TXP_MR_10E_C, TXP_MR_10E_L, TXP_MR_2.5G, TXPP_MR_2.5G, MXP_MR_10G, MXP_MR_10E, ADM-10G, and OTU2_XP card.

Step 2 Click the **Provisioning** > **OTN** > **OTN Lines** tabs.

Step 3 In the FEC column, click **Enable** to activate the FEC feature. This causes a different OTN frame to be transmitted. Alternately, in the E-FEC column (TXP_MR_10E and MXP_MR_10E), click Enable to activate the Enhanced FEC feature.

Step 4 Verify that the far-end card is configured the same way by repeating Step 1, on page 93 through Step 3, on page 93.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

FEED-MISMATCH

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

Logical Objects: EQPT

The Feed Mismatch alarm is raised when the mandatory power module input feed based on Power Supply Unit (PSU) configuration is disconnected or incorrectly connected.

The alarm is cleared when the mandatory feed connection of power module is connected as per the PSU configuration. To re-configure the feed connection, refer to Power Redundancy .

FEPRLF

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

Logical Object: OCN

The Far-End Protection Line Failure alarm occurs when there was an SF (TRUNK) , on page 261 condition on the protect card APS channel coming into the node.

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

Clear the FEPRLF Alarm on an BLSR

Procedure

Step 1 To troubleshoot the FE alarm, determine which node and card is linked directly to the card reporting the FE alarm. For example, an FE alarm or condition on a card in Slot 16 of Node 1 could relate to a main alarm from a card in Slot 16 in Node 2.

Step 2 Log into the node that is linked directly to the card reporting the FE alarm.

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

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

FIBERTEMP-DEG

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

Logical Object: AOTS

The Fiber Temperature Degrade alarm occurs when a DWDM card (OPT-AMP-C) internal heater-control circuit fails. Degraded temperature can cause some signal drift.

Note For general information about DWDM cards, refer to the Card Reference chapter in the *Cisco ONS 15454 DWDM Reference Manual*. For information about changing their settings, refer to the Change DWDM Card Settings chapter in the *Cisco ONS 15454 DWDM Procedure Guide*.

Clear the FIBERTEMP-DEG Alarm

Procedure

For the alarmed card, complete the Physically Replace a Card, on page 313 procedure.

Warning **High-performance devices on this card can get hot during operation. To remove the card, hold it by the faceplate and bottom edge. Allow the card to cool before touching any other part of it or before placing it in an antistatic bag.** Statement 201

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

FIPS-TEST-FAILED

Default Severity: Critical (CR)

Logical Object: EQPT

The FIPS Test Failed alarm is raised on the WSE card. This alarm is raised when the FIPS test fails on the WSE card.

A secure library is used for the FIPS test. A self-test is run on the card during startup to check that the library works with all the algorithms that are supported by FIPS. The FIPS TEST Failed alarm is raised when there is an issue during the self-test on the card.

Clearing the FIPS-TEST-FAILED Alarm

Before you begin

You must have Security super user privileges to clear the alarm.

Procedure

Step 1 Complete the Reset a Card in CTC, on page 310 procedure for the card.

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

Step 2 If the alarm does not clear, complete the Physically Replace a Card, on page 313 procedure.

If the troubleshooting procedure does not clear the alarm, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html or call the Cisco Technical Assistance Center (1 800 553-2447) to report the problem.

FORCED-REQ

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

Logical Object: EQPT, ML1000, ML100T, MLFX, STSMON, VT-MON

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

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

- MAN-REQ (for an ML-Series object)
- RPR-SF
- RPR-SD
- WTR (for an ML-Series object)

Clear the FORCED-REQ Condition

Procedure

Step 1 Complete the Clear a 1+1 Force or Manual Switch Command, on page 308 procedure.

Step 2 If the condition is raised on an IEEE 802.17b-based RPR span, enter the following command in the CLI in RPR-IEEE interface configuration mode:

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

If the troubleshooting procedure does not clear the alarm, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html or call the Cisco Technical Assistance Center (1 800 553-2447) to report the problem.

FORCED-REQ-SPAN (2R, ESCON, FC, GE, ISC, OCN/STMN, OTS)

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

Logical Objects: 2R, ESCON, FC, GE, ISC, OCN/STMN, OTS

The Force Switch Request Span condition applies to Y-cable-protected TXP configurable clients (OC-3, OC-12/STM-4,OC-48/STM-16, OC-192/STM-64, FC, ESCON, or FICON). If traffic is present on a working port and you use the FORCE command to prevent it from switching to the protect port (indicated by FORCED TO WORKING), FORCED-REQ-SPAN indicates this force switch. In this case, the force is affecting not only the facility, but the span.

Note For more information about protection schemes, refer to the Manage the Node chapter of the *Cisco ONS 15454 DWDM Procedure Guide*.

Note For more information about protection schemes, refer to the Manage the Node document.

FORCED-REQ-SPAN (TRUNK)

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

Logical Object: TRUNK

The Force Switch Request Span condition applies to MXP and TXP trunk ports in splitter protection groups. If traffic is present on a working port and you use the FORCE command to prevent it from switching to the protect port (indicated by FORCED TO WORKING), FORCED-REQ-SPAN indicates this force switch. In this case, the force is affecting not only the facility, but the span.

Note For more information about protection schemes, refer to the Manage the Node chapter of the *Cisco ONS 15454 DWDM Procedure Guide*.

Note For more information about protection schemes, refer to the Manage the Node document.

FP-LINK-LOSS

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

Logical Object: EQPT

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

Clear the FP-LINK-LOSS Condition

Procedure

Connect a LAN cable to the front port of the control card.

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

FPGA-UPGRADE-FAILED

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

Logical Object: Equipment

The FPGA-UPGRADE-FAILED alarm is raised when the FPGA upgrade on the TNCS-2 or TNCS-2O control card fails.

Clear the FPGA-UPGRADE-FAILED Alarm

Procedure

Reboot the TNCS-2/TNCS-2O control card on the chassis.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

FRCDSWTOINT

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

Logical Object: NE-SREF

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

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

FRCDSWTOPRI

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

Logical Objects: EXT-SREF, NE-SREF

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

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

FRCDSWTOSEC

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

Logical Objects: EXT-SREF, NE-SREF

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

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

FRCDSWTOTHIRD

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

Logical Objects: EXT-SREF, NE-SREF

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

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

FRNGSYNC

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

Logical Object: NE-SREF

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

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

Clear the FRNGSYNC Condition

Procedure

Step 1 If the system is configured to operate from an external timing source, verify that the BITS timing source is valid. Common problems with a BITS timing source include reversed wiring and bad timing cards. Refer to the Timing chapter in the Reference Manual for more information.

Step 2 If the BITS source is valid, clear alarms related to the failures of the primary and secondary reference sources, such as the SYNCPRI , on page 278 alarm and the SYNCSEC , on page 279 alarm.

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

FSTSYNC

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

Logical Object: NE-SREF

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

The FSTSYNC alarm disappears after approximately 30 seconds.

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

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

FTA-MISMATCH

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

Logical Object: EQPT

The Fan Tray Mismatch condition is raised on the ADM-10G card and OTU2_XP. It indicates that an unsupported version of the fan tray assembly is installed in the shelf. The ADM-10G and OTU2_XP card must be installed in a shelf that has FTA version 4 or higher.

Clear the FTA-MISMATCH Condition

Procedure

Obtain the correct fan tray assembly, and replace the existing FTA with the new one by following the Replace the Fan-Tray Assembly, on page 318 procedure.

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

GAIN-HDEG

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

Logical Object: AOTS

The Gain High Degrade alarm is raised on an amplifier card (OPT-AMP-C),when the amplifier reaches the Gain High Degrade Threshold. (This value is automatically provisioned with the gain setpoint, but the alarm threshold is 2 dBm higher than the setpoint.

Note This alarm is applicable only when the amplifier working mode is set to Control Gain.

Clear the GAIN-HDEG Alarm

Procedure

Step 1 Verify that the LED is correctly illuminated on the physical card. A green ACT/SBY LED indicates an active card. A red ACT/SBY LED indicates a failed card.

Step 2 Complete the procedure on the failing amplifier.

Step 3 If the alarm does not clear, identify all the OCHNC circuits applying to the failing card. Force all the protected circuits on the optical path that the faulty amplifier does not belong to. Switch the OCHNC administrative state of all these circuits to **OOS,DSBLD** (or **Locked,disabled**).

Caution All remaining unprotected circuits will suffer for a traffic hit when you disable the circuits.

Step 4 Switch the administrative state of only one of the OCHNC circuits to **IS,AINS** (or **Unlocked,automaticInService**). This forces the amplifier to recalculate its gain setpoint and value.

Step 5 If the alarm does not clear and no other alarms exist that could be the source of the GAIN-HDEG alarm, or if clearing an alarm did not clear the GAIN-HDEG, place all of the card ports in **OOS,DSBLD** (or **Locked,disabled**) administrative state.

Step 6 Complete the Physically Replace a Card, on page 313 procedure for the reporting card.

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 **High-performance devices on this card can get hot during operation. To remove the card, hold it by the faceplate and bottom edge. Allow the card to cool before touching any other part of it or before placing it in an antistatic bag.** Statement 201

Note Before disconnecting any optical amplifier card fiber for troubleshooting, ensure that the optical amplifier card is unplugged.

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

GAIN-HFAIL

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

Logical Object: AOTS

The Gain High Degrade alarm is raised on an amplifier card (OPT-AMP-C) when the amplifier reaches the Gain High Degrade Threshold. (This value is automatically provisioned with the gain setpoint, but the alarm threshold is 5 dBm higher than the setpoint.)

Note This alarm is applicable only when the amplifier working mode is set to Control Gain.

Clear the GAIN-HFAIL Alarm

Procedure

For the alarmed card, complete the Clear the GAIN-HDEG Alarm, on page 101 procedure.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

GAIN-LDEG

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

Logical Object: AOTS

Gain Low Degrade (GAIN-LDEG) alarm is raised on an amplifier card (OPT-BST, OPT-PRE, OPT-AMP-C, or OPT-AMP-17-C), 40-SMR1-C, or 40-SMR2-C card when the amplifier does not reach the Gain Low Degrade Threshold. (This value is automatically provisioned with the gain setpoint, but the alarm threshold is 2 dBm lower than the setpoint.)

Note This alarm is applicable only when the amplifier working mode is set to Control Gain.

Clear the GAIN-LDEG Alarm

Procedure

For the alarmed card, complete the Clear the GAIN-HDEG Alarm, on page 101 procedure.

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

GAIN-LFAIL

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

Logical Object: AOTS

The Gain High Degrade alarm is raised on an amplifier card (OPT-BST, OPT-PRE, OPT-AMP-C, or OPT-AMP-17-C) when the amplifier does not reach Gain High Degrade Threshold. (This value is automatically provisioned with the gain setpoint, but the alarm threshold is 5 dBm lower than the setpoint. If the alarm cannot be cleared, the card must be replaced.

Note This alarm is applicable only when the amplifier working mode is set to Control Gain.

Clear the GAIN-LFAIL Alarm

Procedure

For the alarmed card, complete the Clear the GAIN-HDEG Alarm, on page 101 alarm.

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

GAIN-NEAR-LIMIT

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

Logical Objects: AOTS

The GAIN-NEAR-LIMIT alarm is raised against optical amplifier cards and SMR cards. It is raised when the Automatic Power Control (APC) regulates an amplifier gain and its value reaches +2 or -2 dB, within the minimum and maximum gain range. The gain check is performed automatically every hour and during the APC run.

Clear the GAIN-NEAR-LIMIT Alarm

Procedure

GAIN-NEAR-LIMIT alarm clears in one of these scenarios:

a) To clear the alarm manually, correct the span loss changes from previous configuration. It reduces AMP gain and clears the alarm.
b) The clear the alarm manually, diable the gain limit check by using .
c) The alarm clears automatically when the periodic check determines that the amplifier gain and its value is not in the range of +2 or -2 dB, within the minimum and maximum gain range.

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

GCC-EOC

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

Logical Object: TRUNK, EQPT

The GCC Embedded Operation Channel Failure alarm applies to the optical transport network (OTN) communication channel for TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, TXP_MR_10E_C, TXP_MR_10E_L, MXP_2.5G_10G, MXP_2.5G_10E, ADM-10G, and OTU2_XP cards. The GCC-EOC alarm is raised when the channel cannot operate.

This alarm applies to trunk ports only when ITU-T G.709 encapsulation is enabled and a general communication channel (GCC) has been provisioned between the two TXP/MXP cards.

Clear the GCC-EOC Alarm

Procedure

Complete the "Clear the EOC Alarm" procedure.

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

GE-OOSYNC (FC, GE, ISC)

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

Logical Objects: FC, GE, ISC

The Gigabit Ethernet Out of Synchronization alarm applies to TXP_MR_10G,TXP_MR_10E, TXP_MR_10E_C, TXP_MR_10E_L, TXP_MR_2.5G,TXPP_MR_2.5G,MXP_MR_2.5G, MXPP_MR_2.5G, GE-XP, 10GE, and ADM-10G cards when the Ethernet signal incoming on the Client-Rx port is out of synchronization.

Clear the GE-OOSYNC (FC, GE, ISC) Alarm

Procedure

Step 1 Ensure that the incoming signal from the Client-Rx port is provisioned with the correct physical-layer protocol (Ethernet).

Step 2 Ensure that the line is provisioned with the correct line speed (10G or 1G Ethernet).

Step 3 Verify that the optical power and the optical signal-to-noise range (OSNR) of the incoming Client-Rx port optical signal are within the accepted ranges. You can find XFP/SFP ranges in the Installing the GBIC, SFP, SFP+, and XFP Optical Modules in Cisco ONS Platforms document.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

GE-OOSYNC (TRUNK)

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

Logical Objects: TRUNK

The Gigabit Ethernet Out of Synchronization alarm applies to TXP_MR_10G,TXP_MR_10E, TXP_MR_10E_C, TXP_MR_10E_L, TXP_MR_2.5G,TXPP_MR_2.5G,MXP_MR_2.5G, MXPP_MR_2.5G, GE-XP, 10GE, and ADM-10G cards only when the ITU-T G.709 encapsulation framer is disabled.

Clear the GE-OOSYNC (TRUNK) Alarm

Procedure

Step 1 Verify that ITU-T G.709 encapsulation is disabled:

a) In node view (single-shelf mode) or shelf view (multishelf mode), double-click the card to display the card view.
b) Click the **Provisioning** > **OTN** > **OTN Lines** tabs.
c) If the G.709 OTN column says Enable, choose **Disable** from the drop-down list.
d) Click **Apply**.

Step 2 For the TRUNK-RX port, double-click the card and click the **Performance** > **OTN PM** > **FEC PM** tabs. If post-FEC errors are present, troubleshoot this problem first. If not, move to next step.

Step 3 Verify the status of far-end TXP/MXP connected to the faulty near-end card. Look for any alarms reported by the Client-Rx port of far-end card. If these alarms exist, troubleshoot them.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

GFP-CSF-SIGLOSS

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

Logical Object: GFP-FAC

The GFP Client Signal Fail due to Sigloss is a secondary alarm raised on local GFP data ports when a remote Service-Affecting (SA) alarm causes invalid data transmission. The alarm is raised locally on AR_MXP and AR_XP GFP data ports and does not indicate that a Service-Affecting (SA) failure is occurring at the local site, but that a SIGLOSS alarm caused by an event is affecting a remote data port's transmission capability.

Clear the GFP-CSF-SIGLOSS Alarm

Procedure

Clear the Service-Affecting (SA) alarm at the remote data port.

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

GFP-CSF-SYNCLOSS

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

Logical Object: GFP-FAC

The GFP Client Signal Fail Due to Syncloss alarm is a secondary alarm raised on local GFP data ports when a remote Service-Affecting (SA) alarm causes invalid data transmission. The alarm is raised locally on AR_MXP and AR_XP GFP data ports and does not indicate that a Service-Affecting (SA) failure is occurring at the local site, but that a SYNCLOSS alarm caused by an event such as a pulled receive cable is affecting a remote data port's transmission capability.

Clear the GFP-CSF-SYNCLOSS Alarm

Procedure

Clear the Service-Affecting (SA) alarm at the remote data port.

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

GFP-LFD

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

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

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

Clear the GFP-LFD Alarm

Procedure

Look for and clear any associated SONET path errors such as LOS or the AU-AIS, on page 29 alarm that originate at the transmit node.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into

http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

GFP-UP-MISMATCH

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

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

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

Clear the GFP-UP-MISMATCH Alarm

Procedure

Step 1 Ensure that the transmit port and receive port are identically provisioned for distance extension by completing the following steps:

a) Double-click the card to open the card view.
b) Click the **Provisioning** > **Port** > **Distance Extension** tabs.
c) Check the check box in the **Enable Distance Extension** column.
d) Click **Apply**.

Step 2 Ensure that both ports are set for the correct media type. For each port, complete the following steps:

a) Double-click the card to open the card view (if you are not already in card view).
b) Click the **Provisioning** > **Port** > **General** tabs.
c) Choose the correct media type (**Fibre Channel - 1Gbps ISL**, **Fibre Channel - 2 Gbps ISL**, **FICON - 1 Gbps ISL**, or **FICON - 2 Gbps ISL**) from the drop-down list.
d) Click **Apply**.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

HELLO

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

Logical Object: OCN

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

Clear the HELLO Alarm

Procedure

Ensure that the area ID is correct on the missing neighbor by completing the following steps:

a) In node view, click the **Provisioning** > **Network** > **OSPF** tabs.
b) Ensure that the IP address in the Area ID column matches the other nodes.
c) If the address does not match, click the incorrect cell and correct it.
d) Click **Apply**.

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

HIBATVG

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

Logical Object: PWR

The High Voltage Battery alarm occurs in a –48 VDC environment when a battery lead input voltage exceeds the high power threshold. This threshold, with a default value of –52 VDC, is user-provisionable. The alarm remains raised until the voltage remains under the threshold for 120 seconds.

Clear the HIBATVG Alarm

Procedure

The problem is external to the system. Troubleshoot the power source supplying the battery leads.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

HI-BER

(Supported only in Release 9.2.2)

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

SONET Logical Objects: FC, GE

The High Bit Error Rate (HI-BER) alarm is raised on the OTU2_XP card when the client and trunk ports receive 16 or more invalid sync-headers in 125 microseconds. The HI-BER alarm occurs when the OTU2_XP card is configured with 10 GE or 10 G FC payloads.

Clear the HI-BER Alarm

Procedure

The alarm clears under the following conditions:

- When high bit error rate is not received on the card port.
- When one of the following OTN alarms are raised on the trunk port:
  - LOF (TRUNK)
  - LOM
  - LOS-P (TRUNK)
  - ODUK-AIS-PM
  - ODUK-LCK-PM
  - ODUK-OCI-PM
  - OTUK-AIS

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

HI-CCVOLT

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

Logical Object: BITS

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

Clear the HI-CCVOLT Condition

Procedure

Step 1 Lower the source voltage to the clock.

Step 2 If the condition does not clear, add more cable length or add a 5 dBm attenuator to the cable.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

HI-LASERBIAS

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

Logical Objects: 2R, EQPT, ESCON, FC, GE, ISC, OCN/STMN, PPM, TRUNK

The Equipment High Transmit Laser Bias Current alarm is raised against TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, TXP_MR_10E_C, TXP_MR_10E_L, MXP_2.5G_10G, OC192-XFP, ADM-10G, and OTU2_XP card laser performance. The alarm indicates that the card laser has reached the maximum laser bias tolerance.

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

Clear the HI-LASERBIAS Alarm

Procedure

Complete the Physically Replace a Card, on page 313 procedure. Replacement is not urgent and can be scheduled during a maintenance window.

Warning **High-performance devices on this card can get hot during operation. To remove the card, hold it by the faceplate and bottom edge. Allow the card to cool before touching any other part of it or before placing it in an antistatic bag.** Statement 201

Caution Removing an active card can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the Protection Switching, Lock Initiation, and Clearing, on page 306 section for commonly used traffic-switching procedures.

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

HI-LASERTEMP

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

Logical Objects: EQPT, OCN/STMN, PPM

The Equipment High Laser Optical Transceiver Temperature alarm applies to the TXP, MXP, and ADM-10G cards. HI-LASERTEMP occurs when the internally measured transceiver temperature exceeds the card setting by 35.6 degrees F (2 degrees C). A laser temperature change affects the transmitted wavelength.

When the TXP or MXP card raises this alarm, the laser is automatically shut off. The LOS (OCN/STMN) alarm is raised at the far-end node and the DUP-IPADDR , on page 64 alarm, is raised at the near end.

Clear the HI-LASERTEMP Alarm

Procedure

Step 1 In node view (single-shelf mode) or shelf view (multishelf mode), double-click the TXP or MXP card to open the card view.

Step 2 Click the **Performance** > **Optics PM** > **Current Values** tabs.

Step 3 Verify the card laser temperature levels. Maximum, minimum, and average laser temperatures are shown in the Current column entries in the Laser Temp rows.

Step 4 Complete the Reset a Card in CTC, on page 310 procedure for the MXP or TXP card.

Step 5 If the alarm does not clear, complete the Physically Replace a Card, on page 313 procedure for the reporting MXP or TXP card.

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

HI-RXPOWER

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

Logical Objects: 2R, ESCON, FC, GE, ISC, OCN/STMN, TRUNK, EQPT

The Equipment High Receive Power alarm is an indicator of the optical signal power that is transmitted to the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, TXP_MR_10E_C, TXP_MR_10E_L, MXP_2.5G_10G, OC192-XFP, GE-XP, 10GE-XP, ADM-10G, or OTU2_XP card. HI-RXPOWER occurs when the measured optical power of the received signal exceeds the threshold. The threshold value is user-provisionable.

Clear the HI-RXPOWER Alarm

Procedure

Step 1 Check the PM of the TRUNK-RX port. Verify that received power is above the optics threshold:

a) In node view (single-shelf mode) or shelf view (multishelf mode), double-click the card to display the card view.

b) For the TRUNK-RX port, double-click the card and click the **Performance** > **Optics PM** > **Historical PM** tabs, choose the port in the Port drop-down list, and click **Refresh**.

c) Compare the refreshed PM values with the threshold (ensuring that it is above the threshold value) by clicking the **Performance** > **Optics PM** > **Current Values** tabs.

d) Ensure that a proper threshold has been provisioned for the receive value. If an incorrect threshold has been set, adjust it to a value within the allowed limits. If instead the alarm condition does not clear, move to next step.

Step 2 Verify that the Trunk-Rx port is cabled correctly, and clean the fiber connecting the faulty TXP/MXP to the Drop port of the DWDM card (32DMX, or 40DMX). If no site cleaning practices are available, refer to the fiber cleaning procedure in the Maintain the Node chapter of the Configuration Guide.

Step 3 Determine whether a bulk attenuator is specified by the Cisco Transport Planner design. If so, verify that the proper fixed attenuation value has been used.

Step 4 Using a test set, check the optical power value of the Drop port of the DWDM card (32DMX, or 40DMX) connected to the faulty TXP/MXP. If the read value is different (+1 dBm or 1 dBm) from the ANS setpoint for Padd&drop-Drop power, move to next step.

Step 5 Look for and troubleshoot any alarm reported by the cards belonging to the OCHNC circuit destinating at the faulty TXP/MXP. Possible alarms include amplifier Gain alarms (the GAIN-HDEG , on page 101 alarm, the GAIN-HFAIL , on page 102 alarm, the GAIN-LDEG , on page 102 alarm, or GAIN-LFAIL , on page 103) alarm; APC alarms (APC-CORR-SKIPPED , on page 20 alarm or APC-OUT-OF-RANGE , on page 22 alarm), or LOS-P alarms on the Add or Drop ports involved in the OCHNC circuit.

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

HITEMP

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

Logical Objects: EQPT, NE

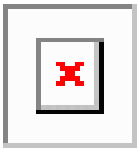
The High Temperature alarm occurs when the temperature of the ONS system is above 122 degrees F (50 degrees C).

Clear the HITEMP Alarm

Procedure

Step 1 View the temperature displayed on the system LCD front panel. For example, the front panel is illustrated in Figure 1: Shelf LCD Panel, on page 114.

Figure 1: Shelf LCD Panel



Step 2 Verify that the environmental temperature of the room is not abnormally high.

Step 3 If the room temperature is not abnormal, physically ensure that nothing prevents the fan-tray assembly from passing air through the system shelf.

Step 4 If airflow is not blocked, physically ensure that blank faceplates fill the system shelf empty slots. Blank faceplates help airflow.

Step 5 If faceplates fill the empty slots, determine whether the air filter needs replacement. Refer to the Inspect, Clean, and Replace the Air Filter, on page 316 procedure.

Step 6 If the fan does not run or the alarm persists, complete the Replace the Fan-Tray Assembly, on page 318 procedure.

Note The fan should run immediately when correctly inserted.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

HI-RXTEMP

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

Logical Objects: TRUNK

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

Clear the HI-RXTEMP Alarm

Procedure

Step 1 If a shelf HITEMP alarm is also present, complete the Clear the HITEMP Alarm.

Step 2 If a HI-LASERTEMP alarm is also present, complete the Clear the HI-LASERTEMP Alarm .

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

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

HI-TXPOWER

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

Logical Objects: 2R, EQPT, ESCON, FC, GE, ISC, OCN/STMN, PPM, TRUNK

The Equipment High Transmit Power alarm is an indicator on the TXP_MR_E, TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, MXP_2.5G_10G, OC192-XFP, ADM-10G, or OTU2_XP card transmitted optical signal power. HI-TXPOWER occurs when the measured optical power of the transmitted signal exceeds the threshold.

Clear the HI-TXPOWER Alarm

Procedure

Step 1 Check the PM of the Trunk-Tx port. Verify that received power is above the optics threshold:

a) In node view (single-shelf mode) or shelf view (multishelf mode), double-click the card to display the card view.

b) For the Trunk-Tx port, double-click the card and click the **Performance** > **Optics PM** > **Historical PM SVO Web Interface** > **SVO Topology** > **Rack View** > **Performance Tab** > **History PM**tabs, choose the port in the Port drop-down list, and click **Refresh**.

c) Compare the refreshed PM values with the threshold (ensuring that it is above the threshold value) by clicking the **Performance** > **Optics PM** > **Current Values SVO Web Interface** > **SVO Topology** > **Rack View** > **Performance Tab** > **PM Live Data**tabs.

d) Ensure that a proper threshold has been provisioned for the receive value. If an incorrect threshold has been set, adjust it to a value within the allowed limits. If instead the alarm condition does not clear, move to next step.

Step 2 Physically verify, by using a standard power meter that the optical output power is overcoming the expected power threshold. If so, the card should be replaced at first opportunity

Note The higher power level is not a major issue for the DWDM card (40MUX, 32WSS-O, or 40WSS-C) connected to the faulty TXP/MXP, because an internal VOA can automatically decrease the optical power to the expected level.

Step 3 Complete the Physically Replace a Card, on page 313 procedure.

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

HLDOVRSYNC

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

Logical Object: NE-SREF

The Holdover Synchronization Mode condition is caused by loss of the primary and second timing references in the node. Timing reference loss occurs when line coding on the timing input is different from the configuration on the node, and it often occurs during the selection of a new node reference clock. The condition clears when primary or second timing is reestablished. After the 24-hour holdover period expires, timing slips could begin to occur on an ONS system relying on an internal clock.

Clear the HLDOVRSYNC Condition

Procedure

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

- FRNGSYNC , on page 99
- FSTSYNC , on page 100
- LOF (BITS) , on page 150
- LOS (BITS) , on page 158
- MANSWTOINT, on page 182
- MANSWTOPRI , on page 182
- MANSWTOSEC , on page 182
- MANSWTOTHIRD , on page 182
- SWTOPRI , on page 276
- SWTOSEC , on page 276
- SWTOTHIRD , on page 277
- SYNC-FREQ , on page 277
- SYNCPRI , on page 278
- SYNCSEC , on page 279
- SYNCTHIRD , on page 280

Step 2 Reestablish a primary and secondary timing source according to local site practice. If none exists, refer to the Turn Up the Network chapter in the Configuration Guide.

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

HP-DEG

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

Logical Object: VMMON-HP, VCTRM-HP

An HP-DEG condition is similar to the SD (TRUNK) , on page 257 condition, but it applies to the HP layer of the SDH overhead. A HP-DEG alarm travels on the B3 byte of the SDH overhead.

For path protection protected circuits, the BER threshold is user-provisionable and has a range for HP-DEG from 1E–9 dBm to 1E–5 dBm. For MS-SPRing 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 HP-DEG condition causes a switch from the working card to the protect card at the path level. On MS-SPRing, 1+1, and on unprotected circuits, an HP-DEG 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.

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

Clear the HP-DEG Condition

Procedure

Complete the Clear the SD (TRUNK) Condition, on page 257 procedure.

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

HP-ENCAP-MISMATCH

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

Logical Object: VCTRM-HP

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

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

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

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

An example situation that would raise an HP-ENCAP-MISMATCH alarm is if a circuit created between two ML-Series cards has GFP framing provisioned on one end and high-level data link control (HDLC) framing with LEX encapsulation provisioned on the other. The GFP framing card transmits and expects a C2 byte of 0x1B, while the HDLC framing card transmits and expects a C2 byte of 0x01.

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

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

This alarm is demoted by a path label mismatch (PLM) such as LP-PLM.

Note By default, an HP-ENCAP-MISMATCH alarm causes an ML-Series card data link to go down. This behavior can be modified using the command-line interface (CLI) command **no pos trigger defect encap**.

Clear the HP-ENCAP-MISMATCH Alarm

Procedure

Step 1 Ensure that the correct framing mode is in use on the receiving card by completing the following steps:

a) In node view, double-click the ML-Series card to display the card view.
b) Click the **Provisioning** > **Card** tabs.
c) In the Mode drop-down list, ensure that the correct mode (GFP-F or HDLC) is selected. If it is not, choose it and click **Apply**.

Step 2 Ensure that the correct framing mode is in use on the transmit card, and that it is identical to the framing mode used on the receiving card by completing the following steps:

a) In node view, double-click the ML-Series card to display the card view.
b) Click the **Provisioning** > **Card** tabs.
c) In the Mode drop-down list, ensure that the same mode (GFP-F or HDLC) is selected. If it is not, choose it and click **Apply**.

Step 3 If the alarm does not clear, use the ML-Series card CLI to ensure that the remaining settings are correctly configured:

- Encapsulation
- CRC size
- Scrambling state

To open the interface, click the card view **IOS** tab and click **Open IOS Connection**.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

HP-EXC

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

Logical Objects: VCMON-HP, VCTRM-HP

An HP-EXC condition is similar to the SF (TRUNK) , on page 261 condition, but it applies to the path layer B3 byte of the SONET overhead. It can trigger a protection switch.

The HP-EXC 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 HP-EXC Condition

Procedure

Complete the Clear the SF (TRUNK) Condition, on page 262 procedure.

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

HP-PLM

The HP-PLM condition is not used in this platform in this release. It is reserved for development.

HP-RFI

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

Logical Object: VCMON-HP

The High-Order Remote Failure Indication (RFI) condition indicates that there is a remote failure indication in the high-order (VC-4 or VC-3) path, and that the failure has persisted beyond the maximum time allotted for transmission system protection. The HP-RFI is sent as the protection switch is initiated. Resolving the fault in the adjoining node clears the HP-RFI condition in the reporting node.

Clear the HP-RFI Condition

Procedure

Step 1 Log into the node at the far end of the reporting NCS.

Step 2 Determine whether there are any related alarms, especially the LOS(STM1E, STMN).

Step 3 Clear the main alarm. See the appropriate alarm section in this chapter for procedures.

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

HP-TIM

Default Severities: Critical (CR), Service-Affecting (SA) for VCTRM-HP; Minor (MN), Non-Service-Affecting (NSA) for VCMON-HP

Logical Objects: VCMON-HP, VCTRM-HP

The TIM High-Order TIM Failure alarm indicates that the trace identifier J1 byte of the high-order (VC-4 or VC-3) overhead is faulty. HP-TIM occurs when there is a mismatch between the transmitted and received J1 identifier byte in the SONET path overhead. The error can originate at the transmit end or the receive end.

Clear the HP-TIM Alarm

Procedure

Step 1 Use an optical test set capable of viewing SONET path overhead to determine the validity of the J1 byte. For specific procedures to use the test set equipment, consult the manufacturer. Examine the signal as near to the reporting card as possible.

- Examine the signal as close as possible to the output card.

Step 2 If the output card signal is valid, complete the Clear the SYNCPRI Alarm, on page 279 procedure.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

HP-UNEQ

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

Logical Object: VCMON-HP, VCTRM-HP

The signal label mismatch fault (SLMF) Unequipped High-Order Path alarm applies to the C2 path signal label byte in the high-order (VC-4) path overhead. HP-UNEQ occurs when no C2 byte is received in the SONET path overhead.

Clear the HP-UNEQ Alarm

Procedure

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Right-click the alarm to display the Select Affected Circuits shortcut menu.

Step 3 Click **Select Affected Circuits**.

Step 4 When the affected circuits appear, look in the Type column for a virtual circuit (VC).

Step 5 If the Type column does not contain a VC, there are no VCs. Go to Step 7, on page 121.

Step 6 If the Type column does contain a VC, attempt to delete these row(s) by completing the following steps:

Note The node does not allow you to delete a valid VC.

a) Click the VC row to highlight it. Complete the Delete a Circuit, on page 314 procedure.
b) If an error message dialog box appears, the VC is valid and not the cause of the alarm.
c) If any other rows contain VT, repeat Steps 6.a, on page 121through 6.b, on page 121.

Step 7 If all ONS nodes in the ring appear in the CTC network view, verify that the circuits are all complete by completing the following steps:

a) Click the **Circuits** tab.
b) Verify that INCOMPLETE is not listed in the Status column of any circuits.

Step 8 If you find circuits listed as incomplete, verify that these circuits are not working circuits that continue to pass traffic, using an appropriate optical test set and site-specific procedures. For specific procedures to use the test set equipment, consult the manufacturer.

Step 9 If the incomplete circuits are not needed or are not passing traffic, delete the incomplete circuits.

Complete the Delete a Circuit, on page 314 procedure.

Step 10 Recreate the circuit with the correct circuit size. Refer to the Create Circuits and Tunnels chapter in the configuration guide for circuit procedures.

Step 11 Log back in and verify that all circuits terminating in the reporting card are active by completing the following steps:

a) Click the **Circuits** tab.

b) Verify that the **Status** column lists all circuits as active.

Step 12 If the alarm does not clear, clean the far-end optical fiber according to site practice. If no site practice exists, complete the procedure in the Maintain the Node chapter in the Configuration guide.

On the OC192 LR/STM64 LH 1550 card:

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

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

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

Step 13 If the alarm does not clear, complete the Physically Replace a Card, on page 313 procedure for the optical and/or electrical cards.

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.

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

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

I-HITEMP

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

Logical Object: NE

The Industrial High Temperature alarm occurs when the temperature of the ONS system is above 149 degrees F (65 degrees C) or below –40 degrees F (–40 degrees C). This alarm is similar to the HITEMP , on page 113 alarm but is used for the industrial environment. If this alarm is used, you can customize your alarm profile to ignore the lower-temperature HITEMP alarm.

Clear the I-HITEMP Alarm

Procedure

Complete the Clear the HITEMP Alarm, on page 114 procedure.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

ILK-FAIL

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

Logical Object: TRUNK

The ADM Peer Group Interlink Failure condition is raised on the ADM-10G card. This condition occurs when one of the following SONET/OTN alarms is detected on the interlink ports of the ADM-10G card.

- LOS (TRUNK) , on page 162 alarm
- LOF (TRUNK) , on page 151 alarm
- SF (TRUNK) , on page 261 alarm

Clear the ILK-FAIL Alarm

Procedure

Clear the root-cause service-affecting alarm by using one of the following procedures, as appropriate:

- Clear the LOS (TRUNK) Alarm, on page 163 procedure
- Clear the LOF (TRUNK) Alarm, on page 152 procedure
- Clear the SF (TRUNK) Condition, on page 262 procedure

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

IMPROPRMVL

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

Logical Objects: EQPT, PPM

The Improper Removal (IMPROPRMVL) alarm occurs under the following conditions:

- A card is removed when the card was rebooting. It is recommended that after the card completely reboots, delete the card in CTC and only then remove the card physically. When you delete the card, CTC loses connection with the node view (single-shelf mode) or shelf view (multishelf mode), and goes to network view.
- When a card is deleted from CTC before physically removing the card from its slot. It is recommended that the card be physically removed from its slot before deleting it from CTC.

Note CTC provides the user approximately 15 seconds to physically remove the card before it begins rebooting the card.

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

- A card is inserted into a slot but is not fully plugged into the backplane.
- A PPM (SFP) is provisioned but the physical module is not inserted into the port.
- Removal of an SFP from the client ports of a Y-cable protection group card causes an IMPROPRMVL (PPM) alarm.

  The working port raises the CR,IMPROPRMVL,SA alarm and the protected port raises the MN,IMPROPRMVL,NSA alarm. The severity on the client ports is changed according to the protection switch state.
- Electrical issues such as short circuit or failure of DC-DC conversion.

Clear the IMPROPRMVL Alarm

Procedure

Step 1 In node view (single-shelf mode) or shelf view (multishelf mode), right-click the card reporting the IMPROPRMVL.

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

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

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

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

a) In node view (single-shelf mode) or shelf view (multishelf mode), double-click the reporting card to open the card view.
b) Click the **Provisioning** > **Line** tabs.
c) Click the Admin State column of any in-service (IS) ports.
d) Choose **OOS,MT** (or **Locked,maintenance**) to take the ports out of service.

Step 4 If a circuit has been mapped to the card, complete the Delete a Circuit, on page 314 procedure.

Caution Before deleting the circuit, ensure that the circuit does not carry live traffic.

Step 5 If the card is paired in a protection scheme, delete the protection group by completing the following steps:
a) Click **View** > **Go to Previous View** to return to node view (single-shelf mode) or shelf view (multishelf mode).
b) If you are already in node view (single-shelf mode) or shelf view (multishelf mode), click the **Provisioning** > **Protection** tab.
c) Click the protection group of the reporting card.
d) Click **Delete**.

Step 6 If the card is provisioned for DCC, delete the DCC provisioning by completing the following steps:
a) In node view (single-shelf mode) or multishelf view (multishelf mode), click the ONS system **Provisioning** > **Comm Channels** > **SDCC** (or **Provisioning** > **Comm Channels** > **MS DCC**) tabs.
b) Click the slots and ports listed in DCC terminations.
c) Click **Delete** and click **Yes** in the dialog box that appears.

Step 7 If the card is used as a timing reference, change the timing reference by completing the following steps:
a) In node view (single-shelf mode) or shelf view (multishelf mode), click the **Provisioning** > **Timing** > **General** tabs.
b) Under NE Reference, click the drop-down arrow for **Ref-1**.
c) Change Ref-1 from the listed OC-N/STM-N card to **Internal Clock**.
d) Click **Apply**.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

INHSWPR

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

Logical Object: EQPT

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

Clear the INHSWPR Condition

Procedure

Step 1 If the condition is raised against a 1+1 port, complete the Initiate a 1+1 Manual Switch Command, on page 307 procedure.

Step 2 If it is raised against a 1:1 card, complete the Initiate a 1:1 Card Switch Command, on page 307 procedure to switch it back.

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

INHSWWKG

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

Logical Object: EQPT

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

Clear the INHSWWKG Condition

Procedure

Step 1 If the condition is raised against a 1+1 port, complete the Initiate a 1+1 Manual Switch Command, on page 307 procedure.

Step 2 If it is raised against a 1:1 card, complete the Initiate a 1:1 Card Switch Command, on page 307 procedure to switch it back.

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

INCOMPATIBLE-SEND-PDIP

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

Logical Object: SYSTEM

The Incompatible Software alarm is raised when CTC send PDI-P provisioning differs from the host node's provisioning.

Clear the INCOMPATIBLE-SEND-PDIP Alarm

Procedure

Reconfigure CTC send PDI-P alarm capability to align with the host node settings.

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

INCOMPATIBLE-SW

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

Logical Object: SYSTEM

The Incompatible Software alarm is raised when CTC cannot connect to the NE due to differing, incompatible versions of software between CTC and the NE. The alarm is cleared by restarting CTC in order to redownload the CTC JAR files from the NE.

The INCOMPATIBLE-SW alarm is also raised when CTC nodes in the network have R10.6 packages and earlier and password policy is greater than 80 characters (127 characters).

Clear the INCOMPATIBLE-SW Alarm

Procedure

Restart the CTC application.

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

INTRUSION-PSWD

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

Logical Object: NE

The Security Intrusion Incorrect Password condition occurs after a user attempts a provisionable (by Superuser) number of unsuccessful logins, a login with an expired password, or an invalid password. The alarmed user is locked out of the system, and INTRUSION-PSWD condition is raised. This condition is only shown in Superuser login sessions, not in login sessions for lower-level users. The INTRUSION-PSWD condition is automatically cleared when a provisionable lockout timeout expires, or it can be manually cleared in CTC by the Superuser if the lockout is permanent.

Clear the INTRUSION-PSWD Condition

Procedure

Step 1 Log in as a user ID with superuser rights. (For more information about this, refer to the Connect the PC and Log Into the GUI chapter in the *Cisco ONS 15454 DWDM Procedure Guide*Connect the PC and Log into the GUI document.)

Step 2 In node view (single-shelf mode) or multishelf view (multishelf mode), click the .

Step 3 Click **Clear Security Intrusion Alarm**.

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

INVALID-SYSDB

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

Logical Object: EQPT

An Invalid SYSDB alarm is raised when the valid system DB file is not available on the controller card.

Clear the INVALID-SYSDB Alarm

Procedure

Step 1 Soft Reboot the ACT controller card if reported on Active.

Step 2 Soft Reboot the Standby card if reported on Standby.

Step 3 If the alarm is raised on Active and Standby at the same instance, contact TAC.

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

INVALID-MUXCONF

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

Logical Object: EQPT

The INVALID-MUXCONF alarm is raised when the 10x10G muxponder operation mode is created between an unlicensed 10x10G-LC card and a licensed 100G-LC-C card.

Clear the INVALID-MUXCONF Alarm

Procedure

Replace the unlicensed 10x10G-LC card with a licensed 10x10G-LC card.

To replace the card, complete the procedure "Physically Replace a Card, on page 313".

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

INVMACADR

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

Logical Objects: AIP, BP

The Invalid MAC Address alarm occurs when the system MAC address is invalid. Each system has a unique, permanently assigned MAC address. The address resides on an AIP or backplane EEPROM. BP or backplane applies to NCS 2002, NCS 2006, and NCS 2015 chassis. The control cards read the address value from the AIP or backplane chip during boot-up and keeps this value in its synchronous dynamic RAM (SDRAM).

An invalid MAC address can be caused when:

- There is a read error from the backplane EEPROM during boot-up. The TNC/TNCE/TSCE/TNCS/TNCS-O cards use the default MAC address (00:11:22:33:44:55).
- There is a read error occurring on one of the redundant control cards that read the address from the backplane; these cards read the address independently and could therefore each read different address values.

Clear the INVMACADR Alarm

Procedure

Step 1 Complete the Resetting the Controller Card procedure for TNC/TNCE/TSC/TSCE/TNCS/TNCS-O cards.

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

Step 2 If the reset card has not rebooted successfully, or the alarm has not cleared, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

IMPROPRMVL-FS

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

Logical Objects: PSHELF

The Improper Removal of Fiber Shuffle (IMPROPRMVL-FS) condition occurs when a provisioned and associated Passive Shelf is unplugged from its USB Port. It occurred due to an improper removal of the device.

The condition will clears when the Passive Shelf is plugged back in the USB port. This transient condition does not result in a standing condition.

IPC-LASER-FAIL

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

Logical Objects: EQPT

The Internal Patch-cord Connection (IPC) Laser Fail alarm is raised when the laser fails to produce output power. The laser failure is detected when the laser is powered up. The laser is embedded inside 20SMR FS CV card for connection verification.

The alarm is cleared automatically when laser output power is detected during or after a power module reset.

IPC-LOOPBACK-MISS

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

Logical Objects: OTS

The Internal Patchcord Connection (IPC) Loopback Miss alarm is raised when the MF-DEG-5-CV, MF-UPG-4-CV, or MF-M16LC-CV modules contain one or more than one disconnected port (port without a patchcord cord or loopback cap). These passive modules are provided with loopback cap on disconnected ports in order to pre-test all possible optical paths inside the node. The uninstalled loopback will raise the alarm.

A false IPC-LOOPBACK-MISS alarm is raised if, a fibre inside an MPO has a very high insertion loss.

Clear the IPC-LOOPBACK-MISS Alarm

Procedure

To clear the IPC-LOOPBACK-MISS alarm, do one of the below mentioned steps, as required:

a) Replace the missing loopback cap on the disconnected port.
b) Install a patchcord on the disconnected port if you cannot replace the missing loopback. Update the node IPC list .

The alarm will be cleared during the nest manual/automatic connection verification. The automatic connection verification occurs every six hours.

If the troubleshooting procedure does not clear the alarm, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html or call the Cisco Technical Assistance Center (1 800 553-2447) to report the problem.

IPC-VERIFICATION-DEGRADE

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

Logical Objects: NE

The Internal Patchcord Connection (IPC) Verification Degrade condition occurs when the connection verification detects a minor problem in the internal patchcords that includes:

- A minimum of one patchcord with insertion loss more than minor degrade threshold and less than major degrade threshold
- A minimum of one patchcord is in Not Measurable state.

For more information on connection verification procedure, refer to NTP-G356 Verify Connections in Optical Cables.

The condition is cleared automatically when no minor problem is detected during the connection verification process.

IPC-VERIFICATION-FAIL

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

Logical Objects: NE

The Internal Patchcord Connection (IPC) Verification Fail condition occurs when the connection verification detects a major problem in the internal patchcords that includes:

- A minimum of one patchcord is disconnected
- A minimum of one patchcord with insertion loss greater than the major degrade threshold (measured loss is greater than 3 dBm).

Note 1 dBm (degrade) and 3 dBm (fail) are the default threshold values, these are the NE default values and can be changed in the range from 0 dBm to 20 dBm.

For more information on connection verification procedure, refer to NTP-G356 Verify Connections in Optical Cables.

The condition is cleared automatically when no major problem is detected during the connection verification process.

ISIS-ADJ-FAIL

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

Logical Object: OCN

The Open System Interconnection (OSI) Intermediate System to Intermediate-System (IS-IS) Adjacency Failure alarm is raised by an intermediate system (node routing IS Level 1 or Level 1 and 2) when no IS or end system (ES) adjacency is established on a point-to-point subnet. The Intermediate-System Adjacency Failure alarm is not supported by ES. It is also not raised by IS for disabled routers.

The alarm is typically caused by a misconfigured router manual area adjacency (MAA) address.

Clear the ISIS-ADJ-FAIL Alarm

Procedure

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

a) At the local node, in node view, click the **Provisioning** > **Comm Channels** >**MSDCC** tabs.
b) Click the row of the circuit. Click **Edit**.
c) In the Edit MSDCC termination dialog box, view and record the following selections: Layer 2 protocol (LAPD or PPP); Mode radio button selection (AITS or UITS); Role radio button selection (Network or User); MTU value; T200 value, and T203 selections.
d) Click **Cancel**.
e) Log in to the remote node and follow the same steps, also recording the same information for this node.

Step 2 If both nodes do not use the same Layer 2 settings, you will have to delete the incorrect termination and recreate it. To delete it, click the termination and click **Delete**. To recreate it, refer to the Turn Up Node chapter in the Configuration guide for the procedure.

Step 3 If the nodes use PPP Layer 2, complete the Clear the RS-EOC Alarm, on page 255 procedure. If the alarm does not clear, go to Step 7, on page 132.

Step 4 If both nodes use the LAPD Layer 2 protocol but have different Mode settings, change the incorrect node entry by clicking the correct setting radio button in the Edit MSDCC termination dialog box and clicking **OK**.

Step 5 If the Layer 2 protocol and Mode settings are correct, ensure that one node is using the Network role and the other has the User role. If not (that is, if both have the same mode settings), correct the incorrect one by clicking the correct radio button in the Edit MSDCC termination dialog box and clicking **OK**.

Step 6 If the Layer 2, Mode, and Role settings are correct, compare the MTU settings for each node. If one is incorrect, choose the correct value in the Edit MSDCC dialog box and click **OK**.

Step 7 If all of the preceding settings are correct, ensure that OSI routers are enabled for the communications channels at both ends by completing the following steps:

a) Click **Provisioning** > **OSI** > **Routers** > **Setup**.
b) View the router entry under the **Status** column. If the status is Enabled, check the other end.
c) If the Status is Disabled, click the router entry and click **Edit**.
d) Check the **Enabled** check box and click **OK**.

Step 8 If the routers on both ends are enabled and the alarm still has not cleared, ensure that both ends of the communications channel have a common MAA by completing the following steps:

a) Click the **Provisioning** > **OSI** > **Routers** > **Setup** tabs.
b) Record the primary MAA and secondary MAAs, if configured.

Tip You can record long strings of information such as the MAA address by using the CTC export and print functions. Export it by choosing File > Export > html. Print it by choosing File > Print.

c) Log into the other node and record the primary MAA and secondary MAAs, if configured.
d) Compare this information. There should be at least one common primary or secondary MAA in order to establish an adjacency.
e) If there is no common MAA, one must be added to establish an adjacency. Refer to the Turn Up Node chapter of the Configuration guide for procedures to do this.

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

IPC-VERIFICATION-RUNNING

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

Logical Objects: EQPT

The Internal Patchcord Connection (IPC) Verification Running alarm is raised when the patchcord verification tasks start.

Clear the IPC-VERIFICATION-RUNNING Alarm

Procedure

This alarm is cleared automatically when the patchcord verification tasks are complete.

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

KEY-EX-FAIL

Default Severity: Major (MJ)

Logical Object: TRUNK (OTU)

The Key Exchange Fail (KEY-EX-FAIL) alarm is raised on the OTU trunk port of the WSE card when the source and destination WSE cards do not exchange primary keys used for encryption.

Note The KEY-EX-FAIL alarm is raised and cleared(within one minute) during provision or de-provision of Corresponding Client Payload on the 400G-XP-LC card. This is a known behaviour.

Note The KEY-EX-FAIL alarm is raised on the trunk port. However, there is no correlation with the OTN alarms that are raised on the trunk.

Note The KEY-EX-FAIL alarm is raised on the 400G-XP-LC, MR-MXP, and WSE cards when the near-end node has older release and the far-end node has R11.12 or vice versa and encryption is enabled between the nodes. However, the encrypted traffic is not affected.

This alarm may be raised during these scenarios:

- A loss of signal on a fibre that may occur during key exchange. This results in failure of primary key exchange.
- Bit errors on the line during key exchange.
- Incorrect configuration of destination IP address, destination port or both in **Provisioning** > **Encryption** > **GCC2 Settings** in CTC.
- Card authentication enabled on one end and disabled on the other end.

Clearing the KEY-EX-FAIL Alarm

Note To clear the alarm raised on the 400G-XP-LC, MR-MXP, and WSE cards due to mismatch of release between near-end and far-end nodes running encrypted traffic, upgrade the node having lower release to R11.12.

Before you begin

You must have Security user or Security super user privileges to clear the alarm.

Procedure

Step 1 Ensure that there are no alarms on the client or trunk ports. This is because a loss of synchronization in the client port may result in an AIS in the trunk port, which in turn cascades on the TLS.

Step 2 Reset the primary key from CTC:

a) In node view (single shelf mode), or shelf view (multi-shelf mode), double-click the WSE card for which you want to reset the primary key.
b) Go to **Provisioning** > **Encryption** > **Key Management**.
c) Click the **Reset Master Key** button for the port to reset the primay key.

d) Click **Apply**.

If the troubleshooting procedure does not clear the alarm, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html or call the Cisco Technical Assistance Center (1 800 553-2447) to report the problem.

KEY-WRITE-FAIL

Default Severity: Major (MJ)

Logical Object: TRUNK (OTU)

The Key Write Failure alarm is raised on the OTU trunk port in the WSE card. This alarm is raised when the programming of the key to the crypto FPGA fails.

Clearing the KEY-WRITE-FAIL Alarm

Before you begin

You must have Security user or Security super user privileges to clear the alarm.

Procedure

Step 1 In node view (single shelf mode), or shelf view (multi-shelf mode), double click the WSE card for which you want to reset the primary key.

Step 2 Go to **Provisioning** > **Encryption** > **Key Management**.

Step 3 Click the **Reset Master Key** button for the port to reset the primary key.

Step 4 Click **Apply**.

If the troubleshooting procedure does not clear the alarm, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html or call the Cisco Technical Assistance Center (1 800 553-2447) to report the problem.

LASER-APR

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

Logical Object: AOTS

The Laser Automatic Power Reduction (APR) alarm condition is raised by OPT-AMP-C, and OPT-AMP-17-C cards when the laser is working in power reduction mode. The condition clears as soon as safety conditions are released and the power value reaches the normal setpoint.

Warning Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments. Statement 1051.

Note Only inactivate the APR function temporarily for installation or maintenance reasons. Activate APR immediately after maintenance or installation.

Note LASER-APR is an informational condition and does not require troubleshooting.

LASER-OFF-WVL-DRIFT

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

Logical Objects: OCN, TRUNK, CLIENT

The Laser shutdown due to wavelength drift condition is raised when the transmit wavelength of the ONS-XC-10G-C XFP drifts beyond the threshold limit. This causes the TX laser to shut down to avoid transmitting a wavelength that is not provisioned in the network.

Clear the LASER-OFF-WVL-DRIFT Condition

Procedure

Provision a different wavelength or replace the affected ONS-XC-10G-C XFP. Refer to the NTP-G326 Install, Provision, and Delete PPMs section in the Installing the GBIC, SFP, SFP+, and XFP Optical Modules in Cisco ONS Platforms to replace the affected XFP.

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

LASERBIAS-DEG

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

Logical Objects: AOTS, OTS

The Laser Bias Current Degrade alarm occurs on an amplifier card (OPT-AMP-C when laser aging causes a degrade, but not failure, of laser transmission.

Clear the LASERBIAS-DEG Alarm

Procedure

For the alarmed card, complete the Physically Replace a Card, on page 313 procedure.

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

Note Before disconnecting any optical amplifier card fiber for troubleshooting, ensure that the optical amplifier card is unplugged.

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

LASERBIAS-FAIL

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

Logical Object: AOTS

The Laser Bias Current Failure alarm occurs on an amplifier card (OPT-AMP-C) when the laser control circuit fails or if the laser itself fails service.

Clear the LASERBIAS-FAIL Alarm

Procedure

For the alarmed card, complete the Physically Replace a Card, on page 313 procedure.

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

Note Before disconnecting any optical amplifier card fiber for troubleshooting, ensure that the optical amplifier card is unplugged.

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

LASEREOL

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

Logical Object: OCN

The Laser Approaching End of Life alarm applies to cards. It is typically accompanied by the HI-LASERBIAS , on page 111 alarm. It is an indicator that the laser in the card must be replaced. How soon the replacement must happen depends upon the HI-LASERBIAS alarm threshold. If the threshold is set under 100 percent, the laser replacement can usually be done during a maintenance window. But if the HI-LASERBIAS threshold is set at 100 percent and is accompanied by data errors, LASEREOL indicates the card must be replaced sooner.

Clear the LASEREOL Alarm

Procedure

Complete the Physically Replace a Card, on page 313 procedure.

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

LASERTEMP-DEG

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

Logical Object: AOTS

The Laser Temperature Degrade alarm occurs when the Peltier control circuit fails on an amplifier card OPT-AMP-C). The Peltier control provides cooling for the amplifier.

Clear the LASERTEMP-DEG Alarm

Procedure

For the alarmed card, complete the Physically Replace a Card, on page 313 procedure.

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

Note Before disconnecting any optical amplifier card fiber for troubleshooting, ensure that the optical amplifier card is unplugged.

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

LICENSE-EXPIRED

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

Logical Object: EQPT

The License Expired (LICENSE-EXPIRED) alarm is raised when an evaluation license or a temporary license expires and there is no other valid license installed on the device.

Traffic continues to flow even after this alarm is raised. However, the traffic will stop once the CPT 50 panel, TNC card, TSC card, fabric card, or line card is resetthe licensed card or the controller card is reset, or there is a side-switch of the controller card. To prevent traffic disruption, ensure that a valid license is installed on the device.

Traffic on the base functionality is not affected when LICENSE-EXPIRED alarm is raised.

Clear the LICENSE-EXPIRED Alarm

The LIC-EXPIRED alarm clears in one of the following scenarios:

- When the user discontinues or disables the associated feature that raised the license expired alarm. After this alarm clears, the line card resumes normal operation. The line card maintains the associated license status as expired and does not raise an alarm.
- When a switchover of control card or soft reboot/hard reboot of the target line card is performed. After the reboot, the card raises an LIC-MISSING.
- When a permanent license is installed.

Procedure

Procure and install a permanent license. For more information on installing a license, see the Licensing Configuration Guide.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

LIC-EXPIRING-SHORTLY

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

Logical Object: EQPT

The License Expiring Shortly (LIC-EXPIRING-SHORTLY) alarm is raised when the cumulative validity period of the existing evaluation and temporary licenses is in the range of 0 to 24 hours.

An evaluation license and multiple temporary licenses can co-exist on a device and the validity period of each license can vary.

Clear the LIC-EXPIRING-SHORTLY Alarm

Procedure

Procure and install a permanent license. For more information on installing a license, see the Licensing Configuration guide.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

LIC-EXPIRING-SOON

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

Logical Object: EQPT

The License Expiring Soon (LIC-EXPIRING-SOON)alarm is raised when the cumulative validity period of the existing evaluation and temporary licenses is in the range of 1 to 14 days.

An evaluation license and multiple temporary licenses can co-exist on a device and the validity period of each license can vary.

Clear the LIC-EXPIRING-SOON Alarm

Procedure

Procure and install a permanent license. For more information on installing a license, see the Licensing Configuration guide.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

LIC-MISSING

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

Logical Object: PORT

The License Missing (LIC-MISSING) alarm is raised when a valid license on the one Gigabit Ethernet port of the CPT 50 panel licensed port expires.

Clear the LIC-MISSING Alarm

Procedure

Procure and install a valid license for the one Gigabit Ethernet port on CPT 50 panelport. For more information on installing a license, see the Licensing Configuration guide.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

LMP-FAIL

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

Logical Object: GE

The Link Management Protocol Fail alarm is raised by the control card when an LMP control channel fails or when there is a traffic engineering (TE) link correlation error. When the alarm is raised against a control channel, it uses a control channel (CTRLx) AID. When the alarm is raised against a TE link, a TE link AID (TLINKx) is used.

The alarm clears when the control channel or TE link is restored.

Note LMP-FAIL occurs independently of the condition hierarchy between LMP-SD, on page 143, LMP-SF, on page 144, or LMP-UNALLOC, on page 145.

Note When the LMP-FAIL alarm is reported against a control channel (CTRLx) AID, it only refers to control channel failure. It does not directly indicate data link or traffic engineering link status.

Note When the LMP-FAIL alarm is reported against a TE link AID (TLINKx), it refers only to TE link status, not to control channel or data link status.

Clear the LMP-FAIL Alarm

Procedure

Step 1 Verify the AID (CTRLx or TLINKx) of the alarm.

Step 2 If the alarm is against the control channel AID, this is caused by mismatched control channel parameters between the near-end NCS and the far-end node (which may be another vendor's equipment). Complete the following steps:

a) Determine whether both near-end and far-end sides of the control channel are in the IS administrative state:

- Click the **Provisioning** > **Comm Channels** > **LMP** > **Control Channels** tabs and view the Admin State column content for the channel.
- If the status does not say IS, change it and click **Apply**.

b) Determine whether the near-end node LMP configuration contains the far-end node's IP address as its remote node IP. Also verify that the near-end node's LMP configuration uses the LMP node ID as its own remote node ID. If one or more of these values is incorrect, enter it correctly.

c) Determine whether the far-end node LMP configuration contains the near-end node's IP address as its remote node IP. Also verify that the far-end node's LMP configuration uses the LMP node ID as its own remote node ID. If one or more of these values is incorrect, enter it correctly.

d) Verify that the far-end node is using the near-end node's IP address as its remote node IP address, and that the far end is also using the LMP node ID as its remote node ID. Update the far end's values if they are incorrect.

Step 3 If instead the alarm is raised against the TE link AID, complete the following steps:

a) Determine whether both near-end and far-end sides of the TE link are in the IS administrative state. If either end is currently down, update its administrative state to IS:

- Click the **Provisioning** > **Comm Channels** > **LMP** > **TE links** tab.
- If the status does not say IS, change it and click **Apply**.

b) Determine whether the near-end node's remote TE link ID matches the far-end node's local TE link ID. If the near-end node's remote value is incorrect, enter it correctly.

c) Determine whether the far-end node's remote TE link ID corresponds to the near-end node's local TE link ID. If the far-end node's remote value is incorrect, enter it correctly.

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

LMP-SD

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

Logical Object: GE

The LMP Data Link Signal Degrade condition occurs for when the control card receives an LMP link summary or channel status message that the control channel is not available from the far end, so the data link level of service is not guaranteed. The degrade range is provisionable.

LMP-SD clears when the control card receives a link summary or channel status message reporting that the data link is in the Signal Okay (OK) state.

LMP-SD is part of an alarm hierarchy that includes LMP-SF, on page 144, and LMP-UNALLOC, on page 145. The hierarchy is as follows: If LMP-UNALLOC is raised, LMP-SF and LMP-SD are suppressed. If LMP-SF is raised, it suppresses LMP-SD. LMP-SF and LMP-UNALLOC both suppress near-end LOS-type alarms for DWDM clients. LMP-SD, however, does not suppress LOS alarms.

This condition clears when the far-end trouble has been cleared.

Clear the LMP-SD Condition

Procedure

Look for and clear any of the following alarms in Table 2: Transponder Trunk Alarms that Cause LMP-SD, on page 143 and Table 3: Transponder Client Alarm that Causes LMP-SD, on page 143 occurring on the far-end port.

Table 2: Transponder Trunk Alarms that Cause LMP-SD

Trunk Port Alarm	LMP Failure	Direction
SD	SD	Tx
OTUK-SD	SD	Tx
ODUK-SD-PM	SD	Tx
ODUK-SD-TCM1	SD	Tx
ODUK-SD-TCM2	SD	Tx

Table 3: Transponder Client Alarm that Causes LMP-SD

Client Port Alarm	LMP Failure	Direction
SD	SD	Rx

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

LMP-SF

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

Logical Object: GE

The LMP Data Link Signal Fail condition notifies the near-end user of a far-end problem (and thus is NSA for the near end). The near-end control card receives an LMP link summary or channel status message that the data link service has failed. The signal fail threshold provisionable.

LMP-SF clears when the control card receives a link summary or channel status message reporting that the data link is in the Signal Okay (OK) state.

LMP-SF is part of an alarm hierarchy that includes LMP-SD, on page 143, and LMP-UNALLOC, on page 145. The hierarchy is as follows: If LMP-UNALLOC is raised, LMP-SF and LMP-SD are suppressed. If LMP-SF is raised, it suppresses LMP-SD. LMP-SF and LMP-UNALLOC both suppress near-end LOS-type alarms for DWDM clients, but LMP-SD does not suppress LOS-type alarms.

This condition clears when the far-end trouble has been cleared.

Clear the LMP-SF Condition

Procedure

Look for and clear any of the following alarms in Table 4: Transponder Card Alarms that Cause LMP-SF, on page 144, Table 5: Transponder Trunk Alarms that Cause LMP-SF, on page 144, or Table 6: Transponder Client Alarms that Cause LMP-SF, on page 145 occurring on the far-end port.

Table 4: Transponder Card Alarms that Cause LMP-SF

Card Alarm	LMP Failure	Direction
EQPT	SF	Tx
IMPROPRMVL	SF	Tx

Table 5: Transponder Trunk Alarms that Cause LMP-SF

Trunk Port Alarm	LMP Failure	Direction
LOS	SF	Tx
OTUK-LOF	SF	Tx
OTUK-AIS	SF	Tx

Trunk Port Alarm	LMP Failure	Direction
LOM	SF	Tx
OTUK-SF	SF	Tx
ODUK-SF-PM	SF	Tx
ODUK-SF-TCM1	SF	Tx
ODUK-SF-TCM2 SF	SF	Tx
FEC-MISM	SF	Tx

Table 6: Transponder Client Alarms that Cause LMP-SF

Client Alarm	LMP Failure	Direction
LOS	SF	Rx
SIGLOSS	SF	Rx
SYNCLOSS	SF	Rx
CARLOSS	SF	Rx
LOF	SF	Rx

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

LMP-UNALLOC

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

Logical Object: GE

The LMP Data Link Unallocated condition is raised when the control card receives an LMP link summary or channel status message reporting that the data link as unallocated for data traffic. The condition clears when the data link is allocated and sends an LMP link summary or channel status message to this effect. If a data link has the LMP-UNALLOC alarm raised against it, this should suppress all other alarms on the client port, since the far-end node is not using the errored port. (Consequently you do not have to clear any alarms on the far-end node unused port.)

LMP-UNALLOC is part of an alarm hierarchy that includes LMP-SD, on page 143, and LMP-SF, on page 144. The hierarchy is as follows: If LMP-UNALLOC is raised, LMP-SF and LMP-SD are suppressed. If LMP-SF is raised, it suppresses LMP-SD. LMP-SF and LMP-UNALLOC both suppress near-end LOS-type DWDM client alarms, but LMP-SD does not.

In most cases, this condition is an informational notice at the near-end node that the far-end port is not being utilized. If, however, the far-end port should be allocated for traffic, log into the Technical Support Website

at http://www.cisco.com/cisco/web/support/index.html for more information or call Cisco TAC (1 800 553-2447)..

LOCAL-CERT-CHAIN-VERIFICATION-FAILED

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

Logical Object: EQPT

The Local Certificate Chain Verification Failed alarm is raised when the verification of an active certificate chain in the card fails.

Clear the LOCAL-CERT-CHAIN-VERIFICATION-FAILED Alarm

Procedure

This alarm is cleared when the verification of an active certificate chain in the card is pass.

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

LOCAL-CERT-ISSUED-FOR-FUTURE-DATE

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

Logical Object: EQPT

The Local Certificate Issued for Further Date alarm is raised when the validity time of the active certificate chain is greater than the node time.

Clear the LOCAL-CERT-ISSUED-FOR-FUTURE-DATE Alarm

Procedure

This alarm is cleared when the validity time of the active certificate chain is less than or equal to the node time.

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

LOCAL-CERT-EXPIRING-WITHIN-30-DAYS

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

Logical Object: EQPT

The Local Certificate Expiring Within 30 Days alarm is raised when the validity time of the active certificate chain expires within 30 days.

Clear the LOCAL-CERT-EXPIRING-WITHIN-30-DAYS Alarm

Procedure

This alarm is cleared when the validity time of the active certificate chain expires on or after 30 days.

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

LOCAL-SUDI-CERT-VERIFICATION-FAILED

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

Logical Object: EQPT

The Local SUDI Certificate Verification Failed alarm is raised when the active SUDI certificate verification fails.

Clear the LOCAL-SUDI-CERT-VERIFICATION-FAILED Alarm

Procedure

This alarm is cleared when the verification of an active SUDI certificate passes.

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

LOCAL-CERT-EXPIRED

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

Logical Object: EQPT

The Local Certificate Expired alarm is raised when the validity of an active certificate chain expires.

Clear the LOCAL-CERT-EXPIRED Alarm

Procedure

Procure and install a the local active certificate chain.

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

LOCAL-FAULT

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

Logical Objects: ETH

The LOCAL-FAULT alarm is raised on the GE_XP, GE_XPE, 10GE_XP, and 10GE_XPE card ports provisioned in 10 GE LAN PHY mode under the following conditions:

- when there is a loss of signal on the port.
- when a local fault character sequence is received in the incoming MAC stream as defined in IEEE 802.3ae, 10 GE fault signaling scheme.

The LOCAL-FAULT alarm is raised on the 40G-MXP-C, 40E-MXP-C, and 40ME-MXP-C card client ports provisioned with 10 GE or 10 GE FC payloads when a local fault character sequence is received in the incoming MAC stream as defined in IEEE 802.3ae, 10 Gigabit Ethernet fault signaling scheme.

The 40G-MXP-C, 40E-MXP-C, and 40ME-MXP-C cards pass the loss of signal and local fault errors transparently.

Clear the LOCAL-FAULT Alarm

Procedure

Verify and resolve the loss of signal on the port where the alarm is raised.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

LOCKOUT-REQ

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

Logical Objects: 2R, EQPT, ESCON, FC, GE, ISC, OTS, TRUNK

The Lockout Switch Request on Facility or Equipment condition occurs when a user initiates a lockout switch request for an OC-N port in a 1+1 facility protection group. This can be accomplished by locking traffic onto the working port with the LOCK ON command (thus locking it off the protect port), or locking it off the protect port with the LOCK OUT command. In either case, the protect port will show Lockout of Protection, and the Conditions window will show the LOCKOUT-REQ condition.

A lockout prevents protection switching. Clearing the lockout again allows protection switching and clears the LOCKOUT-REQ condition.

Clear the LOCKOUT-REQ Condition

Procedure

Complete the Clear a Lock-On or Lockout Command, on page 309 procedure.

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

LOCKOUT-REQ (2R, EQPT, ESCON, FC, GE, ISC)

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

Logical Objects: 2R, EQPT, ESCON, FC, GE, ISC

The Lockout Switch Request on Facility or Equipment condition occurs in a Y-cable MXP or TXP client protection group for the above-listed clients when a user initiates a lockout switch request. The condition is raised when you lock traffic onto the working port with the Lock On command (thus locking it off the protect port), or you lock it off the protect port with the Lock Out command. In either case, the protect port will show Lockout of Protection, and the Conditions window will show the LOCKOUT-REQ condition.

A lockout prevents protection switching. Clearing the lockout again allows protection switching and clears the LOCKOUT-REQ condition.

Clear the LOCKOUT-REQ (2R, EQPT, ESCON, FC, GE, ISC) Condition

Procedure

Complete the Clear a Lock-On or Lockout Command, on page 309 procedure.

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

LOCKOUT-REQ (TRUNK)

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

Logical Object: TRUNK

The Lockout Switch Request on Facility or Equipment condition occurs in an MXP or TXP trunk port splitter protection group when you lock traffic onto the working port with the Lock On command (thus locking it off the protect port), or lock it off the protect port with the Lock Out command. In either case, the protect port will show Lockout of Protection, and the Conditions window will show the LOCKOUT-REQ condition.

A lockout prevents protection switching. Clearing the lockout again allows protection switching and clears the LOCKOUT-REQ condition.

Clear the LOCKOUT-REQ (TRUNK) Condition

Procedure

Complete the Clear a Lock-On or Lockout Command, on page 309 procedure.

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

LOF (BITS)

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

Logical Object: BITS

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

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

Clear the LOF (BITS) Alarm

Procedure

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

a) In node or card view, note the slot and port reporting the alarm.
b) Find the coding and framing formats of the external BITS timing source. The formats should be in the user documentation for the external BITS timing source or on the timing source itself.
c) In node view (single-shelf mode) or shelf view (multishelf mode), click the **Provisioning** > **Timing** > **BITS Facilities** tabs.
d) Verify that the Coding setting matches the coding of the BITS timing source, either B8ZS or AMI.
e) If the coding does not match, click **Coding** and choose the appropriate coding from the drop-down list.
f) Verify that Framing matches the framing of the BITS timing source, either ESF or SF (D4).
g) If the framing does not match, click **Framing** and choose the appropriate framing from the drop-down list.

Note On the timing subtab, the B8ZS coding field is normally paired with ESF in the Framing field and the AMI coding field is normally paired with SF (D4) in the Framing field.

Step 2 If the alarm does not clear when the line framing and line coding match between the BITS input and the control card, complete the Physically Replace a Card, on page 313 procedure for the control card.

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

LOF (TRUNK)

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

Logical Object: TRUNK, OCN

The Loss of Frame for the DWDM trunk applies to the trunk optical or electrical signal that is carried to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, TXP_MR_10E_C, TXP_MR_10E_L, MXP_2.5G_10G, ADM-10G and OTU2_XP cards. It indicates that the receiving ONS system has lost frame delineation in the incoming data from trunk that serves the cards. LOF occurs when the SONET overhead loses a valid framing pattern for 3 milliseconds. Receiving two consecutive valid A1/A2 framing patterns clears the alarm.

Note In R7.01, when an LOF alarm occurs on TXP or MXP trunks, G709/SONET/SDH TCAs are suppressed. For details, see the Alarm and TCA Monitoring and Management chapter in the *Cisco ONS 15454 DWDM Reference Manual*.For details, see the Alarm and TCA Monitoring and Management document.

Clear the LOF (TRUNK) Alarm

Procedure

Step 1 Using site practices, verify fiber continuity to the port. Refer to the Network Reference chapter of the Configuration guide for a procedure to detect a fiber cut.

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

a) Confirm that the LED is correctly illuminated on the physical card. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

b) To determine whether the port is in service, in node view (single-shelf mode) or shelf view (multishelf mode), double-click the card in CTC to open the card view.

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

d) Verify that the Admin State column lists the port as IS (or Unlocked).

e) If the Admin State column lists the port as OOS,MT (or Locked,maintenance) or OOS,DSBLD (or Locked,disabled), click the column and choose IS (or Unlocked).

f) Click **Apply**.

Step 3 If the correct port is in service, clean the fiber according to site practice. If no site practice exists, complete the fiber cleaning procedure in the Maintain the Node chapter of the Configuration guide.

Step 4 If the alarm does not clear, verify that the power level of the optical signal is within the TXP or MXP card receiver specifications. (These specifications are listed in the Hardware Specifications appendix of the Configuration guideHardware Specifications document.)

Step 5 If the optical power level is within specifications, use an optical test set to verify that a valid signal exists on the line. For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving card as possible.

Step 6 If a valid signal exists, replace the connector on the backplane.

Step 7 Repeat Steps Step 1, on page 152 to Step 6, on page 152 for any other port on the card reporting the LOF.

Step 8 If the alarm does not clear, look for and troubleshoot any other alarm that could identify the source of the problem.

Step 9 If no other alarms exist that could be the source of the LOF, or if clearing an alarm did not clear the LOF, complete the Physically Replace a Card, on page 313 procedure for the reporting card.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

LOGBUFR90

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

Logical Object: SYSTEM

The Log Buffer Over 90 alarm indicates that the per-NE queue of incoming alarm, event, or update capacity of 5000 entries is over 90 percent full. LOGBUFR90 will clear if CTC recovers. If it does not clear, LOGBUFROVFL occurs.

Note LOGBUFR90 is an informational alarm and does not require troubleshooting.

LOGBUFROVFL

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

Logical Object: SYSTEM

The Log Buffer Overflow alarm indicates that the CTC per-NE queue of incoming alarm, event, or updates, which has a capacity of 5,000 entries, has overflowed. This happens only very rarely. However if it does, you must restart the CTC session. It is likely that some updates will have been missed if this alarm occurs.

Clear the LOGBUFROVFL Alarm

Procedure

Restart the CTC sessions.

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

LO-LASERBIAS

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

Logical Objects: EQPT, OCN/STMN, PPM

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

If the LO-LASERBIAS alarm threshold is set at 0 percent (the default), the laser's usability has ended. If the threshold is set at 5 percent to 10 percent, the card is still usable for several weeks or months before you need to replace it.

Clear the LO-LASERBIAS Alarm

Procedure

Complete the Physically Replace a Card, on page 313 procedure.

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

LO-LASERTEMP

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

Logical Objects: EQPT, OCN/STMN, PPM

The Equipment Low Laser Optical Transceiver Temperature alarm applies to the TXP and MXP cards. LO-LASERTEMP occurs when the internally measured transceiver temperature falls below the card setting by35.6 degrees F or 2 degrees C. A laser temperature change affects the transmitted wavelength. (This temperature is equivalent to about 200 picometers of wavelength.)

When the TXP or MXP card raises this alarm, the laser is automatically shut off. The An LOS for OCN/STMN is raised at the far-end node and the DUP-IPADDR , on page 64 alarm is raised at the near end. (Both of these alarms are described in the Alarm Troubleshooting chapter of the Troubleshooting guide. Maximum, minimum, and average laser temperatures are shown in the Current column entries in the Laser Temp rows.

Clear the LO-LASERTEMP Alarm

Procedure

Step 1 In node view (single-shelf mode) or shelf view (multishelf mode), complete the procedure for the reporting MXP or TXP card.

Step 2 If the alarm does not clear, complete the Physically Replace a Card, on page 313 procedure for the reporting MXP or TXP card.

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

LOM

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

Logical Object: TRUNK, EQPT

The Optical Transport Unit (OTU) Loss of Multiframe alarm is an OTN alarm for the trunk port and occurs when the Multi Frame Alignment Signal (MFAS) is corrupted. The alarm applies to MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, TXP_MR_10E, TXP_MR_10E_C, TXP_MR_10E_L, TXPP_MR_2.5G, ADM-10G, and OTU2_XP cards when the MFAS) overhead field is errored for more than five frames and persists for more than 3 milliseconds.

Clear the LOM Alarm

Procedure

Step 1 Ensure that the fiber connector for the card is completely plugged in. For more information about fiber connections and card insertion, refer to the Turn Up a Node chapter in the Configuration guide.

Step 2 If the bit error rate (BER) threshold is correct and at the expected level, use an optical test set to measure the power level of the line to ensure it is within guidelines. For specific procedures to use the test set equipment, consult the manufacturer.

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

Step 4 If receive levels are good, clean the fibers at both ends according to site practice. If no site practice exists, complete the fiber cleaning procedure in the Maintain the Node chapter in the Configuration guide.

Step 5 If the condition does not clear, verify that single-mode fiber is used.

Step 6 If the fiber is of the correct type, verify that a single-mode laser is used at the far-end node.

Step 7 Clean the fiber connectors at both ends for a signal degrade according to site practice.

Step 8 Verify that a single-mode laser is used at the far end.

Step 9 If the problem does not clear, the transmitter at the other end of the optical line could be failing and require replacement. Refer to the Physical Card Reseating, Resetting, and Replacement, on page 312 section.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

LOP-P

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

Logical Object: STSMON, STSTRM

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

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

For the FC_MR-4 card, an LOP-P is raised if a port is configured for a SONET signal but receives an SONET signal instead. (This information is contained in the H1 byte bits 5 and 6.)

Clear the LOP-P Alarm

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

Procedure

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

Step 2 Verify the circuit size listed in the Size column. If the size is different from what is expected, such as an STS3c instead of an STS1, this causes the alarm.

Step 3 If you have been monitoring the circuit with optical test equipment, a mismatch between the provisioned circuit size and the size expected by the test set can cause this alarm. For specific procedures to use the test set equipment, consult the manufacturer. Ensure that the test set monitoring is set up for the same size as the circuit provisioning.

Refer to the manufacturer instructions for test-set use.

Step 4 If the error is not due to an incorrectly configured test set, the error is in the provisioned CTC circuit size. Complete the Delete a Circuit, on page 314 procedure.

Step 5 Recreate the circuit for the correct size. For procedures, refer to the Create Circuits and VT Tunnels chapter in the Configuration guide.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

LO-RXPOWER

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

Logical Objects: 2R, ESCON, FC, GE, ISC, OCN/STMN, TRUNK

The Equipment Low Receive Power alarm is an indicator for TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, TXP_MR_10E_C, TXP_MR_10E_L, MXP_2.5G_10G, OC192-XFP, ADM-10G, and OTU2_XP card received optical signal power. LO-RXPOWER occurs when the measured optical power of the received signal falls below the threshold value, which is user-provisionable.

Clear the LO-RXPOWER Alarm

Procedure

Step 1 Check the PM of the TRUNK-RX port. Verify that received power is above the optics threshold:

a) In node view (single-shelf mode) or shelf view (multishelf mode), double-click the card to display the card view.

b) For the TRUNK-RX port, double-click the card and click the .

c) Compare the refreshed PM values with the threshold (ensuring that they are above the threshold value) by clicking the .

d) Ensure that a proper threshold has been provisioned for the receive value. (Refer to the Provision Transponder and Muxponder Cards chapter in the Configuration guide.) If an incorrect threshold has been set, adjust it to a value within the allowed limits. If instead the alarm condition does not clear, move to next step.

Step 2

Step 3 Determine whether a bulk attenuator is specified by the Cisco TransportPlanner design. If so, verify that the proper fixed attenuation value has been used.

Step 4

Step 5 Look for any alarm reported by the DWDM cards belonging to the OCHNC circuit whose destination is the faulty TXP/MXP and first troubleshoot that alarm. Possible alarm related include: amplifier Gain alarms (the GAIN-HDEG , on page 101 alarm, the GAIN-HFAIL , on page 102 alarm, the GAIN-LDEG , on page 102 alarm, or GAIN-LFAIL , on page 103 alarm); APC alarms (the APC-CORR-SKIPPED , on page 20 alarm or APC-OUT-OF-RANGE , on page 22 alarm), and LOS-P alarms on the Add or Drop ports belonging to the OCHNC circuit.

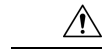
If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

LOS (2R)

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

Logical Object: 2R

The Loss of Signal for a 2R client applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, TXP_MR_10E_C, TXP_MR_10E_L, and MXP_2.5G_10G cards. The alarm is raised when the card port is not receiving input. An AIS is sent upstream.



Caution Always use the supplied electrostatic discharge wristband when working with a powered NCS system. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly. To verify cable continuity, follow site practices.

Clear the LOS (2R) Alarm

Procedure

Step 1 Ensure that the signal entering the Client-Rx port is provisioned with the correct physical-layer protocol.

Step 2 Ensure that the signal feeding the Client-Rx port is provisioned with the correct line speed.

Step 3 Check the PM of the Client-Rx port.

Step 4 Verify that received power is above the optics threshold.

Step 5 Ensure that a proper threshold has been provisioned. (Refer to the Provision Transponder and Muxponder Cards chapter in the Configuration guide. Refer to the SFP/XFP plug-in specifications located in the Installing the GBIC, SFP, SFP+, and XFP Optical Modules in Cisco ONS PlatformsInstalling the GBIC, SFP, SFP+, QSFP, XFP, CXP, CFP and CPAK Optical Modules in Cisco NCS Platforms document.) If an incorrect threshold has been set, adjust it to a value within the allowed limits.

Step 6 Verify the proper cabling and clean the fibers according with the site practice. Cabling procedures are located in the Turn Up a Node chapter of the Configuration guide, and a fiber-cleaning procedure is located in the Maintain the Node chapter of the same guide.

Step 7 Verify using an optical test set that a valid signal exists on the line and feeds the Client-Rx port. (For specific procedures to use the test set equipment, consult the manufacturer.) Test the line as close to the receiving card as possible. If the alarm condition does not clear, move to next step.

Step 8 Complete the Install an SFP, SFP+, or XFP Connector procedure or the Physically Replace a Card, on page 313 procedure as appropriate for your purposes.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

LOS (BITS)

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

Logical Object: BITS

Resource Type: OCn/STMn/Port

The LOS (BITS) alarm indicates that the control card has an LOS from the BITS timing source. LOS for BITS means the BITS clock or the connection to it failed.

Clear the LOS (BITS) Alarm

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

Procedure

Step 1 Verify the wiring connection from the BITS clock pin fields on the NCS system backplane to the timing source.

Step 2 If wiring is good, verify that the BITS clock is operating properly.

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

LOS (ESCON)

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

Logical Object: ESCON

The ESCON LOS alarm occurs on the TXP_MR_2.5G or TXPP_MR_2.5G card when there is a loss of signal for this payload, usually due to a physical error such as incorrect cabling connections, faulty cabling, or a break. It can also be caused by an incorrectly configured SFP.

Clear the LOS (ESCON) Alarm

Procedure

Step 1 Check for any upstream equipment failures that could cause the ESCON LOS alarm in this node.

Step 2 If there is no cause upstream, verify cabling continuity from the transmitting port to the receiving port reporting this LOS. To verify cable continuity, follow site practices.

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

Step 3 If the continuity is good, clean the fiber according to site practice. If none exists, complete the fiber-cleaning procedure in the Maintain the Node chapter in the Configuration guide.

Step 4 Ensure that the PPM (SFP) is correctly configured for this payload:

a) In node view (single-shelf mode) or shelf view (multishelf mode), double-click the card to open the card view.

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

c) Check the **Pluggable Port Modules** area for the PPM (SFP) associated with the port.

d) In the Pluggable Ports area, ensure that the rate for the errored PPM (SFP) is ESCON.

Note For information about provisioning PPMs (SFPs), refer to the Turn Up a Node chapter in the Configuration guide. PPM (SFP) specifications are listed in the the Installing the GBIC, SFP, SFP+, and XFP Optical Modules in Cisco ONS PlatformsInstalling the GBIC, SFP, SFP+, QSFP, XFP, CXP, CFP and CPAK Optical Modules in Cisco NCS Platforms document.

Step 5 If the physical cabling and PPM (SFP) are good but the alarm does not clear, verify that the correct port is actually in service:

a) Confirm that the LED is correctly lit on the physical TXP card.

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

b) To determine whether the port is in service, double-click the card in CTC to open the card view.
c) Click the **Provisioning** > **Line** tabs.
d) Verify that the Admin State column lists the port as IS, or (Unlocked).
e) If the Admin State column lists the port as OOS,MT (or Locked,maintenance) or OOS,DSBLD (or Locked,disabled), click the column and choose **IS** or **Unlocked**. Click **Apply**.

Step 6 If the correct port is in service but the alarm has not cleared, use an optical test set to confirm that a valid signal exists on the line. For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving card as possible.

Step 7 If the signal is valid, ensure that the transmit and receive outputs from the patch panel to your equipment are properly connected. For more information about fiber connections and terminations, refer to the Turn Up a Node chapter in the Configuration guide.

Step 8 If a valid signal exists but the alarm does not clear, replace the cable connector on the NCS system.

Step 9 Repeat Steps Step 2, on page 159 through Step 6, on page 160 for any other port on the card that reports the LOS (ESCON).

Step 10 If the alarm does not clear, the cabling could still be faulty despite correct attachments. Use the test set to locate the bad cable and replace it using the procedures in the Configuration guide.

Step 11 If the alarm does not clear, look for any card-level alarm that could cause this port alarm.

Step 12 If the alarm does not clear, complete the Physically Replace a Card, on page 313 procedure for the reporting card.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

LOS (ISC)

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

Logical Object: ISC

The LOS alarm for the ISC port applies to TXPP_MR_2.5G or TXP_MR_2.5G client PPMs (SFPs) provisioned at the ISC port rate. Troubleshooting is similar to the LOS (2R) alarm.

Clear the LOS (ISC) Alarm

Before you begin

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

Procedure

Complete the Clear the LOS (2R) Alarm, on page 158 procedure.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

LOS (OTS)

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

Logical Object: OTS

The Loss of Signal for the OTS applies to the OSC-3-RX port of the OPT-BST, OPT-AMP-C, or OPT-AMP-17-C amplifier card, LINE-2-RX port of the OSCM or OSC-CSM card, and LINE-RX port of the 40-SMR1-C or 40-SMR2-C card. It indicates that a fiber cut has occurred and no power is being received from the span. The alarm is raised when both LOS-P and LOS-O alarms occur, and demotes them.

Clear the LOS (OTS) Alarm

Procedure

Step 1 To troubleshoot this alarm, see the steps below.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

Step 2 Isolate the span affected by the fiber cut.

a) Go to CTC network view.
b) Identify the span connection that is gray.

Step 3 Verify the alarm is valid, then perform the following steps for both DWDM nodes connected to the span identified in Step 1.

a) Double-click the card directly connected to the span (either the OPT-BST or the OSC-CSM).
b) Click the **Alarms** tab and verify that a LOS condition is present on the LINE-RX port. If the alarm is correctly reported, move to Fix a Fiber Cut. If not, close the CTC application, delete the CTC cache and reopen the CTC connection.
c) Click the **Synchronize** button on the bottom left of the window.

Note If the "gray condition" of the span persists, log into Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

Step 4 If the network ALS setting on the DWDM nodes that you are troubleshooting is Auto Restart, continue with Fix a Fiber Cut; if the network ALS setting is DISABLE, go to Fix a Fiber Cut.

Step 5 Isolate the fiber affected by the fiber cut. For the two fibers belonging to the span, identify the fiber belonging to the west-to-east (W–E) line direction:

a) Go into the upstream node and identify the OSCM or OSC-CSM card managing the OSC termination referring to the faulty span.
b) Double-click the card, then click the **Maintenance Panel** tab.
c) Force the OSC-TX laser to be active by setting the ALS Mode to **DISABLE.**
d) Go into the downstream node and verify if OSC power is being received.
   - If a pair of OPT-BST + OSCM cards terminate the OSC connection, click the Provisioning > Optical Line > Parameters tabs, then verify that there is power for OSC-TX (Port 4).
   - If an OSC-CSM terminates the OSC connection, click the Provisioning > Optical Line > Parameters tabs, then verify that there is power for OSC-RX (Port 6).
e) If no power is detected and the LOS (OC-3) alarm persists, go to Fix a Fiber Cut; otherwise, the fiber under test is good. In this case, go to Step f to check the other fiber.
f) Repeat Steps a to d for the other fiber to verify that it is at fault.

Step 6 Repair the identified broken fiber to restore the internode link.

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

Note Before disconnecting any optical amplifier card fiber for troubleshooting, ensure that the optical amplifier card is unplugged.

LOS (TRUNK)

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

Logical Object: TRUNK

The Loss of Signal (LOS) for a TRUNK applies to GE-XP, 10GE-XP, TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, TXP_MR_10E_C, TXP_MR_10E_L, MXP_2.5G_10G, AR_MXP, AR_XP, AR_XPE, ADM-10G, and OTU2_XP cards.

Note The MXP_2.5G_10E card has no LOS (TRUNK) option, because G.709 cannot be disabled on the card.

The alarm is raised when the card port is not receiving input. An AIS is sent upstream.

The purpose of the LOS (TRUNK) alarm is to alert the user that no optical power is being received from the fiber. A typical fault condition signalled by the LOS (TRUNK) alarm is a fiber cut. In this case, neither the payload nor the overhead signals are being received.

Note With G.709 off, the alarm coming from the trunk is LOS (TRUNK) in accordance with SONET standards.

Note In R7.01, when an LOS (TRUNK) alarm occurs on TXP and MXP trunks, G709/SONET/SDH TCAs are suppressed.

Clear the LOS (TRUNK) Alarm

Check the PMs of the TRUNK-RX port and verify that the received power is above the optics threshold.

Procedure

Step 1 Check that a proper threshold has been provisioned. (For procedures, refer to the Provision Transponder and Muxponder Cards chapter in the Configuration guide.) If an incorrect threshold has been set, adjust it to a value within the allowed limits. If the alarm condition does not clear, move to next step.

Step 2

Step 3 Using an optical test set, verify that a valid signal exists on the line and feeds the TRUNK-RX port.(For specific procedures to use the test set equipment, consult the manufacturer.) Test the line as close to the receiving card as possible. If the alarm condition does not clear, move to next step.

Step 4 Verify whether a bulk attenuator is specified in the Cisco TransportPlanner design. If so, verify that the proper fixed attenuation value has been used.

Step 5 If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

Step 6 Look for and troubleshoot any alarms reported by the DWDM cards belonging to the OCHNC circuit whose destination is the faulty TXP/MXP. Possible alarms include: amplifier gain alarms (the GAIN-HDEG , on page 101 alarm, the GAIN-HFAIL , on page 102 alarm, the GAIN-LDEG , on page 102 alarm or GAIN-LFAIL , on page 103 alarm); APC alarms (the APC-CORR-SKIPPED , on page 20 alarm and APC-OUT-OF-RANGE , on page 22 alarm), OR LOS-P alarms on the Add or Drop ports belonging to the OCHNC circuit.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into

http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

LOS-O

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

Logical Objects: OCH, OMS, OTS

The Incoming Overhead Loss of Signal alarm applies to the OSC-TX port of OPT-AMP-C card. It is raised when the monitored input power crosses the FAIL-LOW threshold associated to the OSC Power received. The is alarm is demoted if another LOS alarm is also present.

Clear the LOS-O Alarm

Procedure

Step 1 Verify fiber continuity to the port by following site practices. Refer to the Network Reference chapter of the Configuration guide for a procedure to detect a fiber cut.

Step 2 If the cabling is good, confirm that the LED is correctly illuminated on the physical card. A green ACT/SBY LED indicates an active card. A red ACT/SBY LED indicates a failed card.

Step 3 Display the optical thresholds by clicking one of the following tabs:

- For the OPT-AMP-C card, .

Step 4 Verify that OSC Fail Low thresholds are correct . To identify the MP value:

a) In node view (single-shelf mode) or shelf view (multishelf mode), .

b) Identify the following parameter: east or west side Rx channel OSC LOS threshold.

Step 5 If the port power is below the threshold, verify that OSC connections have been created on the other side of the span. If the connections are not present, refer to the Configuration guide for procedures.

Step 6 If OSC connections are present, check the OSC transmitted power using CTC on the far-end node. Refer to the Turn Up Node chapter of the Configuration guide for the proper procedure.

Step 7 If the transmitted OSC value is out of range, troubleshoot that problem first.

Step 8 If the OSC value is within range, come back to the port reporting the LOS-O alarm and clean the fiber according to site practice. If no site practice exists, complete the fiber-cleaning procedure in the Maintain the Node chapter of the Configuration guide.

Step 9 If the alarm does not clear, look for and troubleshoot any other alarm that could identify the source of the problem.

Step 10 If no other alarms exist that could be the source of the LOS-O, place all of the card ports in **OOS,DSBLD** (or **Locked,disabled**) administrative state.

Step 11 Complete the Physically Replace a Card, on page 313 procedure for the reporting card.

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

LOS-P (AOTS, OMS, OTS)

Clear the LOS-P (AOTS, OMS, OTS) Alarm

Procedure

Step 1 Verify that the card has the correct physical behavior by checking the LED on the physical card. A green ACT/SBY LED indicates an active card, and a red ACT/SBY LED indicates a failed card. If the LED is red, complete the Physically Replace a Card, on page 313 procedure and call Cisco TAC (1 800 553-2447).

Note When you replace a card with an identical type of card, you do not need to make any changes to the database other than restoring the card port to the IS,AINS administrative state.

Step 2 Verify that there truly is a loss of input signal by completing the following steps:

a) In node view (single-shelf mode) or shelf view (multishelf mode), double-click the card to open the card view.

b) Verify the proper input power values by clicking one of the following tabs as appropriate:

c) Display the proper Power Failure Low threshold by clicking one of the following tabs as appropriate:

Tip To view the alarm thresholds (as opposed to the warning thresholds), check the **Alarm** check box on the bottom-left of the Optics Thresholds tab and click **Reset**.

d) Compare the actual Power value with the Alarm Threshold value and complete one of the following actions:

- If the Power value is less than the Fail Low threshold, go to Step 3, on page 165.
- If the Power value is greater than the Fail Low threshold plus the alarm hysteresis (allowance value) default of 1 dBm, complete the Reset a Card in CTC, on page 310 procedure for the card.

If the alarm does not clear, complete the Physically Replace a Card, on page 313 procedure and and call Cisco TAC (1 800 553-2447).

Note When you replace a card with an identical type of card, you do not need to make any changes to the database other than restoring the card port to the IS,AINS administrative state.

Step 3 Verify the fiber continuity to the port by following site practices. Refer to the Network Reference chapter of the Configuration guide for a procedure to detect a fiber cut.

Step 4 Check the Internal Connections file generated by Cisco Transport Planner for the node where the errored card is located. If necessary, recable the node cabling in accordance with the MP file connections list. To cable a DWDM node, refer to the Turn Up a Node chapter in the Configuration guide.

Step 5 If the cabling is good, use an optical test set to measure the power value on the output port connected to the alarmed card. For specific procedures to use the test set equipment, consult the manufacturer. If the power difference reported is greater than 1 dBm (standard fiber jumper insertion loss is 0.3 dBm), clean the fiber according to site practice. If no site practice exists, complete the fiber-cleaning procedure in the Maintain the Node chapter of the Configuration guide.

Note Unplugging the fiber can cause a traffic hit. To avoid this, perform a traffic switch if possible. Refer to the Configuration guide for detailed information.

Step 6 If the port on which the alarm is raised is connected to a remote CRS-1 or ASR 9000 series router, verify that the wavelength configured on the router interface is the same as that configured for the port. Check the router configuration by using these steps:

a) Enter the following command on the router to validate the remote node configuration.

```
Router> show controllers dwdm interface id x/x/x/x
```

b) Check the information displayed under Optics Status to verify the configured wavelength.

c) If the wavelength is different from that configured for the port, reset it by entering the following command on the router in global configuration mode.

```
Router (config)# controller dwdm interface id x/x/x/x wavelength channel number
```

Note The wavelength configured for the port can be checked in CTC card view.

Step 7 If the alarm does not clear, follow the general troubleshooting rules in the Network Reference chapter in the Configuration guide for identifying any other upstream alarm in the logical signal flow that could be the root cause of the outstanding alarm.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

LOS-P (OCH)

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

Logical Object: OCH

For the 32WSS-O and 40WSS-C, the LOS-P alarm can be associated with Add ports as well as pass-through internal ports. If the LOS-P (OCH) alarm is raised against this kind of port a different troubleshooting procedure is needed because the port does not have an optical power source directly connected to it. In this case, follow the general troubleshooting rules for network-level (inter-node) troubleshooting in the chapter, General Troubleshooting to identify upstream alarms in the logical signal flow that could cause an LOS-P.

LOS-P (OCH) indicates a loss of received signal, which means the monitored input power value has crossed the Power Failure Low threshold associated with the port in accordance with the specific VOA power reference setpoint provisioned on VOA along the path.

Clear the LOS-P (OCH) Alarm

Procedure

Step 1 Verify that the card is exhibiting correct behavior by checking the LED behavior on the physical card. A green ACT/SBY LED indicates an active card, and a red ACT/SBY LED indicates a failed card. If the LED is red, complete the Physically Replace a Card, on page 313 procedure and continue with Step 9, on page 169.

Note When you replace a card with an identical type of card, you do not need to make any changes to the database other than restoring the card's port to the IS,AINS administrative state.

Step 2 Verify that there truly is a loss of received signal by completing the following steps:

a) In node view (single-shelf mode) or shelf view (multishelf mode), double-click the card to open the card view.

b) View the proper input power values by clicking one of the following tabs as appropriate:

- For the ADM-10G card, click **Performance** > **Optics PM** > **Current Values** tabs.
- For the 32WSS-O and 40WSS-C cards, click the **Provisioning** > **Optical Chn: Optical Connector** x > **Parameters** tabs.
- For the 40-SMR1-C and 40-SMR2-C cards, click the **Provisioning** > **Optical Line** > **Parameters** tabs.

c) Display the proper Power Failure Low threshold by clicking one of the following tabs as appropriate:

- For the ADM-10G card, click **Provisioning** > **Optics Thresholds** tabs.
- For the 32WSS-O and 40WSS-C cards, click the **Provisioning** > **Optical Chn: Optical Connector** x > **Optics Thresholds** tabs.
- For the 40-SMR1-C and 40-SMR2-C cards, click the **Provisioning** > **Optical Line** > **Optics Thresholds** tabs.

Tip To view the alarm thresholds (as opposed to the warning thresholds), check the **Alarm** check box on the bottom-left of the Optics Thresholds tab and click **Reset**.

d) Compare the actual assigned Power value with the Alarm Threshold value and complete one of the following actions:

- If the Power value is less than the Fail Low threshold, go to Step 3, on page 168.
- If the Power value is greater than the Fail Low threshold plus the alarm hysteresis (or allowance value) default of 1 dBm, complete the Reset a Card in CTC, on page 310 procedure for the card.

If the alarm does not clear, complete the Physically Replace a Card, on page 313 procedure and continue to Step 9, on page 169.

Note When you replace a card with an identical type of card, you do not need to make any changes to the database other than restoring the card's port to the IS,AINS administrative state.

Step 3 Verify the fiber continuity to the port using site practices. Refer to the Network Reference chapter of the Configuration guide for a procedure to detect a fiber cut.

Step 4 Check the Internal Connections file generated by Cisco TransportPlanner for the node where the card is located. If necessary, recable the node in accordance with the MP file connections list. For procedures to cable a DWDM node, refer to the Turn Up a Node chapter of the Configuration guide.

Note If no LOS-P (OTS) alarm is present on the COM port of the 80-WXC-C card that is configured in the DMX mode and a LOS-P (OCH) alarm is raised on the wavelengths passing through the COM port, it can indicate incorrect cabling of the COM and MON ports. In this case, swap the fiber between the COM and MON ports to clear the alarm

Step 5 If the cabling is good, verify that each involved optical signal source, including TXP, MXP or ITU-T line card trunk transmit ports, is in the IS (or Unlocked) administrative state. To do this, click the following tabs as appropriate:

- For the ADM-10G card, click the **Provisioning** > **Line** > **Ports** tabs.
- For the TXP_MR_10G card, click the **Provisioning** > **Line** > **SONET** (or **Provisioning** > **Line** > **SDH**) tabs.
- For the TXP_MR_10E card, click the **Provisioning** > **Line** > **SONET** (or **Provisioning** > **Line** > **SDH**) tabs.
- For the TXP_MR_2.5G card, click the **Provisioning** > **Line** > **SONET** (or **Provisioning** > **Line** > **SDH**) tabs.
- For the TXPP_MR_2.5G card, click the **Provisioning** > **Line** > **SONET** (or **Provisioning** > **Line** > **SDH**) tabs.
- For the MXP_MR_2.5G card, click the **Provisioning** > **Line** > **SONET** (or **Provisioning** > **Line** > **SDH**) tabs.
- For the MXPP_MR_2.5G card, click the **Provisioning** > **Line** > **SONET** (or **Provisioning** > **Line** > **SDH**) tabs.
- For the MXP_2.5G_10E card, click the **Provisioning** > **Line** > **Trunk** tabs.
- For the MXP_2.5G_10G card, click the **Provisioning** > **Line** > **SONET** (or **Provisioning** > **Line** > **SDH**) tabs.

If the port administrative state is not IS (or Unlocked), choose **IS** (or **Unlocked**), from the Admin state drop-down list. If the alarm does not clear, continue with Step 9, on page 169.

Note If the LOS-P (OCH) alarm applies to a 32WSS-O passthrough port, it means that a single optical source is not directly connected to the port. In this case, follow the general troubleshooting rules given in Network Level (Internode) Troubleshooting to identify any other alarm upstream to the logical signal flow that could be the root cause for the outstanding alarm.

Step 6 If the signal source is in IS (or Unlocked) administrative state, use an optical test set to verify that the transmit laser is active. For specific procedures to use the test set equipment, consult the manufacturer.

Step 7 If the laser is active, compare the card's provisioned transmit optical power value with the expected range in the Provision Transponder and Muxponder Cards chapter of the Configuration guide. To display the provisioned transmit optical power values, click the following tabs as appropriate:

- For the ADM-10G card, click **Performance** > **Optics PM** > **Current Values** tabs.

- For the TXP_MR_10G card, click the **Performance** > **Optics PM** > **Current Values** > **Trunk Port** tabs.
- For the TXP_MR_10E card, click the **Performance** > **Optics PM** > **Current Values** > **Trunk Port** tabs.
- For the MXP_2.5G_10E card, click the **Performance** > **Optics PM** > **Current Values** > **Trunk Port** tabs.
- For the MXP_2.5G_10G card, click the **Performance** > **Optics PM** > **Current Values** > **Trunk Port** tabs.

Step 8 Use a standard power meter to measure actual transmit optical power for the following cards as applicable:

- GE-XP
- 10GE-XP
- ADM-10G
- TXP_MR_2.5G
- TXPP_MR_2.5G
- MXP_MR_2.5G
- MXPP_MR_2.5G
- Every ITU-T line card

If the tested optical transmit optical power is within the expected range, go to Step 9, on page 169. If the actual power value is outside the specification range, complete the Physically Replace a Card, on page 313. When the newly installed card becomes active, verify that the LOS-P (OCH) alarm clears. If it does not, continue with Step 9, on page 169.

Tip If a spare card is unavailable and the transmit power still functions, you can temporarily clear the LOS-P alarm by following the general procedure to add path VOAs during startup failure as noted in the Perform Node Acceptance Tests chapter of the Configuration guide. For more information about provisioning VOA setpoints, refer to the Network Reference chapter of the Configuration guide.

Step 9 If the power is within the expected range, return to the port that reported LOS-P and clean the alarmed port's fiber according to site practice. If no site practice exists, complete the procedure in the Maintain the Node chapter of the Configuration guide.

Note Unplugging the fiber can cause a traffic hit. To avoid this, perform a traffic switch if possible.

Step 10 If the alarm does not clear, add path VOAs during startup failure as noted in the Perform Node Acceptance Tests chapter of the Configuration guide to remedy the problem.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

LOS-P (TRUNK)

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

Logical Object: TRUNK

The Loss of Signal Payload (LOS-P) alarm for the trunk layer indicates that the incoming payload signal is absent at the input trunk port. There still may be optical power on the fiber, but the payload data is missing. This alarm applies to the following cards: TXP_MR_10G, TXP_MR_10E, MXP_2.5G_10G, TXP_MR_2.5G, TXPP_MR_2.5G, MXP_MR_2.5G, MXPP_MR_2.5G, GE-XP, 10GE-XP, ADM-10G, OTU2_XP, 40G-MXP-C, 40E-MXP-C, 40ME-MXP-C, 40E-TXP-C, 40-ME-TXP-C, and every ITU-T line card.

Note The MXP_2.5G_10E has no LOS-P (TRUNK) option, because ITU-T G.709 encapsulation on the card cannot be disabled.

Note With ITU-T G.709 encapsulation on, the alarm coming from the trunk is LOS-P (TRUNK) in accordance with the OTN standards.

Note When the near-end and far-end trunk ports of the 1.2T-XP-LC card are set at different frequencies, traffic is affected. The LOS-P alarm is raised on the trunk ports instead of the Wavelength Mismatch (WAV_UNLOCK) condition. This is hardware limitation as the WAV_UNLOCK condition is related to hardware laser failure.

Note In R7.01, when an LOS-P (TRUNK) alarm occurs on TXP and MXP trunks, G709/SONET/SDH TCAs are suppressed. For details, see the Alarm and TCA Monitoring and Management chapter in the *Cisco ONS 15454 DWDM Reference Manual*.For details, see the Alarm and TCA Monitoring and Management document.

Clear the LOS-P (TRUNK) Alarm

Procedure

Step 1 Verify that the card behaves correctly by checking the LED behavior on the physical card. A green ACT/SBY LED indicates an active card, and a red ACT/SBY LED indicates a failed card. If the LED is red, complete the Physically Replace a Card, on page 313 procedure and continue to Step 7, on page 171.

Note When you replace a card with an identical type of card, you do not need to make any changes to the database other than restoring the card's port to the IS,AINS administrative state.

Step 2 Verify that there truly is a loss of received optical power by completing the following steps:

a) In node view (single-shelf mode) or shelf view (multishelf mode), double-click the alarmed card to open the card view.
b) Click the **Performance** > **Optics PM** > **Current Values** > **Trunk Port** tabs and view the RX Optical Pwr value.
c) Compare the actual power levels with the expected power range given in the Configuration guide. Complete one of the following actions:
   - If power is higher than –40 dBm (that is, –20 dBm, –1 dBm, 0 dBm or 10 dBm) and within the accepted range go to Step 4, on page 171.
   - or if the power is lower than –40 dBm (that is, –40 dBm, –45 dBm or –50 dBm) complete the Reset a Card in CTC, on page 310 procedure for the card.

Step 3 If the alarm does not clear, complete the Physically Replace a Card, on page 313 procedure for the reporting card and then call Cisco TAC (1 800 553-2447) .

Note When you replace a card with an identical type of card, you do not need to make any changes to the database other than restoring the card's port to the IS,AINS administrative state.

Step 4 Verify the fiber continuity to the port by following site practices. Refer to the Network Reference chapter of the Configuration guide for a procedure to detect a fiber cut.

Step 5 Check the Internal Connections file generated by Cisco TransportPlanner for the node containing the alarmed card. If necessary, recable the node in accordance with the MP file connections list. For procedures to cable a DWDM node, refer to the Turn Up a Node chapter of the Configuration guide.

Step 6

Step 7 If the power difference reported is greater than 1 dBm (standard fiber jumper insertion loss is 0.3 dBm), clean the fiber according to site practice. If no site practice exists, complete the procedure in the Maintain the Node chapter of the Configuration guide.

Note Unplugging the fiber can cause a traffic hit. To avoid this, perform a traffic switch if possible.

Step 8 If the alarm does not clear, follow the general troubleshooting rules stated in the Network Reference chapter of the Configuration guide to identify upstream alarms in the logical signal flow that could cause an LOS-P.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

LOS-RAMAN (OTS)

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

SONET Logical Objects: OTS

The Loss of Raman signal alarm indicates that the Raman signal has not received by the RX RAMAN port on the OPT-RAMP-C, OPT-RAMP-CE, EDRA-1-xx, EDRA-2-xx, and RAMAN-CTP card.

Clear the LOS-RAMAN Condition

Procedure

Step 1 Verify no RLS alarm is raised by the card. If there is an RLS alarm, seeClear the RLS Condition for more details.

Step 2 Verify that the fiber cable is properly connected and attached to the correct port. For more information about fiber connections and terminations, refer to the Install Cards and Fiber-Optic Cables chapter in the Configuration guide.

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

Step 3 Verify the card facing to this card in the far end site. If the facing card has an RLS alarm, the problem is on that card, see Clear the RLS Condition for more details.

Step 4 If no other alarms are present that could be the source of the LOS-RAMAN condition, or if clearing an alarm did not clear the LOS-RAMAN condition, complete the Physically Replace a Card, on page 313 procedure for the reporting card.

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

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

LO-TXPOWER

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

Logical Objects: 2R, EQPT, ESCON, FC, GE, ISC, OCN/STMN, PPM, TRUNK

The Equipment Low Transmit Power alarm is an indicator for the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, TXP_MR_10E_C, TXP_MR_10E_L, MXP_2.5G_10G, OC192-XFP, ADM-10G, and OTU2_XP card transmitted optical signal power. LO-TXPOWER occurs when the measured optical power of the transmitted signal falls under the threshold. The threshold value is user-provisionable.

The LO-TX-POWER alarm is raised and the traffic is dropped when TX and RX connectors of the ONS-XC-10G-C or ONS-XC-10G-96C XFP connected to the trunk port of an ADM-10G, OTU2_XP, GE_XP, GE_XPE, 10GE_XP, or 10GE_XPE card are swapped.

Clear the LO-TXPOWER Alarm

Procedure

Step 1 To clear the LO-TXPOWER alarm on the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, TXP_MR_10E_C, TXP_MR_10E_L, MXP_2.5G_10G, OC192-XFP, ADM-10G, or OTU2_XP card, perform the following:

a) In node view (single-shelf mode) or single-shelf view (multishelf mode), display the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, TXP_MR_10E_C, TXP_MR_10E_L, MXP_2.5G_10G, OC192-XFP, ADM-10G, or OTU2_XP card view.

b) Click the .

c) For the ADM-10G card, click the .

d) Increase the TX Power Low column value by 0.5 dBm.

e) If the card transmit power setting cannot be increased without affecting the signal, complete the Physically Replace a Card, on page 313 procedure.

Step 2 To clear the LO-TXPOWER alarm raised due to swapping of TX and RX connectors of the ONS-XC-10G-C or ONS-XC-10G-96C XFP connected to the trunk port of an ADM-10G, OTU2_XP, GE_XP, GE_XPE, 10GE_XP, or 10GE_XPE card , perform the following:

a) Reconnect the TX and RX connectors of the ONS-XC-10G-C or ONS-XC-10G-96C XFP correctly.

b) Set the trunk port to OOS,DSBLD (ANSI) or Locked,disabled (ETSI) state and then back into the IS (ANSI) or Unlocked (ETSI) state.

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

LPBKCRS

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

Logical Objects: STSMON, STSTRM

The Loopback Cross-Connect condition indicates that there is a software cross-connect loopback active between an optical card and an OC-192 card. A cross-connect loopback test occurs below line speed and does not affect traffic.

Note Cross-connect loopbacks occur below line speed. They do not affect traffic.

Clear the LPBKCRS Condition

Procedure

Step 1 To remove the loopback cross-connect condition, double-click the optical card in CTC to display the card view.

Step 2 Complete the Clear an STM-N Card XC Loopback Circuit, on page 316 procedure.

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

LPBKFACILITY (ESCON)

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

Logical Object: ESCON

The LPBKFACILITY (ESCON) condition occurs on a TXP_MR_2.5G or TXPP_MR_2.5G card PPM (SFP) provisioned for FICON1G or FICON 2G line speed when there is a facility loopback active on the card.

For information about troubleshooting these circuits with loopbacks, refer to the Troubleshooting MXP, TXP, XP, or ADM-10G Circuit Paths With Loopbacks section.

Clear the LPBKFACILITY (ESCON) Condition

Procedure

Complete the Clear an MXP, TXP, GE-XP, 10GE-XP, and ADM-10G Card Loopback Circuit, on page 315 procedure.

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

LPBKFACILITY (FC)

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

Logical Object: FC

A Loopback Facility condition for the FC payload occurs on a fibre channel (FC) line when a software facility (line) loopback is active for an MXPP_MR_2.5G, MXP_MR_2.5G, TXPP_MR_2.5G, and TXP_MR_2.5G card client PPM (SFP) provisioned at the FC1G, FC2G, FICON1G, or FICON 2G line speed.

For information about troubleshooting these circuits with loopbacks, refer to the Troubleshooting MXP, TXP, XP, or ADM-10G Circuit Paths With Loopbacks.

Note For general information about MXP and TXP cards, refer to the Card Reference chapter in the *Cisco ONS 15454 DWDM Reference Manual*. For information about provisioning them, refer to the Provision Transponder and Muxponder Cards chapter in the *Cisco ONS 15454 DWDM Procedure Guide*.

Note For general information about MXP and TXP cards and provisioning them, refer to the Provision Transponder and Muxponder Cards chapter in the *Cisco ONS 15454 DWDM Configuration GuideCisco NCS 2000 Series Configuration Guide*.

Clear the LPBKFACILITY (FC) Condition

Procedure

Complete the Clear an MXP, TXP, GE-XP, 10GE-XP, and ADM-10G Card Loopback Circuit, on page 315 procedure.

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

LPBKFACILITY (GE)

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

Logical Object: GE

A Loopback Facility condition for a Gigabit Ethernet (GE) port occurs when a software facility (line) loopback is active for an MXP_MR_2.5G, MXPP_MR_2.5G, TXP_MR_2.5G, TXPP_MR_2.5G, GE-XP, 10GE-XP, and ADM-10G card client PPM (SFP) provisioned at the ONE_GE port rate. For the TXP_MR_10E and TXP_MR_10G cards, this condition occurs when there is a facility loopback on a client PPM (SFP) provisioned at the TEN_GE port rate.

For information about troubleshooting these circuits with loopbacks, refer to the Troubleshooting MXP, TXP, XP, or ADM-10G Circuit Paths With Loopbacks section.

Clear the LPBKFACILITY (GE) Condition

Procedure

Complete the Clear an MXP, TXP, GE-XP, 10GE-XP, and ADM-10G Card Loopback Circuit, on page 315 procedure.

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

LPBKFACILITY (ISC)

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

Logical Object: ISC

A Loopback Facility condition for an ISC port occurs when a software facility (line) loopback is active for a TXPP_MR_2.5G or TXP_MR_2.5G client PPM (SFP) provisioned at the ISC port rate.

For information about troubleshooting these circuits with loopbacks, refer to the Troubleshooting MXP, TXP, XP, or ADM-10G Circuit Paths With Loopbacks section.

Clear the LPBKFACILITY (ISC) Condition

Procedure

Complete the Clear an MXP, TXP, GE-XP, 10GE-XP, and ADM-10G Card Loopback Circuit, on page 315 procedure.

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

LPBKFACILITY (TRUNK)

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

Logical Object: TRUNK

A Loopback Facility condition on MXP, TXP, GE-XP, 10GE-XP, and ADM-10G card trunk ports indicates that there is an active facility (line) loopback on the port. For this condition to be present, the administrative state is OOS,MT (or Locked,maintenance).

For information about troubleshooting these circuits with loopbacks, refer to the Troubleshooting MXP, TXP, XP, or ADM-10G Circuit Paths With Loopbacks section.

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

Clear the LPBKFACILITY (TRUNK) Condition

Procedure

Complete the Clear an MXP, TXP, GE-XP, 10GE-XP, and ADM-10G Card Loopback Circuit, on page 315 procedure.

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

LPBKTERMINAL (ESCON)

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

Logical Object: ESCON

The LPBKTERMINAL (ESCON) condition occurs on a TXP_MR_2.5G or TXPP_MR_2.5G card PPM (SFP) provisioned for FICON1G or FICON 2G line speed when there is a terminal loopback active on the card.

For information about troubleshooting these circuits with loopbacks, refer to the Troubleshooting MXP, TXP, XP, or ADM-10G Circuit Paths With Loopbacks section.

Clear the LPBKTERMINAL (ESCON) Condition

Procedure

Complete the Clear an MXP, TXP, GE-XP, 10GE-XP, and ADM-10G Card Loopback Circuit, on page 315 procedure.

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

LPBKTERMINAL (FC)

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

Logical Object: FC

A Loopback Terminal condition for the FC payload occurs on an FC when a software terminal (inward) loopback is active for an MXP_MR_2.5G, MXPP_MR_2.5G, TXP_MR_2.5G, TXPP_MR_2.5G, GE-XP, and 10GE-XP card client PPM (SFP) provisioned at the FC1G, FC2G, FICON1G, or FICON2G line speed.

For information about troubleshooting these circuits with loopbacks, refer to the Troubleshooting MXP, TXP, XP, or ADM-10G Circuit Paths With Loopbacks section.

Clear the LPBKTERMINAL (FC) Condition

Procedure

Complete the Clear an MXP, TXP, GE-XP, 10GE-XP, and ADM-10G Card Loopback Circuit, on page 315 procedure.

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

LPBKTERMINAL (GE)

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

Logical Object: GE

A Loopback Terminal condition for a GE port occurs when a software terminal (inward) loopback is active for an MXP_MR_2.5G, MXPP_MR_2.5G, TXP_MR_2.5G, and TXPP_MR_2.5G card client PPM (SFP) provisioned at the ONE_GE port rate. For the TXP_MR_10E and TXP_MR_10G cards, this condition occurs when there is a facility loopback on a client PPM (SFP) provisioned at the TEN_GE port rate.

For information about troubleshooting these circuits with loopbacks, refer to the Troubleshooting MXP, TXP, XP, or ADM-10G Circuit Paths With Loopbacks section.

Clear the LPBKTERMINAL (GE) Condition

Procedure

Complete the Clear an MXP, TXP, GE-XP, 10GE-XP, and ADM-10G Card Loopback Circuit, on page 315 procedure.

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

LPBKTERMINAL (ISC)

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

Logical Object: ISC

A Loopback Terminal condition for an ISC port occurs when a software terminal (inward) loopback is active for a TXPP_MR_2.5G or TXP_MR_2.5G client PPM (SFP) provisioned at the ISC port rate.

For information about troubleshooting these circuits with loopbacks, refer to the Troubleshooting MXP, TXP, XP, or ADM-10G Circuit Paths With Loopbacks section.

Clear the LPBKTERMINAL (ISC) Condition

Procedure

Complete the Clear an MXP, TXP, GE-XP, 10GE-XP, and ADM-10G Card Loopback Circuit, on page 315 procedure.

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

LPBKTERMINAL (TRUNK)

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

Logical Object: TRUNK

A Loopback Terminal condition on MXP or TXP trunk card indicates that there is an active terminal (inward) loopback on the port.

For information about troubleshooting, refer to the Troubleshooting MXP, TXP, XP, or ADM-10G Circuit Paths With Loopbacks section.

Clear the LPBKTERMINAL (TRUNK) Condition

Procedure

Complete the Clear an MXP, TXP, GE-XP, 10GE-XP, and ADM-10G Card Loopback Circuit, on page 315 procedure.

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

LSC-NOT-PRESENT-MIC-IN-USE

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

Logical Object: EQPT

The LSC Not Present Mic In Use alarm is raised when the LSC is not present, and use LSC option is checked.

Clear the LSC-NOT-PRESENT-MIC-IN-USE Alarm

Procedure

Install LSC if use MIC or use LSC option is checked in CTC.

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

LWBATVG

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

Logical Object: PWR

The Low Voltage Battery alarm occurs in a 48 VDC environment when a battery lead input voltage falls below the low power threshold. This threshold, with a default value of 44 VDC, is user-provisionable. The alarm remains raised until the voltage remains above the threshold for 120 seconds. (For information about changing this threshold, refer to the Turn Up Node chapter in the Configuration guide.

Clear the LWBATVG Alarm

Procedure

The problem is external to the NCS system. Troubleshoot the power source supplying the battery leads.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

MAN-LASER-RESTART

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

Logical Objects: OTS, AOTS

The Manual Laser Restart condition is raised when a ALS mode is set to Manual Restart or Manual Restart for test.

Clear the MAN-LASER-RESTART Condition

Procedure

Set the ALS Mode to a value different from Manual Restart or Manual Restart for test.

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

MAN-REQ

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

Logical Object: EQPT

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

Clear the MAN-REQ Condition

Procedure

Complete the Initiate a 1+1 Manual Switch Command, on page 307 procedure.

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

MANRESET

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

Logical Object: EQPT

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

MANSWTOINT

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

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)

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)

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.

MANSWTOTHIRD

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

Logical Objects: EXT-SREF, NE-SREF

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

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

MANUAL-REQ-SPAN (2R, ESCON, FC, GE, ISC, OCN/STMN, OTS)

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

Logical Objects: 2R, ESCON, FC, GE, ISC, OCN/STMN, OTS

The Manual Switch Request on Ring condition for clients occurs when a user initiates a Manual Span command on an MXP or TXP client for the above-listed client types to move 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.

MANUAL-REQ-SPAN (TRUNK)

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

Logical Object: TRUNK

The Manual Switch Request on Ring condition for the trunk occurs when a user initiates a Manual Span command on an MXP or TXP trunk port in a splitter protection group to move 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.

MEA (AIP)

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

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.

Clear the MEA (AIP) Alarm

Procedure

Complete the Replace the Alarm Interface Panel, on page 319 procedure.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

MEA (EQPT)

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

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. Removing the incompatible cards clears the alarm. For more information about card compatibility, refer to the Configuration guide.

Clear the MEA (EQPT) Alarm

Procedure

Step 1 Physically verify the type of card that is installed in the slot reporting the MEA alarm. In node view (single-shelf mode) or shelf view (multishelf mode), click the **Inventory** tab and compare it to the actual installed card.

Step 2 Determine whether the NCS system 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 here, then you are using an earlier shelf assembly.

Note On the 15454-SA-HD (P/N: 800-24848), 15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1 (P/N: 800-07149) shelves, the AIP cover is clear plastic. On the 15454-SA-ANSI shelf (P/N: 800-19857), the AIP cover is metal.

Step 3 If you prefer the card type depicted by CTC, complete the Physically Replace a Card, on page 313 procedure for the reporting card.

Step 4 If you prefer the card that physically occupies the slot but the card is not in service, does not have circuits mapped to it, and is not part of a protection group, place the cursor over the provisioned card in CTC and right-click to choose **Delete Card**.

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

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

Step 5 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.

a) In node view (single-shelf mode) or shelf view (multishelf mode), double-click the reporting card to open the card view.
b) Click the **Provisioning** tab.
c) Click the administrative state of any in-service ports.
d) Choose **OOS,MT** (or **Locked,maintenance**)to take the ports out of service.

Step 6 If a circuit has been mapped to the card, complete the Delete a Circuit, on page 314 procedure.

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

Step 7 If the card is paired in a protection scheme, delete the protection group:
a) node view (single-shelf mode) or shelf view (multishelf mode), click the **Provisioning** > **Protection** tabs.
b) Choose the protection group of the reporting card.
c) Click **Delete**.

Step 8 Right-click the card reporting the alarm.

Step 9 Choose **Delete**.

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

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

MEA (PPM)

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

Logical Object: PPM

The Missing Equipment Attributes alarm for the PPM (SFP) is raised when the PPM (SFP) is misprovisioned or unsupported. It can occur when you provision the PPM (SFP) for a wavelength that is explicitly not the first tunable wavelength.

Note When the TNCS-2 card is replacing the TNC card pre-provisioned with OC3 payload on a chassis, the PROV-MISMATCH/MEA alarm is raised. Delete the pre-provisioning on the TNCS-2 card to proceed.

Clear the MEA (PPM) Alarm

Procedure

Step 1 To provision the PPM (SFP), you must first create it in CTC. To do this, complete the following steps:

a) In node view (single-shelf mode) or shelf view (multishelf mode), double-click the reporting card to open the card view.
b) Click the **Provisioning** > **Pluggable Port Modules** tabs. (If you already see the PPM [SFP] listed in the Pluggable Port Modules Area, go to Step 2, on page 186.)
c) Under the Pluggable Port Modules area, click **Create**.
d) In the Create PPM dialog box, choose the card PPM (SFP) number from the drop-down list (for example, PPM 1).
e) Choose the PPM (SFP) type from the second drop-down list, for example PPM (1 Port).
f) Click **OK**.

Note For more information about provisioning MXP or TXP PPMs (SFPs), refer to the Turn Up a Node chapter in the Configuration guide. For information to provision PPMs (SFPs) for the MRC-12 and OC192/STM64-XFP, refer to the Optical Cards chapter in the Configuration guide.

Step 2 After you have created the PPM (SFP), or if you see it listed in the Pluggable Port Modules area but not in the Selected PPM area, choose the port rate:

a) Under the Selected PPM area, click **Create**.
b) In the Create Port dialog box, choose the port (for example, 1-1) from the drop-down list.
c) Choose the correct port type from the drop-down list. (For more information about selecting PPM (SFP) port types, refer to the Provision Transponder and Muxponder Cards chapter of the Configuration guide.)
d) Click **OK**.

Step 3 If you see the port listed in the Pluggable Port Modules area and the Selected PPM area, the MEA indicates that the incorrect port rate was selected. Click the port in the Selected PPM area and click Delete.

Step 4 Complete Step 2, on page 186 to correctly provision the port rate.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

MEA (SHELF)

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

Logical Object: SHELF

The MEA (Shelf) condition is raised when ANSI and ETSI shelves exist in the same node. For example, an ANSI subtended shelf is configured on an ETSI node controller or an ETSI subtended shelf is configured on an ANSI node controller.

The MEA (Shelf) condition is also raised when the original subtended shelf is disconnected and another subtended shelf of different shelf type is connected with the same shelf ID.

Clear the MEA (SHELF) Condition

Procedure

Step 1 (For the first scenario) Ensure that the shelves in the node are either ANSI only or ETSI only.

Step 2 (For the second scenario) Disconnect the newly connected subtended shelf.

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

MEM-GONE

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

Logical Object: EQPT

The Memory Gone alarm occurs when data generated by software operations exceeds the memory capacity of the control cards. The control cards which exceed the memory capacity reboot to avoid failure of card operations.

Note The alarm does not require user intervention. The MEM-LOW alarm always preceeds the MEM-GONE alarm.

MEM-LOW

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

Logical Object: EQPT

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

The alarm does not require user intervention.

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

MFGMEM

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

Logical Objects: AICI-AEP, AICI-AIE, AIP, BPLANE, FAN, PPM, ECU, LCD, PWRM

EEPROM stores manufacturing data that a system uses to determine system compatibility and shelf inventory information.

The Manufacturing Data Memory Failure alarm occurs when:

- EEPROM fails on a card or component.
- The control card cannot read data from EEPROM.

Clear the MFGMEM Alarm

Procedure

Step 1 Soft reset the standby control card.

Step 2 When the standby control card boots up, soft reset the active control card.

Step 3 Reset the specific card on which the EEPROM has failed.

Step 4 If the reset card has not rebooted successfully, or the alarm has not cleared, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

MS-AIS

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

Logical Object: STM1E, STMN

The Multiplex Section (MS) AIS condition indicates that there is a defect in the multiplexing section layer of the SONET overhead. The multiplex section refers to the segment between two SONET devices in the circuit and is also known as a maintenance span. The multiplex section layer of the SONET overhead deals with payload transport, and its functions include multiplexing and synchronization.

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

Clear the MS-AIS Condition

Procedure

Complete the Clear the AIS Condition, on page 18 procedure.

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

MS-DEG

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

Logical Object: STM1E

The Multiplex Section Signal Degrade condition is similar to the SDBER-EXCEED-HO , on page 260 alarm, but applies only to the multiplex section overhead of the EQPT object.

Clear the MS-DEG Condition

Procedure

Complete the Clear the SDBER-EXCEED-HO Condition, on page 260 procedure.

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

MS-EOC

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

Logical Object: STMN

The MS-DCC Termination Failure alarm occurs when the system loses its data communications channel. The DCC is nine bytes, D4 through D12, in the SONET overhead. The bytes convey information about Operation, Administration, Maintenance, and Provisioning (OAM&P). The system uses the DCC on the SONET section overhead to communicate network management information.

Clear the MS-EOC Alarm

Procedure

Complete the Clear the RS-EOC Alarm, on page 255 procedure.

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

MS-EXC

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

Logical Object: STM1E

The Multiplex Section Signal Excessive BER condition is similar to the SDBER-EXCEED-HO , on page 260 alarm, but applies only to the multiplex section overhead of the EQPT object.

Clear the MS-EXC Condition

Procedure

Complete the Clear the SDBER-EXCEED-HO Condition, on page 260 procedure.

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

MS-RFI

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

Logical Object: STM1E, STMN

The MS Remote Fault Indication (RFI) condition indicates that there is an RFI occurring at the SONET overhead multiplexing section level.

An RFI occurs when the NCS detects an RFI in the SONET overhead because of a fault in another node. Resolving the fault in the adjoining node clears the MS-RFI condition in the reporting node.

Clear the MS-RFI Condition

Procedure

Step 1 Log into the far-end node of the reporting NCS.

Step 2 Determine whether there are other alarms, especially the LOS(STM1E, STMN).

Step 3 Clear the main alarm. See the appropriate alarm section in this chapter for the procedure.

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

MT-OCHNC

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

Logical Object: OTS

The MT-OCHNC condition occurs when the user provisions a specific wavelength for maintenance on a WXC card from an input port (EXP1-8, ADD-RX) to the output port (COM-TX).

Clear the MT-OCHNC Condition

Procedure

Delete the provisioned wavelength that was specifically tuned for maintenance purposes on a WXC card.

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

NO-SHARED-CIPHERS Alarm

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

Logical Object: OTS

The NO-SHARED-CIPHERS alarm is raised when the certificates with different encryption cipher or algorithm are provisioned on either the server or the client.

Clear the NO-SHARED-CIPHERS Alarm

Procedure

Verify the same encryption cipher or algorithm is provisioned on both the server and the client.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

NO-VALID-USB-DB

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

Logical Object: USB MODULE

The NO-VALID-USB-DB alarm occurs when all USB database partition validations fail.

Clearing the NO-VALID-USB_DB Alarm

The NO-VALID-USB-DB alarm clears automatically when at least one USB database partition is written and verified successfully during the USBSYNC operation.

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

NON-CISCO-PPM

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

Logical Object: PPM

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

Clear the NON-CISCO-PPM Condition

Procedure

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

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

NON-TRAF-AFFECT-SEC-UPG-REQUIRED

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

Logical Objects: EQUIPMENT

The NON-TRAF-AFFECT-SEC-UPG-REQUIRED alarm is raised when the partition of the control FPGA is not locked.

When you downgrade the WSE card from Release 11.12 to older releases such as R11.1.1.2, R11.0, R10 and so on, the NON-TRAF-AFFECT-SEC-UPG-REQUIRED alarm is raised and does not clear.

Clear the NON-TRAF-AFFECT-SEC-UPG-REQUIRED alarm

Procedure

Step 1 (For WSE card) Place the client and trunk ports in OOS-MT state.

(For WSE card) Place the client and trunk ports in OOS-DSBLD state, if both the NON-TRAF-AFFECT-SEC-UPG-REQUIRED and TRAF-AFFECT-SEC-UPG-REQUIRED alarms are raised on the card.

Step 2 (For WSE card) Perform the FPGA/firmware upgrade.

Step 3 Upgrade the FPGA image and lock the partition of the control FPGA.

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

NODE-FACTORY-MODE

Default Severity: Critical (CR)

Logical Object: NE

The Node Factory Mode alarm is raised when the database is not available due to the following:

- New installation.
- Reset NE to factory defaults.
- Mode conversion from ANSI to ETSI.

Clear the NODE-FACTORY-MODE Alarm

Procedure

Reset to the default setting using 'Rebuild DB' option.

(or)

Restore the database.

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

NOT-AUTHENTICATED

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

Logical Object: SYSTEM

The NOT-AUTHENTICATED alarm is raised by CTC (not by the NE) when 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 , on page 127 alarm, because INTRUSION-PSWD occurs when a user exceeds the login failures threshold.

The NOT_AUTHENTICATED alarm is also raised, when CTC nodes in the network have R10.6 packages and earlier and password policy is less than 80 characters.

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

OCHNC-BDI

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

Logical Objects: OTS

The Optical Channel Network Connection (OCHNC) Backward Defect Indication (BDI) alarm is raised when an OCHNC signal is interrupted along the circuit path and the system is not able to recover it.

Clear the OCHNC-BDI Alarm

Procedure

This alarm is cleared automatically when the interrupt is rectified and the signal flows properly.

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

OCHNC-INC

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

Logical Object: OCHNC-CONN

The Optical Channel (OCH) Incomplete Cross-Connection condition is raised when an OCH cross connection on a two-way circuit is deleted. For example, if you create an OCH circuit on a linear DWDM structure with Nodes A, B and C—originating at Node A, traversing through Node B, and terminating at Node C—then mistakenly delete a cross-connect (such as by TL1 command DLT-WLEN) on Nodes B or C, this condition is raised on the source node (A). The condition is corrected by regenerating the cross-connect. The alarm also follows these guidelines:

- Two-way circuit with Nodes A, B, and C (as described in the preceding example): Deleting a cross-connection on Nodes B or C will raise OCHNC-INC on the Node A cross connection.
- Two-way circuit with Nodes A, B, and C: Deleting a cross connection on Node A will raise an OCHNC-INC alarm on the Node C cross connection.
- One-way circuit with Nodes A, B and C: Deleting a cross connection on Nodes B or C will raise an OCHNC-INC alarm on Node A cross connection.

- One-way circuit with Nodes A, B, and C: Deleting a cross connection on Node A will not raise an OCHNC-INC alarm.

Note If you delete one of the cross-connects, you might not be able to recreate this same circuit because the wavelength is already being used on the other component nodes for add, drop, or express.

The OCHNC-INC alarm can also be raised if you restore one node's database that is inconsistent with other node databases, following the guidelines previously listed. (That is, an inconsistent database that does not contain up-to-date circuit cross-connection information will cause the same problem as if you had deleted the cross-connect.)

Caution It is important to create a backup version of the database for each node of a topology during a known-stable situation. You should give the saved files names that indicate their version and date or any other information needed to verify their consistency.

Clear the OCHNC-INC Alarm

Procedure

Step 1 To recreate the missing cross-connect, establish a Telnet connection with the node where it was deleted and use the ENT-WLEN command with the Add port, Drop port, or Express port on the node.

For information about establishing a TL1 session connection, refer to the SONET TL1 Reference guide. For more information about ENT-WLEN and other TL1 commands, as well as their syntax, refer to the SONET TL1 Command guide.

Step 2 If the alarm is not due to a deleted cross-connect but instead to an inconsistent database being restored on a node, correct the problem by restoring the correct backup version to that node. For the restore procedure, refer to the Maintain the Node chapter in the Configuration guide.

Note When you restore a database on a node, it replaces the database being used on both (ACT and SBY) the control cards as the cards synchronize this version into their active flash memory. If the active (ACT) control card is reset, the standby (SBY) control cards will therefore use the same database version from its active flash memory. In the case of a power-up, both the control cards boot and choose which database to use from two criteria: (1) the most recent version compatible with the node software, and (2) the most recently loaded version of that compatible database (with the highest sequence number).

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

OCHNC-SIP

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

Logical Objects: OTS

The OCHNC Startup in Progress(SIP) alarm is raised when an OCHNC is created and the optical regulation to bring up the traffic is in progress.

Clear the OCHNC-SIP Alarm

Procedure

This alarm is cleared automatically when the OCHNC is successfully created and the optical regulation is complete.

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

OCHTERM-INC

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

Logical Object: OCHTERM

The Optical Termination Incomplete condition is raised against an OCH termination when there is no peer OCH termination at the other end of a span.

Clear the OCHTERM-INC Condition

Procedure

Create an OCH termination at the other end of the span. For procedures to do this, refer to the Configuration guide.

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

ODUK-1-AIS-PM

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

Logical Object: TRUNK

The ODUK-1-AIS-PM is a secondary condition raised on MXP and ADM-10G cards trunk signals when they experience an LOS (2R). Although the ODUK-1-AIS-PM is raised against the TRUNK object, it actually refers to the client signals contained within the trunk.

A single ODUK-x-AIS-PM can occur when one far-end client signal is lost; multiple ODK-x-AIS-PMs can occur (ODUK-1-AIS-PM, ODUK-2-AIS-PM, ODUK-3-AIS-PM, ODUK-4-AIS-PM) if more than one far-end client is lost. If the entire trunk signal is lost, LOS (TRUNK) occurs and demotes any LOS (2R) alarms.

Clear the ODUK-1-AIS-PM Condition

Procedure

Look for and clear the LOS (2R) alarm on the far-end client. This should clear the ODUK-1-AIS-PM condition on the trunk.

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

ODUK-2-AIS-PM

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

Logical Object: TRUNK

The ODUK-2-AIS-PM is a secondary condition raised on MXP and ADM-10G cards trunk signals when they experience an LOS (2R). Although the ODUK-2-AIS-PM is raised against the TRUNK object, it actually refers to the client signals contained within the trunk.

Clear the ODUK-2-AIS-PM Condition

Procedure

Complete the Clear the ODUK-1-AIS-PM Condition, on page 197 procedure.

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

ODUK-3-AIS-PM

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

Logical Object: TRUNK

The ODUK-3-AIS-PM is a secondary condition raised on MXP and ADM-10G cards trunk signals when they experience an LOS (2R). Although the ODUK-3-AIS-PM is raised against the TRUNK object, it actually refers to the client signals contained within the trunk.

Clear the ODUK-3-AIS-PM Condition

Procedure

Complete the Clear the Clear the ODUK-1-AIS-PM Condition, on page 197 procedure.

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

ODUK-4-AIS-PM

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

Logical Object: TRUNK

The ODUK-4-AIS-PM is a secondary condition raised on MXP and ADM-10G cards trunk signals when they experience an LOS (2R). Although the ODUK-4-AIS-PM is raised against the TRUNK object, it actually refers to the client signals contained within the trunk.

Clear the ODUK-4-AIS-PM Condition

Procedure

Complete the Clear the ODUK-1-AIS-PM Condition, on page 197 procedure.

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

ODUK-AIS-PM

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

Logical Object: TRUNK

The Optical Data Unit (ODUK) AIS Path Monitoring (PM) condition is raised when ITU-T G.709 encapsulation is enabled for the cards. ODUK-AIS-PM is a secondary condition that indicates a more serious condition such as the LOS (OCN/STMN) alarm occurring downstream. The ODUK-AIS-PM condition is reported in the

path monitoring area of the optical data unit wrapper overhead. ODUK-AIS-PM is caused by the upstream ODUK-OCI-PM , on page 200.

ITU-T G.709 encapsulation refers to a digital data wrapper that is transparent across networking standards such as SONET and protocols (such as Ethernet or IP).

Clear the ODUK-AIS-PM Condition

Procedure

Step 1 Determine whether the upstream nodes and equipment have alarms, especially the LOS (OCN/STMN) alarm, or OOS (or Locked) ports.

Step 2 Clear the upstream alarms using the Clear the LOS (OCN/STMN) Procedure located in the Troubleshooting guide.

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

ODUK-BDI-PM

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

Logical Object: TRUNK

The ODUK Backward Defect Indicator (BDI) PM condition is raised when ITU-T G.709 encapsulation is enabled for the cards. It indicates that there is a path termination error upstream in the data. The error is read as a BDI bit in the path monitoring area of the digital wrapper overhead.

Clear the ODUK-BDI-PM Condition

Procedure

Complete the Clear the OTUK-BDI Condition, on page 222 procedure.

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

ODUK-LCK-PM

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

Logical Object: TRUNK

The ODUK Locked Defect (LCK) PM condition is raised when ITU-T G.709 encapsulation is enabled for the cards. ODUK-LCK-PM indicates that a signal is being sent downstream to indicate that the upstream connection is locked, preventing the signal from being passed. The lock is indicated by the STAT bit in the path overhead monitoring fields of the optical transport unit overhead of the digital wrapper.

Clear the ODUK-LCK-PM Condition

Procedure

Unlock the upstream node signal.

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

ODUK-OCI-PM

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

Logical Object: TRUNK

The ODUK Open Connection Indication (OCI) PM condition is raised when ITU-T G.709 encapsulation is enabled for the cards. It indicates that the upstream signal is not connected to a trail termination source. The error is read as a STAT bit in the path monitoring area of the digital wrapper overhead. ODUK-OCI-PM causes a downstream ODUK-LCK-PM , on page 199 alarm.

Clear the ODUK-OCI-PM Condition

Procedure

Verify the fiber connectivity at nodes upstream.

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

ODUK-SD-PM

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

Logical Object: TRUNK

The ODUK Signal Degrade (SD) PM condition is raised when ITU-T G.709 encapsulation is enabled. ODUK-SD-PM indicates that incoming signal quality is poor, but the incoming line BER has not passed the fail threshold. The BER problem is indicated in the path monitoring area of the optical data unit frame overhead.

Clear the ODUK-SD-PM Condition

Procedure

Complete the Clear the OTUK-SD Condition, on page 225 procedure.

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

ODUK-SF-PM

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

Logical Object: TRUNK

The ODUK Signal Fail (SF) PM condition (ODUK-SD-PM) is raised when ITU-T G.709 encapsulation is enabled. ODUK-SF-PM indicates that incoming signal quality is poor and the incoming line BER has passed the fail threshold. The BER problem is indicated in the path monitoring area of the optical data unit frame overhead.

Clear the ODUK-SF-PM Condition

Procedure

Complete the Clear the SF (DS1, DS3) Condition procedure located in the Alarm Troubleshooting chapter of the Troubleshooting guide.

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

ODUK-TIM-PM

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

Logical Object: TRUNK

The ODUK-TIM- PM condition applies to the path monitoring area of the OTN overhead. The condition occurs when there is a trace identifier mismatch in the data stream. ODUK-TIM-PM causes an ODUK-BDI-PM , on page 199, downstream.

The ODUK-TIM-PM condition applies to TXP cards and MXP cards when ITU-T G.709 encapsulation is enabled for the cards. It indicates that there is an error upstream in the optical transport unit overhead of the digital wrapper.

ITU-T G.709 encapsulation refers to a digital data wrapper that is transparent across networking standards such as SONET and protocols (such as Ethernet or IP).

Clear the ODUK-TIM-PM Condition

Procedure

Complete the Clear the TIM-P Condition procedure located in the Alarm Troubleshooting chapter of the Troubleshooting guide.

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

OPEN-SLOT

Default Severity: Minor (MN)

Logical Object: SHELF

The Open Slot alarm is raised when an empty slot is detected in a chassis. Empty slots in a chassis lead to thermal failures due to increased temperature of the line cards. Use passive cards such as fillers to prevent air leakage in the chassis.

Note It is recommended to use filler cards to fill in the empty slots. Blank cards are not detected by the software.

Clear the OPEN-SLOT Alarm

Procedure

Use filler cards to fill the empty slots. Blank cards are not detected by the software. For more details about the filler cards, see the Cisco NCS 2000 Series Hardware Installation Guide.

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

OPTNTWMIS

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

Logical Object: NE

The Optical Network Type Mismatch alarm is raised when DWDM nodes are not configured for the same type of network, either MetroCore or MetroAccess. All DWDM nodes on the same network must be configured for the same network type because APC and ANS behave differently on each of these network types. For more information about APC and ANS, refer to the Network Reference chapter in the Configuration guide.

When the OPTNTWMIS alarm occurs, the APC-DISABLED , on page 20 alarm could also be raised.

Clear the OPTNTWMIS Alarm

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode) of the alarmed node, click the **Provisioning** > **WDM-ANS** > **Provisioning** tabs.

Step 2 Choose the correct option from the Network Type list box, and click **Apply**.

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

OPWR-HDEG

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

Logical Objects: AOTS, OCH, OCH-TERM, OMS, OTS

The OPWR- HDEG alarm is raised on the 80-WXC-C ports when the optical power level exceeds the saturation limit of the OCM. The OCM saturation is caused by a power level that is outside the set power range of the OCM. The OCM power range is tuned using the LOS or OPWR-LFAIL threshold values associated with the 80-WXC-C port. The saturation level is +30dBm.

Note The OPWR-HDEG alarm may be raised on the WSS pass through ports of a ROADM configuration when the attenuation is increased at the span level.

Clear the OPWR-HDEG Alarm

Procedure

Step 1 Verify fiber continuity to the port by following site practices. Refer to the Network Reference chapter of the Configuration guide for a procedure to detect a fiber cut.

Step 2 If the cabling is good, confirm that the LED is correctly illuminated on the physical card. A green ACT/SBY LED indicates an active card. A red ACT/SBY LED indicates a failed card.

Step 3 Verify that the power read by photodiode on the port is within the expected range as projected by Cisco TransportPlanner. The application generates a spreadsheet of values containing this information.

Step 4 If the optical power level is within specifications, check the opwrMin threshold. (These are listed in the Configuration guide.) Refer to the *Cisco Transport Planner DWDM Operations Guide* and decide what value to use for modifying the power level:

a) In node view (single-shelf mode) or shelf view (multishelf mode), double-click the card to open the card view.

b) Display the optical thresholds by clicking the following tabs:

- For the OPT-BST, OPT-AMP-C, or OPT-AMP-17-C cards, click the **Provisioning** > **Opt. Ampli. Line** > **Optics Thresholds** tabs.
- For the OPT-PRE, OPT-AMP-C, or OPT-AMP-17-C cards, click the **Provisioning** > **Opt. Ampli. Line** > **Optics Thresholds** tabs.
- For the WXC card, click the **Provisioning** > **Optical Chn** > **Optics Thresholds** tabs.
- For the AD-xC-xx.x card, click the **Provisioning** > **Optical Chn** > **Optics Thresholds** tabs.
- For the AD-xB-xx.x card, click the **Provisioning** > **Optical Band** > **Optics Thresholds** tabs.
-
-
- For the 32WSS card, click the **Provisioning** > **Optical Chn: Optical Connector** *x* > **Optics Thresholds** tabs.
- For the OSCM or OSC-CSM cards, click the **Provisioning** > **Optical Line** > **Optics Thresholds** tabs.
- For the 40-SMR1-C and 40-SMR2-C cards, click the **Provisioning** > **Optical Line** > **Optics Thresholds** tabs.

Step 5 If the received optical power level is within specifications, refer to the *Cisco Transport Planner DWDM Operations Guide* to determine the correct levels and check the opwrMin threshold. (These are listed in the Configuration guide.) If necessary, modify the value as required.

Step 6 If the optical power is outside of the expected range, verify that all involved optical signal sources, namely the TXP or MXP trunk port or an ITU-T line card, are in IS administrative state by clicking the correct tab:

- For the MXPP_MR_2.5G card, click the **Provisioning** > **Line** > **SONET** (or **Provisioning** > **Line** > **SDH**) tabs.
- For the MXP_2.5G_10E card, click the **Provisioning** > **Line** > Trunk tabs.
- For the MXP_2.5G_10G card, click the **Provisioning** > **Line** > **SONET** (or **Provisioning** > **Line** > **SDH**) tabs.
- For the MXP_MR_2.5G card, click the **Provisioning** > **Line** > **SONET** (or **Provisioning** > **Line** > **SDH**) tabs.
- For the TXPP_MR_2.5G card, click the **Provisioning** > **Line** > **SONET** (or **Provisioning** > **Line** > **SDH**) tabs.
- For the TXP_MR_10E card, click the **Provisioning** > **Line** > **SONET** (or **Provisioning** > **Line** > **SDH**) tabs.
- For the TXP_MR_10G card, click the **Provisioning** > **Line** > **SONET** (or **Provisioning** > **Line** > **SDH**) tabs.

- For the TXP_MR_2.5G card, click the **Provisioning** > **Line** > **SONET** (or **Provisioning** > **Line** > **SDH**) tabs.

If it is not IS, choose **IS** (or **Unlocked**) from the administrative state drop-down list. This creates the IS-NR service state.

Step 7 If the port is in IS (or Unlocked) state but its output power is outside of the specifications, complete the Clear the LOS-P (OCH) Alarm, on page 167 procedure. (These specifications are listed in the Configuration guide.)

Step 8 If the signal source is IS and within expected range, come back to the unit reporting OPWR-HDEG and clean all connected fiber in the same line direction as the reported alarm according to site practice. If no site practice exists, complete the procedure in the Maintain the Node chapter of the Configuration guide.

Note Unplugging fiber can cause a traffic hit. To avoid this, perform a traffic switch if possible. Refer to the procedures in the Protection Switching, Lock Initiation, and Clearing, on page 306 section. For more detailed protection switching information, refer to the Configuration guide.

Step 9 Repeat Steps Step 1, on page 203 to Step 8, on page 205 for any other port on the card reporting the OPWR-HDEG alarm.

Step 10 If the optical power is outside of the expected range for the 80-WXC-C card, check the power level coming from the another card port that is connected to the alarmed 80-WXC-C port and verify if a bulk attenuator was installed as provisioned by CTP.

Step 11 If the OCM power range is incorrect for the 80-WXC-C card, verify if the Channel LOS Threshold parameter associated with the failing port and wavelength was imported correctly from CTP to CTC using the NE update file and if the parameter was applied to the card ports using the Launch ANS function.

Step 12 If the alarm does not clear, look for and troubleshoot any other alarm that could identify the source of the problem.

Step 13 If no other alarms exist that could be the source of the OPWR-HDEG, or if clearing an alarm did not clear the alarm, place all of the card ports in **OOS,DSBLD** (or **Locked,disabled**) administrative state.

Step 14 Complete the Physically Replace a Card, on page 313 procedure for the reporting card.

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

OPWR-HFAIL

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

Logical Objects: AOTS, OCH, OMS, OTS

The Output Power Failure alarm occurs on an amplifier card (OPT-BST, OPT-PRE, OPT-AMP-C, EDRA-x-xx, or OPT-AMP-17-C) AOTS port; 40-SMR1-C and 40-SMR2-C card LINE-RX port; and WXC card OCH port. This alarm is raised in the control gain mode and the control power working mode.

Clear the OPWR-HFAIL Alarm

Procedure

Step 1 In the amplifier card view, navigate to **Provisioning** → **Optical Line** → **Parameters** tab to check whether the value of the Transmit Optical Power on the adjacent site is within the limit.

Step 2 If the Transmit Optical Power is too high, check for the OSC PPM mode in network view by navigating to **Provisioning** → **WDM-ANS** → **Provisioning** tab. Validate if it is correct.

Step 3 Set the OSC PPM mode in the TNCS-O card view by navigating to **Provisioning** → **Line**→ **Ports** tab as per the requirement (LX, SX, ULH, LR2, T, FX, LX_10). Rate may vary the transmit power value from high power to low power.

Step 4 Check if the alarm clears on the other end.

Note There is no threshold value for this alarm on the card to validate and change.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

OPWR-LDEG

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

Logical Objects: AOTS, OCH, OCH-TERM, OMS, OTS

The OPWR-LDEG alarm is raised on the 80-WXC-C ports when the optical power level is lower than the saturation limit of the OCM.

Clear the OPWR-LDEG Alarm

Procedure

Complete the Clear the OPWR-HDEG Alarm, on page 203 procedure.

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

OPWR-LFAIL

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

Logical Objects: AOTS, OCH, OCH-TERM, OMS, OTS

Clear the OPWR-LFAIL Alarm

Procedure

Complete the Clear the OPWR-HDEG Alarm, on page 203 procedure.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

OSRION

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

Logical Objects: AOTS, OTS

The Optical Safety Remote Interlock On (OSRION) condition is raised on an amplifier card when OSRI is set to ON. The condition does not correlate with the OPWR-LFAIL , on page 206 alarm, which is also reported on the same port.

Clear the OSRION Condition

Procedure

Turn the OSRI off:

a) In node view (single-shelf mode) or shelf view (multishelf mode), double-click the card to open the card view.
b) Click the **Maintenance** > **ALS** tabs.
c) In the OSRI column, choose **OFF** from the drop-down list.

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

OTDR-ABSOLUTE-A-EXCEEDED-RX

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

Logical Object: EQPT

The Optical Time Domain Reflectometer (OTDR) Absolute Attenuation Threshold Exceeded in Rx direction alarm is raised when the attenuation event in the last scan exceeds the absolute threshold in the Rx direction.

Clear the OTDR-ABSOLUTE-A-EXCEEDED-RX Alarm

Procedure

The alarm is cleared automatically when one of the following conditions is satisfied in the last scan:

- The attenuation event causing the alarm disappears.
- The attenuation event in the last scan is below the threshold.
- The absolute check is deactivated.

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

OTDR-ABSOLUTE-A-EXCEEDED-TX

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

Logical Object: EQPT

The Optical Time Domain Reflectometer (OTDR) Absolute Attenuation Threshold Exceeded in Tx direction alarm is raised when the attenuation event in the last scan exceeds the absolute threshold in Tx direction.

Clear the OTDR-ABSOLUTE-A-EXCEEDED-TX Alarm

Procedure

The alarm is cleared automatically when one of the following conditions is satisfied in the last scan:

- The attenuation event causing the alarm disappears.
- The attenuation event in the last scan is below the threshold.
- The absolute threshold check is deactivated.

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

OTDR-ABSOLUTE-R-EXCEEDED-RX

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

Logical Object: EQPT

The Optical Time Domain Reflectometer (OTDR) Absolute Reflectance Threshold Exceeded in Rx Direction alarm is raised when the reflectance event in the last scan exceeds the absolute threshold in the Rx direction.

Clear the OTDR-ABSOLUTE-R-EXCEEDED-RX Alarm

Procedure

The alarm is cleared automatically when one of the following conditions is satisfied in the last scan:

- The reflectance event causing the alarm disappears.
- The reflectance event in the last scan is below the threshold.
- The absolute threshold check is deactivated.

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

OTDR-ABSOLUTE-R-EXCEEDED-TX

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

Logical Object: EQPT

The Optical Time Domain Reflectometer (OTDR) Absolute Reflectance Threshold Exceeded in Tx Direction alarm is raised when the reflectance event in the last scan exceeds the absolute threshold in the Tx direction.

Clear the OTDR-ABSOLUTE-R-EXCEEDED-TX Alarm

Procedure

The alarm is cleared automatically when one of the following conditions is satisfied in the last scan:

- The reflectance event causing the alarm disappears.
- The reflectance event in the last scan is below the threshold.
- The absolute threshold check is deactivated.

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

OTDR-BASELINE-A-EXCEEDED-RX

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

Logical Object: EQPT

The Optical Time Domain Reflectometer (OTDR) Baseline Attenuation Threshold Exceeded Rx alarm is raised when an existing attenuation event in the last scan or a new attenuation event exceeds the baseline threshold in the Rx direction.

Clear the OTDR-BASELINE-A-EXCEEDED-RX Alarm

Procedure

The alarm is cleared automatically when one of the following conditions is satisfied:

- The attenuation event causing the alarm disappears.
- The attenuation event is below the threshold.
- The absolute check is activated.

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

OTDR-BASELINE-A-EXCEEDED-TX

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

Logical Objects: EQPT

The Optical Time Domain Reflectometer (OTDR) Baseline Attenuation Threshold Exceeded Tx alarm is raised when an existing attenuation event in the last scan or a new attenuation event exceeds the baseline threshold in the Tx direction.

Clear the OTDR-BASELINE-A-EXCEEDED-TX Alarm

Procedure

The alarm is cleared automatically when one of the following conditions is satisfied:

- The attenuation event causing the alarm disappears.
- The attenuation event is below the threshold.
- The absolute check is activated.

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

OTDR-BASELINE-R-EXCEEDED-RX

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

Logical Objects: PPM

The Optical Time Domain Reflectometer (OTDR) Baseline Reflectance Threshold Exceeded Rx alarm is raised when an existing reflectance event in the last scan or a new reflectance event exceeds the baseline threshold in the Rx direction.

Clear the OTDR-BASELINE-R-EXCEEDED-RX Alarm

Procedure

The alarm is cleared automatically when one of the following conditions is satisfied:

- The reflectance event causing the alarm disappears.
- The reflectance event is below the threshold.
- The absolute threshold check is activated.

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

OTDR-BASELINE-R-EXCEEDED-TX

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

Logical Object: PPM

The Optical Time Domain Reflectometer (OTDR) Baseline Reflectance Threshold Exceeded Tx alarm is raised when an existing reflectance event in the last scan or a new reflectance event exceeds the baseline threshold in the Tx direction.

Clear the OTDR-BASELINE-R-EXCEEDED-TX Alarm

Procedure

The alarm is cleared automatically when one of the following conditions is satisfied:

- The reflectance event causing the alarm disappears.
- The reflectance event is below the threshold.
- The absolute threshold check is activated.

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

OTDR-FAST-FAR-END-IN-PROGRESS

Default Severity: Minor (MN)

Logical Object: EQUIPMENT

The OTDR-FAST-FAR-END-IN-PROGRESS alarm is raised when a fast scan is started on the remote side.

Clear the OTDR-FAST-FAR-END-IN-PROGRESS Alarm

Procedure

Step 1 Wait until the scan on the remote side is completed. The time varies depending on the type of scan.

Step 2 Alternatively, stop the scan by navigating to: **Maintenance**->**DWDM**->**OTDR**; select the side where the scan is ongoing and click **Cancel**. The scan is stopped on both the sides.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OTDR-FAST-SCAN-IN-PROGRESS-RX

Default Severities: Minor (MI), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Optical Time Domain Reflectometer (OTDR) Fast Scan In Progress Rx alarm is raised when the fast OTDR scan starts in the Rx direction.

Clear the OTDR-FAST-SCAN-IN-PROGRESS-RX Alarm

Procedure

Step 1 This alarm is cleared automatically when the fast OTDR scan in the RX direction is complete.

Step 2 Alternatively, stop the scan by navigating to: **Maintenance**->**DWDM**->**OTDR**; select the side where the scan is ongoing and click **Cancel**. The scan is stopped on both the sides.

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

OTDR-FAST-SCAN-IN-PROGRESS-TX

Default Severities: Minor (MI), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Optical Time Domain Reflectometer (OTDR) Fast Scan In Progress TX alarm is raised when the fast OTDR scan starts in the TX direction.

Clear the OTDR-FAST-SCAN-IN-PROGRESS-TX Alarm

Procedure

Step 1 This alarm is cleared automatically when the fast OTDR scan in the TX direction is complete.

Step 2 Alternatively, stop the scan by navigating to: **Maintenance**->**DWDM**->**OTDR**; select the side where the scan is ongoing and click **Cancel**. The scan is stopped on both the sides.

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

OTDR-FIBER-END-NOT-DETECTED-RX

Default Severity: NA

Logical Object: EQUIPMENT

The OTDR-FIBER-END-NOT-DETECTED-RX alarm is raised when the OTDR module cannot return a valid fiber end.

Clear the OTDR-FIBER-END-NOT-DETECTED-RX Alarm

Procedure

Execute the Auto Scan.

Note If the fiber is affected by high reflections or if the fiber is longer than 100 km, the fiber end cannot be found. Hence, the alarm will not be cleared.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OTDR-FIBER-END-NOT-DETECTED-TX

Default Severity: NA

Logical Object: EQUIPMENT

The OTDR-FIBER-END-NOT-DETECTED-TX alarm is raised when the OTDR module cannot return a valid fiber end.

Clear the OTDR-FIBER-END-NOT-DETECTED-TX Alarm

Procedure

Execute the Auto Scan.

Note If the fiber is affected by high reflections or if the fiber is longer than 100 km, the fiber end cannot be found. Hence, the alarm will not be cleared.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OTDR-HYBRID-FAR-END-IN-PROGRESS

Default Severity: NA

Logical Object: EQUIPMENT

The OTDR-HYBRID-FAR-END-IN-PROGRESS alarm is raised when a hybrid scan is started on the remote side.

Clear the OTDR-HYBRID-FAR-END-IN-PROGRESS Alarm

Procedure

Step 1 Wait until the scan on the remote side is completed.

The time varies depending on the type of scan.

Step 2 Alternatively, stop the scan by navigating to: **Maintenance**->**DWDM**->**OTDR**; select the side where the scan is ongoing and click **Cancel**. The scan is stopped on both the sides.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OTDR-HYBRID-SCAN-IN-PROGRESS-RX

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

Logical Objects: PPM

The Optical Time Domain Reflectometer (OTDR) Hybrid Scan In Progress RX condition occurs when a hybrid OTDR scan starts in the RX direction.

Clear the OTDR-HYBRID-SCAN-IN-PROGRESS-RX Alarm

Procedure

Step 1 This alarm is cleared automatically when the hybrid OTDR scan in the RX direction is complete.

Step 2 Alternatively, stop the scan by navigating to: **Maintenance**->**DWDM**->**OTDR**; select the side where the scan is ongoing and click **Cancel**. The scan is stopped on both the sides.

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

OTDR-HYBRID-SCAN-IN-PROGRESS-TX

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

Logical Objects: PPM

The Optical Time Domain Reflectometer (OTDR) Hybrid Scan In Progress TX condition occurs when a hybrid OTDR scan starts in the TX direction.

Clear the OTDR-HYBRID-SCAN-IN-PROGRESS-TX Alarm

Procedure

Step 1 This alarm is cleared automatically when the hybrid OTDR scan in the TX direction is complete.

Step 2 Alternatively, stop the scan by navigating to: **Maintenance**->**DWDM**->**OTDR**; select the side where the scan is ongoing and click **Cancel**. The scan is stopped on both the sides.

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

OTDR-ORL-THRESHOLD-EXCEEDED-RX

Default Severity: Minor (MN)

Logical Object: EQUIPMENT

The OTDR-ORL-THRESHOLD-EXCEEDED-RX alarm is raised if the current ORL value crosses its threshold value.

Clear the OTDR-ORL-THRESHOLD-EXCEEDED-RX Alarm

Procedure

Step 1 Clean the fiber on the major reflection contribution.

Major reflection contribution can be found in the OTDR Scans.

Step 2 Alternatively, change the ORL threshold from Provisioning > WDM-ANS > OTDR > Side > Baseline Thresholds tab.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OTDR-ORL-THRESHOLD-EXCEEDED-TX

Default Severity: Minor (MN),

Logical Object: EQUIPMENT

The OTDR-ORL-THRESHOLD-EXCEEDED-TX alarm is raised if the current ORL value crosses its threshold value.

Clear the OTDR-ORL-THRESHOLD-EXCEEDED-TX Alarm

Procedure

Step 1 Clean the fiber on the major reflection contribution.

Major reflection contribution can be found in the OTDR Scans.

Step 2 Alternatively, change the ORL threshold from Provisioning > WDM-ANS > OTDR > Side > Baseline Thresholds tab.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OTDR-ORL-TRAINING-FAILED-RX

Default Severity: Minor (MN)

Logical Object: EQUIPMENT

The OTDR-ORL-TRAINING-FAILED-RX alarm is raised if the training phase cannot find valid calibration data.

Clear the OTDR-ORL-TRAINING-FAILED-RX Alarm

Procedure

Execute the scan in the RX direction.

Note If the scan shows high reflections, clean the connectors where the reflections are too high or change the corresponding patchcords.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OTDR-ORL-TRAINING-FAILED-TX

Default Severity: Minor (MN)

Logical Object: EQUIPMENT

The OTDR-ORL-TRAINING-FAILED-TX alarm is raised if the training phase cannot find valid calibration data.

Clear the OTDR-ORL-TRAINING-FAILED-TX Alarm

Procedure

Execute the scan in the TX direction.

Note If the scan shows high reflections, clean the connectors where the reflections are too high or change the corresponding patchcords.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OTDR-ORL-TRAINING-IN-PROGRESS-RX

Default Severity: NA

Logical Object: EQUIPMENT

The OTDR-ORL-TRAINING-IN-PROGRESS-RX alarm is raised if the ORL is started in the fast mode on the Rx side.

Clear the OTDR-ORL-TRAINING-IN-PROGRESS-RX Alarm

Procedure

Wait until ORL training is completed in the Rx side. ORL training takes 10 seconds.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OTDR-ORL-TRAINING-IN-PROGRESS-TX

Default Severity: NA

Logical Object: EQUIPMENT

The OTDR-ORL-TRAINING-IN-PROGRESS-TX alarm is raised if the Optical Return Loss (ORL) is started in the fast mode on the Tx side.

Clear the OTDR-ORL-TRAINING-IN-PROGRESS-TX Alarm

Procedure

Wait until ORL training is completed in the Tx side. ORL training takes 10 seconds.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OTDR-OTDR-TRAINING-FAILED-RX

Default Severity: NA

Logical Object: EQUIPMENT

The OTDR-OTDR-TRAINING-FAILED-RX alarm is raised if the training phase cannot find valid calibration data.

Clear the OTDR-OTDR-TRAINING-FAILED-RX Alarm

Procedure

Execute the training scan in the RX direction.

Note If the scan shows high reflections, clean the connectors where the reflections are too high or change the corresponding patchcords.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OTDR-OTDR-TRAINING-FAILED-TX

Default Severity: NA

Logical Object: EQUIPMENT

The OTDR-OTDR-TRAINING-FAILED-TX alarm is raised if the training phase cannot find valid calibration data.

Clear the OTDR-OTDR-TRAINING-FAILED-TX Alarm

Procedure

Execute the training scan in the TX direction.

Note If the scan shows high reflections, clean the connectors where the reflections are too high or change the corresponding patchcords.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OTDR-SCAN-FAILED

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

Logical Object: EQPT

The Optical Time Domain Reflectometer (OTDR) scan failed alarm is raised when the OTDR scan fails and no result is sent to the user.

Clear the OTDR-SCAN-FAILED Alarm

Procedure

This alarm is automatically cleared when no failed scan remains on for all sectors of the target PPM.

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

OTDR-SCAN-IN-PROGRESS

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

Logical Objects: PPM

The Optical Time Domain Reflectometer (OTDR) Scan In Progress condition occurs under one of the following conditions:

A scan is initiated on a node which is running a release that does not support new scan initiated alarms (reporting, scan type, and direction) and full duplex scan (scan started on both nodes).

If communication between the two nodes is available, then the alarm is also raised on remote node (even if the node is running a newer release, supporting new OTDR scan in progress alarms).

The condition is cleared automatically when the OTDR scan is completed (either successfully or by timeout/error). When the scan successfully completes, a graph is obtained in the user interface and OSC links gets re-established. This transient condition does not result in a standing condition.

OTDR-SCAN-NOT-COMPLETED

Default Severity: Minor (MN)

Logical Object: EQUIPMENT

The OTDR-SCAN-NOT-COMPLETED alarm is raised when the scan has not been executed on the span in the TX direction.

Clear the OTDR-SCAN-NOT-COMPLETED Alarm

Procedure

Step 1 Execute a manual OTDR scan over the port or direction where the alarm has been raised.

Step 2 Alternatively, stop the scan by navigating to: **Maintenance**->**DWDM**->**OTDR**; select the side where the scan is ongoing and click **Cancel**. The scan is stopped on both the sides.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OTUK-AIS

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

Logical Object: TRUNK

The Optical Transport Unit (OTUK) AIS condition applies when ITU-T G.709 encapsulation is enabled for the cards. OTUk-AIS is a generic AIS signal with a repeating AIS PN-11 sequence. This pattern is inserted by the card in the ITU-T G.709 frame (Trunk) when a faulty condition is present on the client side.

The detection of an OTUK-AIS on the RX-Trunk port of a near-end TXP or MXP is a secondary condition that indicates a more serious issue occurring on the far-end TXP/MXP card connected upstream, most likely on the client side. OTUK-AIS is reported in the optical transport unit overhead of the digital wrapper.

ITU-T G.709 encapsulation refers to a digital data wrapper that is transparent across networking standards such as SONET and protocols (such as Ethernet or IP).

Clear the OTUK-AIS Condition

Procedure

Complete the Clear the AIS Condition, on page 18 procedure.

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

OTUK-BDI

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

Logical Object: TRUNK

The Section Monitoring Backward Defect Indication (OTUK-BDI) condition when ITU-T G.709 encapsulation feature is enabled for the cards. The presence of OTUK-BDI is detected by ITU-T G.709 frame section-monitoring overhead field. The BDI bit is a single bit defined to convey the signal fail status detected in a section termination sink in the upstream direction.

Note If the near-end TXP detects an OTUK-BDI condition on its Trunk-RX port, this means that the far-end TXP has inserted the BDI bit in the transmitted (Trunk-Tx) frame, because a failure such as LOS or SD was detected on the Trunk-RX port. Troubleshoot the failure on the far-end side to clear this condition. For information about various DWDM LOS alarms, refer to the appropriate sections in this chapter.

ITU-T G.709 encapsulation refers to a digital data wrapper that is transparent across networking standards such as SONET and protocols (such as Ethernet or IP).

Clear the OTUK-BDI Condition

Procedure

Step 1 At the near-end node, use site practices to clean trunk transmitting fiber toward the far-end node and the client receiving fiber.

Step 2 At the far-end node, determine whether an OTUK-AIS , on page 221 condition, is present on the Trunk-RX. If so, the root cause to be investigated is the Trunk-Tx side on the near-end card (the one alarmed for OTUK-BDI) because that is the section where the AIS bit is inserted.

Step 3 If there is no OTUK-AIS at the far-end node, continue to investigate performances of the Trunk-Rx: Look for other OTU-related alarms, such as the OTUK-LOF , on page 223 condition or OTUK-SD , on page 224 condition at the far-end Trunk-RX. If either is present, resolve the condition using the appropriate procedure in this chapter.

Step 4 If the OTUK-BDI alarm does not clear, use an OTN test set such as the Agilent OmniBerOTN tester to to check near-end transmitting signal quality. (For specific procedures to use the test set equipment, consult the manufacturer.)

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

OTUK-IAE

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

Logical Object: TRUNK

The OTUK Section-Monitoring Incoming Alignment Error (IAE) alarm occurs when ITU-T G.709 encapsulation is enabled for the cards and the trunk connection is present. This alarm is raised on the near-end node to indicate that the far-end node it has detected errors in the received OTUK frames, but they are not bad enough to cause an OTUK-LOF , on page 223 alarm.

The IAE bit in the section overhead allows the ingress point (in this case, the far-end node) to inform its corresponding egress (near-end) point that the alignment error is detected on the incoming signal OTUK frame alignment errors from NE. The error is an out-of-frame (OOF) alignment, in which the optical transport unit overhead frame alignment (FAS) area is errored for more than five frames.

Clear the OTUK-IAE Alarm

Procedure

Step 1 At the near-end and far-end node, use site practices to clean transmitting fiber on near-end node's reporting port and receiving fiber on correspondent far-end port.

Step 2 If the OTUK-IAE alarm does not clear, look for other OTU-related alarm, such as the OTUK-LOF , on page 223 alarm, at the far-end node and resolve it using the appropriate procedure in this guide.

Step 3 If the OTUK-IAE alarm does not clear, use an OTN test set such as the Agilent OmniBerOTN tester to to check near-end transmitting signal quality. For specific procedures to use the test set equipment, consult the manufacturer.

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

OTUK-LOF

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

Logical Object: TRUNK

The Optical Transport Unit Loss of Frame (OTUK-LOF) alarm applies when ITU-T G.709 encapsulation is enabled for the cards. The ITU-T G.709 encapsulation refers to a digital data wrapper that is transparent across networking standards such as SONET, Ethernet or IP protocols. The alarm indicates that the card has lost frame delineation on the input data. Loss of frame occurs when the optical transport unit overhead frame alignment (FAS) area is errored for more than five frames and that the error persists more than three milliseconds.

The OTUK-LOF alarm is raised under one of the following conditions:

- FEC settings on the trunk ports of the source and destination cards are different.
- Wavelength received on the trunk port and the wavelength configured on the trunk port is different.

Clear the OTUK-LOF Alarm

Procedure

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

Caution Always use the supplied electrostatic discharge wristband when working with a powered NCS system. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly. To verify cable continuity, follow site practices.

Step 2 At the far-end node, verify the cabling of the Trunk-TX port of the TXP or MXP connected to alarmed card in the near-end. Clean the fibers according with site practice.

Step 3 At the far-end node, verify the ITU-T G.709 encapsulation configuration of the Trunk-TX of the TXP/MXP connected to the alarmed card in the near end.

Step 4 Look for other OTU-related alarms at the far-end Trunk-TX and resolve them if necessary using the appropriate procedure in this guide.

Step 5 If the OTUK-LOF alarm does not clear on the near end, use an OTN test set such as the Agilent OmniBer OTN tester to check far-end ITU-T G.709 transmitting signal quality. (For specific procedures to use the test set equipment, consult the manufacturer.)

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

OTUK-SD

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

Logical Object: TRUNK

The OTUK-SD condition applies when ITU-T G.709 encapsulation is enabled. The condition indicates that incoming signal quality is poor, but the incoming line BER has not passed the fail threshold. The BER value

is calculated on the Trunk-Rx port incoming ITU-T G.709 encapsulation frame. If FEC or E-FEC feature is enabled, the BER is a pre-FEC measurement.

ITU-T G.709 encapsulation refers to a digital data wrapper that is transparent across networking standards such as SONET and protocols (such as Ethernet or IP).

Clear the OTUK-SD Condition

Procedure

Step 1 Ensure that the fiber connector for the card is completely plugged in. For more information about fiber connections and card insertion, refer to the Turn Up a Node chapter in the Configuration guide.

Step 2 If the BER threshold is correct and at the expected level, use an optical test set to measure the power level of the line to ensure it is within guidelines. For specific procedures to use the test set equipment, consult the manufacturer.

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

Step 4 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 Configuration guide.

Step 5 If the condition does not clear, verify that single-mode fiber is used.

Step 6 If the fiber is of the correct type, verify that a single-mode laser is used at the far-end node.

Step 7 Clean the fiber connectors at both ends for a signal degrade according to site practice.

Step 8 Verify that a single-mode laser is used at the far end.

Step 9 If the problem does not clear, the transmitter at the other end of the optical line could be failing and require replacement. Refer to the Physical Card Reseating, Resetting, and Replacement, on page 312 section.

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

OTUK-SF

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

Logical Object: TRUNK

The OTUK-SF condition applies when ITU-T G.709 encapsulation is enabled. The condition indicates that incoming signal quality is poor and that the BER for the incoming line has passed the fail threshold. The BER value is calculated on the Trunk-Rx port incoming ITU-T G.709 encapsulation frame. If FEC or E-FEC feature is enabled, the BER is a pre-FEC measurement.

ITU-T G.709 encapsulation refers to a digital data wrapper that is transparent across networking standards such as SONET and protocols (such as Ethernet or IP).

Clear the OTUK-SF Condition

Procedure

Complete the Clear the OTUK-SD Condition, on page 225 procedure.

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

OTUK-TIM

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

Logical Object: TRUNK

The OTUK-TIM alarm applies when ITU-T G.709 encapsulation is enabled and section trace mode is set to manual. The alarm indicates that the expected section-monitoring trail trace identifier (TT1) string does not match the received TTI string and raises a Trace Identifier Mismatch (TIM) alarm. The TIM alarm in turn, triggers an OTUK-BDI , on page 222 alarm.

ITU-T G.709 encapsulation refers to a digital data wrapper that is transparent across networking standards such as SONET and protocols (such as Ethernet or IP).

When the trace mode is set to manual at the section and path level and the OTUk-TTI string is 64 bytes, the OTUK-TIM alarm is triggered. This error condition occurs when the OTUk-TTI string is configured along with ODUk-TTI string and the OTUk-TTI string is 64 Bytes. If the OTUk-TTI string is 63 bytes or if you configure all the 64 bytes of the OTUk-TTI string without configuring the ODUk TTI string, the alarm is not triggered.

For the above error condition, you can restrict the length of the provisioned OTUk-TIM messages to 32 bytes, or disable manual insertion of TTI in the ODUk layer if you want to configure all the 64 bytes.

Clear the OTUK-TIM Condition

Procedure

Complete the Clear the TIM Alarm, on page 282 procedure.

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

OUT-OF-BUNDLE

Default Severity:

- On GE physical ports: Minor (MN), Non-Service-Affecting (NSA)
- On Channel Group port: Major (MJ), Service-Affecting (SA)

Logical Objects: ETH, CHGRP

The Out Of Bundle (OUT-OF-BUNDLE) condition occurs on GE_XP and 10GE_XP cards when the physical port is placed outside the channel group bundle. It can also be raised on a channel group when all the members of the bundle are placed outside the channel group bundle.

Clear the OUT-OF-BUNDLE Condition

Procedure

Step 1 Make sure that the ports' expected speed and duplex settings are same as that of the channel group.

Step 2 LACP mode configured between the peer ports must be valid. For example, you cannot have a passive-passive combination.

OUT-OF-SYNC

Default Severity: Major (MJ), Service-Affecting (SA); Not Alarmed (NA), Non-Service-Affecting (NSA) for ISC

Logical Objects: FC, GE, ISC, TRUNK

The Ethernet Out of Synchronization condition occurs on TXP_MR_2.5, TXPP_MR_2.5, GE-XP, 10GE-XP, and ADM-10G cards when the PPM (SFP) port is not correctly configured for the Gigabit Ethernet payload rate.

Clear the OUT-OF-SYNC Condition

Procedure

Step 1 In node view (single-shelf mode) or shelf view (multishelf mode), double-click the alarmed card to open the card view.

Step 2 Click the **Provisioning** > **Pluggable Port Modules** tabs.

Step 3 Delete the provisioning for the PPM (SFP) by completing the following steps:

a) Click the PPM (SFP) in the Selected PPM area.
b) Click **Delete**.

Step 4 Recreate the PPM (SFP):

a) In the Pluggable Port Modules area, click **Create**.
b) In the Create PPM dialog box, choose the PPM (SFP) number you want to create.
c) Click **OK**.

Step 5 After the PPM (SFP) is created, provision the port data rate:

a) In the Pluggable Ports area, click **Create**.
b) In Create Port dialog box, choose **ONE_GE** from the Port Type drop-down list.
c) Click **OK**.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

OVER-TEMP-UNIT-PROT

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

Logical Object: EQPT

The OVER_TEMP-UNIT-PROT alarm applies to the 100G-LC-C card. The alarm occurs when the temperature of any one of the internal measurement points exceeds its predefined threshold. The alarm is raised because of one of these reasons:

- An improper rack installation
- Abnormally high environmental temperature
- An unclean air filter
- A hardware failure of the card

When the card raises this alarm, the TX output power is shut down. This mechanism prevents the card from damage.

Clearing the OVER-TEMP-UNIT-PROT Alarm

Procedure

Step 1 Verify that the rack is installed properly. For proper airflow and cooling of the shelf, the shape of the vertical posts of the rack should be such that the airflow vents are not covered. For more information about the installation, refer to the *Hardware Installation Guide*.

Step 2 If the rack installation is proper, verify that the environmental temperature of the room is not abnormally high.

Step 3 If the room temperature is not abnormally high, ensure that nothing prevents the fan-tray assembly from passing air through the NCS system shelf.

Step 4 If airflow is not blocked, determine whether the air filter needs replacement. Refer to the Inspect, Clean, and Replace the Air Filter, on page 316 procedure.

Step 5 If the air filter is clean, complete the Remove and Reinsert (Reseat) Any Card , on page 313 procedure.

Step 6 If the alarm fails to get cleared, complete the Physically Replace a Card, on page 313 procedure.

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

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

PARAM-MISM

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

Logical Objects: AOTS, OCH, OCH-TERM, OMS, OTS

The PARAM-MISM condition is raised on the OPT-EDFA-17 card, when an invalid Gain setpoint is provisioned by the control card.

The Gain setpoint for the OPT-EDFA-17 card is automatically calculated by the control card when the amplifier is turned up. The Gain Degrade Low threshold value is always 2 dB lower than the Gain setpoint value.

The APC-OUT-OF-RANGE alarm is raised on the OPT-EDFA-17 card when the Gain setpoint value that was calculated by the control card sets the Gain Degrade Low threshold to a value that is lower than the minimum setpoint value. The APC-OUT-OF-RANGE alarm triggers the PARAM-MISM alarm. This is because the Gain setpoint or the Gain Degrade Low Threshold value is outside the Gain setpoint range of the OPT-EDFA-17 card.

PATCH-ACTIVATION-FAILED

Default Severity: Critical (CR), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Patch-Activation-Failed alarm is raised when the patch fails to activate. The alarm is cleared when the patch is disabled or when a different patch is activated.

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

PATCH-DOWNLOAD-FAILED

Default Severity: Critical (CR), Non-Service-Affecting (NSA)

Logical Object: NE

The Patch-Download-Failed alarm is raised when the patch fails to download. The patch might not download under the following conditions:

- Wrong patch header
- Communication failure between the user interface and the node controller or standalone shelf. In multishelf setup, communication failure between the node controller and the subtended shelf controller.

The alarm is cleared when the patch is downloaded successfully.

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

PAYLOAD-UNKNOWN

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

Logical Object: PPM

The AR_MXP and AR_XP cards support auto-sensing of client payloads. The PAYLOAD-UNKNOWN alarm occurs when the port is unable to detect a valid signal.

Clear the PAYLOAD-UNKNOWN Alarm

Procedure

Clear the PAYLOAD-UNKNOWN alarm with either of these procedures:

a) Ensure that a valid payload signal is received by the port. The alarm clears after detecting a valid signal.

b) Disable the auto-sense option:

1. Login to CTC.
2. In node view (single-shelf mode) or shelf view (multishelf view), double-click the AR_MXP or AR_XP card where you want to disable auto-sensing.
3. Click the **Provisioning** > **Line** > **Auto Ports** tabs.
4. Uncheck the **Auto Sensing** check box.

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

PDI-P

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

Logical Object: STSMON, STSTRM

PDI-P is a set of application-specific codes indicating a signal label mismatch failure (SLMF) in the NCS 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 , on page 17 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) or the CARLOSS (G1000) 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) 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 SDH Ethernet Card Software Feature and Configuration Guide for more information about ML-Series cards.

Warning **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 SDH Ethernet Card Software Feature and Configuration Guide.

Clear the PDI-P Condition

Procedure

Step 1 Verify that all circuits terminating in the reporting card are DISCOVERED:

a) Click the **Circuits** tab.
b) Verify that the **Status** column lists the circuit as active.
c) If the Status column lists the circuit as PARTIAL, wait 10 minutes for the NCS to initialize fully. If the PARTIAL status does not change after full initialization, call Cisco TAC (1 800 553-247).

Step 2 After determining that the circuit is DISCOVERED, ensure that the signal source to the card reporting the alarm is working.

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

Step 3 If traffic is affected, complete the Delete a Circuit, on page 314 procedure.

Caution Deleting a circuit can affect existing traffic.

Step 4 Recreate the circuit with the correct circuit size. Refer to the Create Circuits and VT Tunnels chapter in the Configuration guide for detailed procedures to create circuits.

Step 5 If circuit deletion and re-creation does not clear the condition, verify that there is no problem stemming from the far-end OC-N card providing STS payload to the reporting card.

Step 6 If the condition does not clear, confirm the cross-connect between the OC-N card and the reporting card.

Step 7 If the condition does not clear, clean the far-end optical fiber according to site practice. If no site practice exists, complete the procedure in the Maintain the Node chapter of the Configuration guide.

Step 8 If the condition does not clear, complete the Physically Replace a Card, on page 313 procedure for the optical/electrical cards.

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

PEER-CERT-VERIFICATION-FAILED

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

Logical Object: OTN

The Peer Certificate Verification Failed alarm is raised when the verification of a peer certificate in the card fails.

Clear the PEER-CERT-VERIFICATION-FAILED Alarm

Procedure

This alarm is cleared when the verification of a peer certificate in the card is successful.

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

PEER-CSF

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

Logical Object: STM/OCN

The Peer Client Signal Fail alarm that is a secondary alarm raised on local OCN, OTU1, or SDI_3G_VIDEO ports when a remote Service-Affecting (SA) alarm causes an invalid data transmission. The alarm is raised locally on AR_MXP and AR_XP ports and does not indicate that a Service-Affecting (SA) failure has occured at the local site. Instead it indicates that an alarm such as LOS, LOS-P, LOF, OTU-AIS is caused by an event affecting the transmission capability of the remote port.

Clear the PEER-CSF Alarm

Procedure

Clear the Service-Affecting (SA) alarm at the remote data port.

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

PEER-NORESPONSE

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

Logical Object: EQPT

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.

Clear the PEER-NORESPONSE Alarm

Procedure

Step 1 Complete the Reset a Card in CTC, on page 310 procedure for the reporting card.

Step 2 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. Verify the LED appearance: A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

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

PMD-DEG

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

Logical Object: Trunk port (dir RX)

The PMD Degrade alarm is raised when the device experiences PMD in excess of 11ps for 40ME-MXP-C and 40-ME-TXP-C cards, 30ps for 40E-MXP-C and 40E-TXP-C cards, and 180ps for 100G-LC-C card.

Clear the PMD-DEG Alarm

Procedure

Switch the traffic on a lower PMD link.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

PMI

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

Logical objects: OCH, OMS, OTS

The Payload Missing Indication (PMI) condition is part of MSTP network-level alarm correlation. It is raised at the far end when OTS or OMS optical payload is missing due to an LOS, LOS-P, or OPWR-LFAIL alarm root cause. A single PMI condition is sent when each channel on the aggregated port is lost.

An LOS, LOS-P, or OPWR-LFAIL alarm on an MSTP circuit causes multiple alarms for each channel. The correlation simplifies troubleshooting by reporting a single alarm for multiple alarms having one root cause, then demoting the root alarms so that they are only visible in the Conditions window (with Not Reported [NR] severity.)

PMI clears when the optical channel is working on the aggregated or single-channel optical port.

Note Network-level alarm correlation is only supported for MSTP communication alarms. It is not supported for equipment alarms.

Clear the PMI Condition

Procedure

Clear the root-cause service-affecting alarm by using one of the following procedures, as appropriate:

- Clear the LOS (OTS) Alarm, on page 161 procedure
- Clear the LOS (TRUNK) Alarm, on page 163 procedure
- Clear the LOS-P (OCH) Alarm, on page 167 procedure
- Clear the LOS-P (AOTS, OMS, OTS) Alarm, on page 165 procedure
- Clear the LOS-P (TRUNK) Alarm, on page 170 procedure
- Clear the OPWR-LFAIL Alarm, on page 207 procedure

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

PORT-COMM-FAIL

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

Logical Object: DWDM_CLIENT, DWDM_TRUNK

The port module communication failure (PORT-COMM-FAIL) alarm is raised on the OTU2XP, GE_XP, GE_XPE, 10GE_XP, 10GE_XPE, 40G-MXP-C, 40E-MXP-C, 40ME-MXP-C, AR-MXP, and AR-XP line cards when there is a pluggable port module (PPM) communication failure. The PPM communication failure is caused due to physical damage or internal errors on the PPM.

Clear the PORT-COMM-FAIL Alarm

Procedure

To Clear the PORT-COMM-FAIL alarm, perform the following:

a) Soft reset the line card.
b) Delete PPM provisioning from the line card.
c) Re-provision the PPM on the line card.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into

http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

PORT-FAIL

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

Logical Object: OCH

The APC Port Failure alarm occurs when amplifier margins and VOA are saturated for a port, so APC cannot apply any control. For example, it is raised if APC attempts to set an OPT-BST, OPT-AMP-C, or OPT-AMP-17-C port gain higher than 20 dBm (the maximum setpoint) or its attenuation on Express VOA lower than 0 dBm (the minimum setpoint).

Clear the PORT-FAIL Alarm

Procedure

Step 1 If a maintenance operation such as fiber repair, adding a card, or replacing a card has just been performed on the optical network (whether at the node raising the PORT-FAIL alarm or at any other node), determine whether this operation has added extra loss. This can happen if the repair is imperfect or if a patchcord is dirty. To test for signal loss, refer to procedures in the Network Reference chapter of the Configuration guide.

Step 2 If there is loss added and fiber has been repaired or removed, first try cleaning the fiber by completing the procedures in the Maintain the Node chapter of the Configuration guide.

Step 3 If the alarm does not clear and fiber has been repaired, perform the repair again with new fiber if necessary. For fibering procedures, refer to the Turn Up a Node chapter in the Configuration guide. If the alarm does not clear, go to Step 4, on page 236.

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

Note Before disconnecting any optical amplifier card fiber for troubleshooting, ensure that the optical amplifier card is unplugged.

Step 4 If a maintenance operation has not been recently executed on the network, the alarm indicates that the network has consumed all of its allocated aging margins.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

PPR-BDI

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

Logical Objects: TRUNK

The Path Protection Regen -Backward Defect Indication (PPR-BDI) alarm occurs in OTU2_XP cards when the card is used as a regenerator in standard regen or enhanced FEC modes and Proactive Protection Regen is enabled. The alarm occurs when the downstream router triggers a PF-BDI signal.

Clear the PPR-BDI Condition

Procedure

To clear the PPR-BDI condition, clear the PPR-FDI and PPR-TRIG-EXCD alarm on the OTU2_XP card.

If the problem does not clear, see to the CRS documentation for more information.

PPR-FDI

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

Logical Objects: TRUNK

The Path Protection Regen-Forward Defect Indication (PPR-FDI) occurs in OTU2_XP cards as soon as the Bit Error Rate (BER) of the optical signal between the upstream router and the NCS node exceeds the trigger threshold value for the duration set as the trigger window. The PPR-FDI alarm is sent to the downstream router which in turn triggers the switch over to the backup path.

Clear the PPR-FDI Condition

Procedure

To clear the PPR-FDI condition, clear the PPR-TRIG-EXCD alarm on the upstream OTU2XP card.

PPR-MAINT

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

Logical Objects: TRUNK

The Path Protection Regen-Maintenance signal (PPR-MAINT) alarm occurs in OTU2_XP cards when the used as a regenerator (standard regen or enhanced FEC) and proactive protection regen is enabled. The alarm occurs when the port receives a maintenance signal from a router (CRS) interface.

PPR-TRIG-EXCD

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

Logical Objects: ETH

The Path Protection Regen-Trigger Crossed (PPR-TRIG-EXCD) alarm applies to OTU2_XP cards when the card is used as a regenerator in standard regen or enhanced FEC modes and Proactive Protection Regen is enabled. The alarm occurs when the pre-FEC BER of the incoming optical signal exceeds the trigger threshold value.

Clear the PPR-TRIG-EXCD Condition

Procedure

Step 1 Ensure that the fiber connector for the card is completely plugged in. For more information about fiber connections and card insertion, refer to the Turn Up a Node chapter in the Configuration guide.

Step 2 If the BER threshold is correct and at the expected level, use an optical power meter to measure the power level of the line to ensure it is within guidelines. For specific procedures to use the test set equipment, consult the manufacturer.

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

Step 4 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 Configuration guide.

Step 5 If the condition does not clear, verify that single-mode fiber is used.

Step 6 If the fiber is of the correct type, verify that a single-mode laser is used at the far-end node.

Step 7 Clean the fiber connectors at both ends according to site practice to avoid a signal degrade.

Step 8 Verify that a single-mode laser is used at the far end.

Step 9 If the problem does not clear, the transmitter at the other end of the optical line could be failing and require replacement. Refer to the “Physical Card Reseating, Resetting, and Replacement” section .

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

PRBS-ENABLED

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

Logical Objects: OCH

The Pseudo−Random Bit Sequence (PRBS) Enable alarm is raised when the PRBS is enabled on an interface.

Clear the PRBS-ENABLED Alarm

Procedure

This alarm is cleared automatically when the PRBS is disabled on an interface.

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

PROT-SOFT-VERIF-FAIL

On the active control card, the alarm severity is Major (MJ) and Service Affecting (SA).

On the standby control card, the alarm severity is Minor (MN) and Non-Service affecting (NSA).

Logical Object: EQPT

The Protect Volume Software Signature Verification Failed (PROT-SOFT-VERIF-FAIL) alarm occurs under the following conditions:

- The software present on the protect volume of control card is tampered with or the software present on the system did not originate from Cisco.
- Problem present in the software is stored in the protect volume of the control card.

Clear the PROT-SOFT-VERIF-FAIL Alarm

Procedure

To clear the PROT-SOFT-VERIF-FAIL alarm, download the software on the standby partition or the standby code volume on the protect flash.

If the troubleshooting procedure does not clear the alarm, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html or call the Cisco Technical Assistance Center (1 800 553-2447) to report the problem.

PROTNA

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

Logical Object: EQPT

The Protection Unit Not Available (PROTNA) alarm is raised when a standby control card is not available.

Clear the PROTNA Alarm

Procedure

Ensure that the standby control card is installed and provisioned in the chassis.

PROV-MISMATCH

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

Logical Object: EQPT and control cards

The Provisioning Mismatch alarm is raised against a PPM connector under one of the following circumstances:

- The physical PPM range or wavelength does not match the provisioned value. PPMs have static wavelength values which must match the wavelengths provisioned for the card in the case of non-DWDM PPMs.
- The PPM reach (loss) value does not meet the reach value needed for the card.
- The reach of the inserted PPM does not match the physical PPM.

The Provisioning Mismatch (PROV-MISMATCH) alarm is raised against a TNC/TNCS/TNCE/TNCS-O card under one of the following circumstances:

- The card mode is set to TNC (default value) with OC3/GE ports provisioned and a TNCS-O card is plugged.
- The card mode is set to TNCO and the plugged card is a TNC/TNCE/TNCS.

The Provisioning Mismatch (PROV-MISMATCH) alarm is raised when a TNCS-O card is replaced by TNCS card. The alarm is also raised when TNCS card is replaced by a TNCS-O card with OC3/GE ports provisioned.

Note When the TNCS-2 card is replacing the TNC card pre-provisioned with OC3 payload on a chassis, the PROV-MISMATCH/MEA alarm is raised. Delete the pre-provisioning on the TNCS-2 card to proceed.

Clear the PROV-MISMATCH Alarm

To clear the alarm when the physical PPM range or wavelength does not match the provisioned value, perform the following steps:

Procedure

Step 1 To clear the PROV-MISMATCH alarm on MXP_2.5G_10E, MXP_2.5G_10E_C, MXP_2.5G_10E_L, MXP_2.5G_10G, MXP_MR_2.5G, MXPP_MR_2.5G, TXP_MR_2.5G, TXP_MR_10E, TXP_MR_10E_C, TXP_MR_10E_L, TXPP_MR_2.5G, GE_XP, 10GE_XP, ADM-10G, OTU2_XP, MR-MXP, WSE, 10x10G-LC,

100G-LC-C, 100G-CK-LC, 200G-CK-LC, 100GS-CK-LC, 400G-XP, CFP-LC, AR-XP, AR-MXP, AR-XPE, 40G-MXP, 40G-TXP, 40E-MXP, and 40E-TXP cards, perform the following steps:

a) Determine what the PPM wavelength range should be by viewing the frequency provisioned for the card:

i. In node view (single-shelf mode) or shelf view (multishelf mode), double-click the card to open the card view.

ii. Click the **Maintenance** > **Info** tabs.

iii. Record the value shown in the Value column.

b) Remove the incorrect PPM connector:

i. Unplug the PPM connector and fiber from the reporting card.

ii. If the PPM connector has a latch securing the fiber cable, pull the latch upward to release the cable.

iii. Pull the fiber cable straight out of the connector.

c) Replace the unit with the correct PPM connector:

i. Plug the fiber into a Cisco-supported PPM connector. For more information about supported PPMs, refer to the Installing the GBIC, SFP, SFP+, and XFP Optical Modules in Cisco ONS PlatformsInstalling the GBIC, SFP, SFP+, QSFP, XFP, CXP, CFP and CPAK Optical Modules in Cisco NCS Platforms document.

ii. If the new PPM connector has a latch, close the latch over the cable to secure it.

iii. Plug the cabled PPM connector into the card port until it clicks.

Step 2 To clear the PROV-MISMATCH alarm on GE_XP or 10GE_XP cards, remove Double Add and Translate Add selective modes, CVLAN Ingress CoS, or MAC address learning on SVLAN configuration.

Step 3 To clear the PROV-MISMATCH alarm on TNC/TNCS/TNCE/TNCS-O cards, do the steps that follow:

a) To clear the alarm when the card mode is TNC with OC3/GE ports provisioned and the plugged card is a TNCS-O, do the steps that follow:

1. Login to CTC.
2. In node view (single-shelf mode) or shelf view (multishelf view), double-click the TNCS-O card where you want to clear the alarm.
3. Delete the provisioned OC3/GE ports.
4. Click the **Provisioning** > **Card** > tabs.
5. Set Mode to TNCS-O.
6. Click **Apply**.

b) To clear the alarm when the card mode is TNCO and the plugged card is a TNC/TNCS/TNCE, do the steps that follow:

1. Login to CTC.
2. In node view (single-shelf mode) or shelf view (multishelf view), double-click the TNC/TNCS/TNCE card where you want to clear the alarm.
3. Open TNC/TNCS/TNCE card panel view.
4. Click the **Provisioning** > **Card** > tabs.

5. Set Mode to TNC.
6. Click **Apply**.

Step 4 To clear the PROV-MISMATCH alarm on TNCS card (the alarm that occurs when you replace a TNCS-O card with a TNCS card), do the steps that follow:

a) Remove the TNCS-O card.
b) Delete the TNCS-O card, refer to DLP-G351 Deleting a Card in CTC .
c) Insert the TNCS card.

Step 5 To clear the PROV-MISMATCH alarm on TNCS-O card (the alarm that occurs when you replace a TNCS card with a TNCS-O card), do the steps that follow:

a) Remove the TNCS card.
b) Delete the TNCS card, refer to DLP-G351 Deleting a Card in CTC .
c) Insert the TNCS-O card.

Note On MR-MXP and 400G-XP-LC cards, when the reach distance of one of the QSFP 10G lanes or ports is configured to **Autoprovision** or the correct reach, the PROV-MISMATCH alarm clears on the QSFP port. The alarm clears irrespective of the reach distances configured on the remaining QSFP 10G lanes or ports.

If the troubleshooting procedure does not clear the alarm, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html or call the Cisco Technical Assistance Center (1 800 553-2447) to report the problem.

PTIM

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

Logical Object: TRUNK, EQPT

The Payload Type Identifier Mismatch (PTIM) alarm occurs when there is a mismatch between the way the ITU-T G.709 encapsulation option is configured on the line card at each end of the optical span.

Clear the PTIM Alarm

Procedure

Step 1 In node view (single-shelf mode) or shelf view (multishelf mode), double-click the alarmed line card to open the card view.

Step 2 Click the **Provisioning** > **OTN** > **OTN Lines** tabs.

Step 3 Ensure that the G.709 OTN check box is checked. If not, check it and click **Apply**.

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

PWR-CON-LMT

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

Logical Object: EQPT

The Power Consumption Limit Has Crossed (PWR-CON-LMT) condition is raised at the shelf level when the total power consumption of the shelf equals or exceeds the maximum power. This alarm is applicable for all the following AC and DC power supply modules.

- NCS2006-DC20
- NCS2006-AC
- NCS2006-DC
- NCS2006-DC40
- 15454-M6-DC20
- 15454-M6-AC2
- 15454-M6-AC
- 15454-M6-DC
- 15454-M6-DC40

Clear the PWR-CON-LMT Alarm

Procedure

Step 1 Remove the card that caused the alarm from the shelf.

Step 2 Remove the card provisioning through the user interface.

Step 3 Place the card in another chassis which supports the required power.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

PWR-FAIL-A

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

Logical 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.

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

Procedure

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

- If the reporting card is an active traffic line port in a 1+1 protection group, 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, on page 306 section for commonly used traffic-switching procedures.

Step 2 If the alarm does not clear, complete the Remove and Reinsert (Reseat) Any Card , on page 313 procedure.

Step 3 If the alarm does not clear, complete the Physically Replace a Card, on page 313 procedure for the reporting card.

Step 4 If the single card replacement does not clear the alarm, or if multiple cards report the alarm, verify the office power. Refer to the Install the Shelf and Common Control Cards chapter in the Configuration guide for procedures.

Step 5 If the alarm does not clear, reseat the power cable connection to the connector.

Step 6 If the alarm does not clear, physically replace the power cable connection to the connector.

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

PWR-FAIL-B

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

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.

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

Procedure

Complete the Clear the PWR-FAIL-A Alarm, on page 244 procedure.

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

PWR-FAIL-RET-A

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

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.

Clear the PWR-FAIL-RET-A Alarm

Procedure

Complete the Clear the PWR-FAIL-A Alarm, on page 244 procedure.

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

PWR-FAIL-RET-B

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

Logical Object: EQPT

The Equipment Power Failure at Connector B alarm occurs when there is no power supplied to the backup power connector on the shelf. This alarm occurs on the electrical interface assemblies (EIA) or the control card.

Clear the PWR-FAIL-RET-B Alarm

Procedure

Complete the Clear the PWR-FAIL-A Alarm, on page 244 procedure.

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

PWR-PROT-ON

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

SONET Logical Objects: OTS

The Raman Power Protection On alarm occurs when the Raman amplifier is used on fiber span that is too short for Raman power.

Clear the PWR-PROT-ON Alarm

Procedure

Step 1 To clear the alarm, check if the Raman amplifier is connected to the wrong span. If it is, check the patch cords setup and fix it.

Step 2 Alternatively, review the network configuration to see if the Raman amplifier has been wrongly used. If it is, remove it.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into

http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

RAMAN-CALIBRATION-FAILED

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

Logical Object: OTS

The RAMAN-CALIBRATION-FAILED alarm is raised on the EDRA-1-xx, EDRA-2-xx, and RAMAN-CTP cards when automatic Raman pump calibration is failed and will not run again. The alarm indicates insufficient Raman Amplification by customer fibre. The Raman calibration can also fail due to the setup issues that include:

- Wrong patch-cords or cabling
- Incorrect ANS
- Missing communication channel between nodes.

Clear the RAMAN-CALIBRATION-FAILED Alarm

Procedure

Step 1 Use optical time domain reflectometer (OTDR) to identity any excess loss between the Raman card LINE-RX port and the customer fibre. After the inspection, a new Raman Calibration is triggered and if the physical problem is fixed, the alarm will clear.

Step 2 If the alarm is caused by a set-up problem, re-verify all node installation steps and manually trigger a Raman Calibration.

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

RAMAN-CALIBRATION-PENDING

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

Logical Object: OTS

The RAMAN-CALIBRATION-PENDING condition is raised on the EDRA-1-xx, EDRA-2-xx, and RAMAN-CTP cards when automatic Raman pump calibration is scheduled to run repeatedly after the first installation or fiber cut. The condition is cleared when the Raman pump calibration succeeds or fails for 30 attempts.

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

RAMAN-CALIBRATION-RUNNING

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

Logical Object: OTS

The RAMAN-CALIBRATION-RUNNING alarm is raised on the EDRA-1-xx, EDRA-2-xx, and RAMAN-CTP cards when the Raman pump calibration is running. The alarm is cleared when the Raman pump calibration succeeds or fails.

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

RAMAN-G-NOT-REACHED

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

Logical Object: OTS

The RAMAN-G-NOT-REACHED alarm is raised on the OPT-RAMP-C cards when the Raman gain value is lower than the ANS target. The alarm also occurs after a cut restoration procedure fails to restore the expected Raman gain set point.

Clear the RAMAN-G-NOT-REACHED Alarm

Procedure

Do the steps that follow to clear the alarm on the OPT-RAMP-C card:

a) Repair the span.
b) Clean the fiber connectors at both ends according to site practice.
c) Check for patch panel connections and fiber splices, if any.
d) Reconnect the fibers according to site practice.
e) Perform the Raman Wizard day-0 procedure to recalibrate the Raman gain setpoint.

REMOTE-FAULT

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

SONET Logical Objects: ETH

- when there is a loss of signal synchronization on the port.

- when a remote fault character sequence is received in the incoming MAC stream as defined in IEEE 802.3ae, 10 Gigabit Ethernet fault signaling scheme.

Clear the REMOTE-FAULT Alarm

Procedure

Step 1 Verify and resolve the client port fault and remote fault errors on the remote or upstream node.

Step 2 Verify and resolve loss of signal synchronization error on the remote or upstream node.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

REP-LINK-FLAPPING

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

Logical Objects: ETH

The REP-LINK-FLAPPING alarm is raised on GE_XP and 10GE_XP cards when a link flap is detected, and is raised against the REP ports (and switches) facing the link flap.

Clear the REP-LINK-FLAPPING

Procedure

The alarm is cleared when the link flapping is over.

REP-NEIHB-ADJ-FAIL

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

Logical Objects: ETH

The REP-NEIHB-ADJ-FAIL (REP-NEIHB-ADJ-FAIL) alarm is raised on GE_XP and 10GE_XP cards when a link flap is detected, and is raised against the REP ports (and switches) facing the link flapping. The alarm is raised till adjacency cannot be established. The alarm is raised in the following scenarios:

- The link between the two REP peer ports is down.
- The switch within the REP segment is down.

The alarm is raised against the REP port facing the immediate loss of adjacency. The alarm is raised on the REP peer port and two peer REP ports impacted by the loss of adjacency based on the two scenarios listed.

Note This alarm does not apply to EdgeNN ports.

Clear the REP-NEIHB-ADJ-FAIL Alarm

Procedure

The alarm is cleared as soon as adjacency is established.

REP-SEGMENT-FAULT

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

Logical Objects: ETH, GE

The REP-SEGMENT-FAULT alarm is raised when a segment failure is detected in the following possible scenarios:

- The link between two REP peer ports is down.
- The switch within the REP segment is down.
- REP protocol failure is present on the switch within the REP segment.

The alarm is raised at all REP ports across all switches participating in the impacted REP segment.

Clear the REP-SEGMENT-FAULT Condition

Procedure

The REP-SEGMENT-FAULT alarm is cleared once the segment is complete.

REROUTE-IN-PROG

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

Logical Objects: OTS

The Reroute in Progress alarm is raised when a control plane service undergoes a reroute operation.

Clear the REROUTE-IN-PROG Alarm

Procedure

This alarm is cleared automatically when the reroute operation is complete.

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

REVERT-IN-PROG

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

Logical Objects: OTS

The Revert in Progress alarm is raised when a control plane service undergoes a revert operation.

Clear the REVERT-IN-PROG Alarm

Procedure

This alarm is cleared automatically when the revert operation is complete.

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

RFI

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

Logical Object: TRUNK

The Remote Failure Indication condition is raised against . The MXP or TXP cards only raise AIS (or remote failure indication [RFI]) when they are in line or section termination mode, that is, when the MXP or TXP cards in line termination mode or section termination mode have improperly terminated overhead bytes.

Clear the RFI Condition

Procedure

Complete the Delete a Circuit, on page 314 procedure and then recreate the circuit.

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

RFI-L

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

Logical Object: TRUNK

A RFI Line condition occurs when the system 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

Procedure

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

Step 2 Identify and clear any alarms, particularly the LOS (OCN) alarm.

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

RFI-P

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

Logical Object: STSMON, STSTRM

The RFI Path condition occurs when the system 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

Procedure

Step 1 Verify that the ports are enabled and in service (IS-NR) on the reporting system:

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

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

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

c) Click the **Provisioning** > **Line** tabs.
d) Verify that the Admin State column lists the port as IS.
e) If the Admin State column lists the port as OOS,MT or OOS,DSBLD , click the column and choose **IS**. Click **Apply**.

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

Step 2 To find the path and node failure, verify the integrity of the SONET STS circuit path at each of the intermediate SONET nodes.

Step 3 Clear alarms in the node with the failure, especially the UNEQ-P , on page 290 alarm.

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

RLS

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

Logical Object: OTS

Clear the RLS Condition

ROUTE-OVERFLOW

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

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 , CTM, Telnet, Ping, and so on.

Clear the ROUTE-OVERFLOW Condition

Procedure

Reconfigure the OSPF network to less than 700 routes.

RS-EOC

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

Logical Object: TRUNK

The SONET Data Communications Channel (DCC) Termination Failure alarm occurs when the system loses its data communications channel. Although this alarm is primarily SONET, it can apply to DWDM. For example, the OSCM card can raise this alarm on its STM-1 section overhead.

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

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

Warning **Class 1M laser radiation when open. Do not view directly with optical instruments.** Statement 1053

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

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

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

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

Clear the RS-EOC Alarm

Procedure

Step 1 If the alarm does not clear on the reporting node, verify the physical connections between the cards and that the fiber-optic cables are configured to carry RS-DCC traffic. If they are not, correct them.

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

If the physical connections are correct and configured to carry DCC traffic, ensure that both ends of the fiber span have unlocked ports. Verify that the ACT/SBY LED on each card is green.

Step 2 When the LEDs on the cards are correctly illuminated, complete the Verify or Create Node RS-DCC Terminations, on page 316 procedure to verify that the DCC is provisioned for the ports at both ends of the fiber span.

Step 3 Repeat Step 2, on page 255 procedure at the adjacent nodes.

Step 4 For all nodes, if the card is in service, use an optical test set to determine whether signal failures are present on fiber terminations. For specific procedures to use the test set equipment, consult the manufacturer.

Step 5 If no signal failures exist on terminations, measure power levels to verify that the budget loss is within the parameters of the receiver.

Step 6 If budget loss is within parameters, ensure that fiber connectors are securely fastened and properly terminated.

Step 7 Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.

Resetting the active control card switches control to the standby control card. If the alarm clears when the node switches to the standby control card, the user can assume that the previously active card is the cause of the alarm.

Step 8 If the control card reset does not clear the alarm, delete the problematic RS-DCC termination by completing the following steps:

a) From card view, click **View** > **Go to Previous View** if you have not already done so.
b) Click the **Provisioning** > **Comm Channels** > **RS-DCC** tabs.
c) Highlight the problematic DCC termination.
d) Click **Delete**.
e) Click **Yes** in the Confirmation Dialog box.

Step 9 Recreate the RS-DCC termination. Refer to the Turn Up Network chapter in the Configuration guide for procedures.

Step 10 Verify that both ends of the DCC have been recreated at the optical ports.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

If the Technical Support technician tells you to reseat the card, complete the Remove and Reinsert (Reseat) Any Card , on page 313 procedure. If the Technical Support technician tells you to remove the card and reinstall a new one, follow the Physically Replace a Card, on page 313 procedure.

RS-TIM

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: STMN

The Regenerator Section TIM alarm occurs when the expected J0 path trace string does not match 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. Follow the procedure below to clear either instance.

Clear the RS-TIM Alarm

Procedure

Complete the Clear the TIM Alarm, on page 282 procedure for the J0 byte.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

SBYTCC-NEINTCLK

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SDH Logical Object: EQPT

The "Standby TCC - NE Clock Is Internal Clock" condition occurs when the standby TCC NE clock switches to the internal oscillator (clock). This alarm occurs when NE is forced to use internal clock or if all the external clocks fails so that the NE automatically switches to internal clock. This also occurs when the sandby TCC fails and starts using internal NE clock instead of tracking the provisioned external clock.

Clear the SBYTCC-NEINTCLK Alarm

Procedure

Step 1 Clear the following alarms that relate to timing:

- FRNGSYNC , on page 99
- FSTSYNC , on page 100
- LOF (BITS) , on page 150

- LOS (BITS) , on page 158
- HLDOVRSYNC , on page 116
- MANSWTOINT, on page 182
- MANSWTOPRI , on page 182
- MANSWTOSEC , on page 182
- MANSWTOTHIRD , on page 182
- SWTOPRI , on page 276
- SWTOSEC , on page 276
- SWTOTHIRD , on page 277
- SYNC-FREQ , on page 277
- SYNCPRI , on page 278
- SYNCSEC , on page 279
- SYSBOOT , on page 280

Step 2 Reestablish a primary and secondary timing source according to local site practice. If none exists, refer to the Change Node Settings chapter in the Configuration guide.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

SD (TRUNK)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: TRUNK

A Signal Degrade (SD) condition on the trunk occurs when the quality of an optical signal to the card has BER on the incoming optical line that passes the signal degrade threshold. The alarm applies to the card ports and the trunk carrying optical or electrical signals to the card.

Signal degrade is defined by Telcordia as a soft failure condition. SD and SF both monitor the incoming BER and are similar, but SD is triggered at a lower BER than SF. The BER threshold on the system is user-provisionable and has a range for SD from 1E9 dBm to 1E5 dBm.

Clear the SD (TRUNK) Condition

Procedure

Step 1 Ensure that the fiber connector for the card is completely plugged in.

Step 2 If the BER threshold is correct and at the expected level, use an optical test set to measure the power level of the line to ensure it is within guidelines. For specific procedures to use the test set equipment, consult the manufacturer.

Step 3 If the optical power level is good, verify that optical receive levels are within the acceptable range.

Step 4 If receive levels are good, clean the fibers at both ends according to site practice.

Step 5 If the condition does not clear, verify that single-mode fiber is used.

Step 6 If the fiber is of the correct type, verify that a single-mode laser is used at the far-end node.

Step 7 Clean the fiber connectors at both ends for a signal degrade according to site practice.

Step 8 Verify that a single-mode laser is used at the far end.

Step 9 If the problem does not clear, the transmitter at the other end of the optical line could be failing and require replacement. Refer to the Physical Card Reseating, Resetting, and Replacement, on page 312 section.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

SD-L

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: STMN

An SD Line condition is similar to the SD (TRUNK) , on page 257 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 and LOS alarms.

Clear the SD-L Condition

Procedure

Complete the Clear the SD (TRUNK) Condition, on page 257 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

SD-L (TRUNK)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: TRUNK

A Signal Degrade (SD) condition on the trunk occurs when the quality of an optical signal to the MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, TXP_MR_10E, TXP_MR_10E_C, TXP_MR_10E_L, TXPP_MR_2.5G, GE-XP, 10GE-XP, and ADM-10G card has bit error rate (BER) on the incoming optical line that passes the signal degrade threshold. The alarm applies to the card ports and the trunk carrying optical or electrical signals to the card.

Clear the SD-L (TRUNK) Condition

Procedure

Complete the Clear the SD (TRUNK) Condition, on page 257 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

SD-P

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: STSMON, STSTRM

An SD Path condition is similar to the SD (TRUNK) , on page 257 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

Procedure

Complete the Clear the SD (TRUNK) Condition, on page 257 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

SDBER-EXCEED-HO

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: VCMON-HP, VCTRM-HP

The Signal Degrade Threshold Exceeded for High Order condition indicates that the signal degrade BER threshold has been exceeded for a high-order (VC-4) path on optical (traffic) cards. SDBER-EXCEED-HO occurs when the signal BER falls within the degrade threshold (typically 1E-7 dBm) set on the node.

Warning **Class 1 laser product.** Statement 1008

Warning **Class 1M laser radiation when open. Do not view directly with optical instruments.** Statement 1053

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

Clear the SDBER-EXCEED-HO Condition

Procedure

Step 1 Determine the BER threshold. Complete the Clear an MXP, TXP, GE-XP, 10GE-XP, and ADM-10G Card Loopback Circuit, on page 315 procedure.

Step 2 If adjustment is acceptable in site practices, adjust the threshold.

Using an optical test set, measure the input power level of the line and ensure that the level is within the guidelines. For specific procedures to use the test set equipment, consult the manufacturer.

Step 3 Verify the input fiber cable connections to the reporting card.

Step 4 Clean the input fiber cable ends according to site practice. If no site practice exists, complete the procedure in the Maintain the Node chapter of the Configuration guide.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

SEQ-MISMATCH-COUNT

Default Severity: Minor (MN)

Logical Object: TRUNK (OTU)

The Sequence Mismatch Count alarm is raised on the OTU trunk port in the WSE card. This alarm is a Threshold Crossing Alert (TCA). This alarm is raised when the sequence mismatch count crosses the provisioned threshold. The TCA is present for a duration of 15 minutes.

Clearing the SEQ-MISMATCH-COUNT Alarm

The alarm is cleared when the polling starts for the following 15 minutes interval, and the sequence mismatch count for that interval is within the threshold value.

If the troubleshooting procedure does not clear the alarm, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html or call the Cisco Technical Assistance Center (1 800 553-2447) to report the problem.

SF (TRUNK)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: TRUNK

A Signal Fail (SF) condition for the trunk occurs when the quality of an optical signal to the TXP or MXP card has BER on the incoming optical line that passes the signal fail threshold. The alarm applies to the card ports and the trunk carrying optical or electrical signals to the card.

Signal fail is defined by Telcordia as a hard failure condition. SF monitors the incoming BER and is triggered when the BER surpasses the default range.

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 (TRUNK) Condition

Procedure

Complete the Clear the SD (TRUNK) Condition, on page 257 procedure.

Caution Always use the supplied electrostatic discharge wristband when working with a powered NCS system. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

SF-L

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: EQPT

An SF Line condition is similar to the SD (TRUNK) , on page 257 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 and LOS alarms.

Clear the SF-L Condition

Procedure

Complete the Clear the SD (TRUNK) Condition, on page 257 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

SF-L (TRUNK)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: TRUNK

A Signal Fail (SF) condition is raised on the trunk when the quality of an incoming optical signal to the MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, TXP_MR_10E, TXP_MR_10E_C, TXP_MR_10E_L,

TXPP_MR_2.5G, or ADM-10G card has high BER due to bent or degraded fiber connected to the trunk, on the incoming optical line that passes the signal fail threshold. The alarm applies to the card ports and the trunk carrying optical or electrical signals to the card.

The SF-L condition monitors the incoming BER and is triggered when the BER surpasses the default range.

Clear the SF-L (TRUNK) Condition

Procedure

Complete the Clear the SD (TRUNK) Condition, on page 257 procedure.

Caution Always use the supplied electrostatic discharge wristband when working with a powered NCS system. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly. For detailed instructions on how to wear the ESD wristband, refer to the Electrostatic Discharge and Grounding Guide.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

SF-P

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: STSMON, STSTRM

An SF Path condition is similar to the SF (TRUNK) , on page 261 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

Procedure

Complete the Clear the SF (TRUNK) Condition, on page 262 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

SFTWDOWN

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: EQPT

A Software Download in Progress alarm occurs when the control card is downloading or transferring software.

If the active and standby control cards have the same versions of software, it takes approximately three minutes for software to be updated on a standby control card.

If the active and standby control cards 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 control card 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 condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

Note SFTWDOWN is an informational alarm.

SFTWDOWN-FAIL

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Software Download Failed (SFTDOWN-FAIL) alarm occurs when the software package download fails on the control card of the system in a multishelf configuration.

An incorrect input that points to the wrong place or file, network issues, or a bad (corrupt) software package can cause this failure. If the software package is corrupt, contact the Cisco Technical Assistance Center (TAC) (1 800 553-2447) for assistance.

Clear the SFTWDOWN-FAIL Alarm

Procedure

Step 1 Verify the network connectivity by pinging the system that is reporting the alarm .

Step 2 Reboot the working (active) control card.

Step 3 Download the software package on the working (active) control card.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

SHELF-COMM-FAIL

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: SHELF

The Shelf Communication Failure alarm applies to optical equipment when an NC shelf is unable to communicate with an SS shelf. Typically this occurs when there is a fiber disconnection. But the alarm can also occur if an SS shelf is resetting.

Clear the SHELF-COMM-FAIL Alarm

Procedure

Step 1 Determine whether an SS shelf controller is being reset. If it is being reset, you must wait for the shelf to reset for this alarm to clear.

Step 2 If the alarm does not clear or if no shelf is being reset, perform the following:

a) NCS 2006 as NC shelf—Check the cabling between the MSM ports of NC shelf and SS shelf controller. Correct it if necessary. Check if the External Connection Unit in the NC and SS shelf is installed correctly.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

SH-IL-VAR-DEG-HIGH

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: OTS

The Switch Insertion Loss Variation Degrade High alarm occurs as the OSC-CSM card optical switch ages and slowly increases its insertion loss. This alarm indicates that the insertion loss has crossed the high degrade threshold. The card must eventually be replaced.

Clear the SH-IL-VAR-DEG-HIGH Alarm

Procedure

For the alarmed card, complete the Physically Replace a Card, on page 313 procedure as appropriate.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

SH-IL-VAR-DEG-LOW

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: OTS

The Switch Insertion Loss Variation Degrade Low alarm occurs as the OSC-CSM card optical switch ages and slowly decreases its insertion loss. This alarm indicates that the insertion loss has crossed the low degrade threshold. The card must eventually be replaced.

Clear the SH-IL-VAR-DEG-LOW Alarm

Procedure

For the alarmed card, complete the Physically Replace a Card, on page 313 procedure as appropriate.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

SHUTTER-OPEN

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: OTS

The SHUTTER-OPEN condition occurs if an OSC-CSM card laser shutter remains open after the LOS (OTS), on page 161 alarm is detected. A laser shutter remains open if an optical safety issue is present and closes when the OSC-CSM card LINE-RX port receives OSC power for three consecutive seconds.

Clear the SHUTTER-OPEN Condition

Procedure

Step 1 Complete the Clear the LOS (OTS) Alarm, on page 161 procedure.

Step 2 If the SHUTTER-OPEN condition still does not clear, it indicates that the unit shutter is not working properly. Complete the Physically Replace a Card, on page 313 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

SIGLOSS

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Objects: FC, GE, ISC, TRUNK

The Signal Loss on Data Interface alarm is raised on MXP cards when there is a loss of signal. (Loss of Gigabit Ethernet client signal results in a CARLOSS [GE], 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

Procedure

Step 1 Ensure that the port connection at the near end of the SONET or SDH (ETSI) link is operational.

Step 2 Verify fiber continuity to the port. To verify fiber continuity, follow site practices.

Step 3 Check the physical port LED on the card. The port LED looks clear (that is, not lit green) if the link is not connected.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

SNTP-HOST

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: NE

The Simple Network Timing Protocol (SNTP) Host Failure alarm indicates that an NCS system serving as an IP proxy for the other NCS system 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 NCS system proxy node is experiencing problems, or the NCS system proxy node itself is not functioning properly.

Clear the SNTP-HOST Alarm

Procedure

Step 1 Ping the SNTP host from a workstation in the same subnet to ensure that communication is possible within the subnet.

Step 2 If the ping fails, contact the network administrator who manages the IP network that supplies the SNTP information to the proxy and determine whether the network is experiencing problems, which could affect the SNTP server/router connecting to the proxy system.

SOFT-VERIF-FAIL

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: EQPT

The Software Signature Verification Failed (SOFT-VERIF-FAIL) alarm occurs under the following conditions:

- The software running on any line card in the system is tampered with or the software running on the system did not originate from Cisco.
- Problem present in the software stored in the line cards.

Clear the SOFT-VERIF-FAIL Alarm

Procedure

To clear the alarm, log into the Technical Support Website at http://www.cisco.com/cisco/web/support/index.html for more information or call Cisco TAC (1 800 553-2447).

SPANLEN-OUT-OF-RANGE

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: OTS

The SPANLEN-OUT-OF-RANGE alarm is raised when span loss measured is higher than the maximum expected span loss (or lower than the minimum expected span loss).

The control card automatically measures span loss every hour, or it calculates it when you perform the Calculate Span Loss operation.

Clear the SPANLEN-OUT-OF-RANGE Alarm

Procedure

Step 1 Determine the maximum and minimum expected span loss values

a) Log into the SVO web interface.
b) Click the hamburger icon at the top-left of the page, and select **Node Configuration**.
c) Click the **Optical Configuration** > **Span Loss** tabs.
d) Check the maximum and minimum expected span loss values.

Step 2 Determine whether the measured span length falls between these two values.

Step 3 If the value falls outside this range, check the following factors in the fibering:

- Clearance
- Integrity
- Connection

Step 4 Determine whether any site variations are present which conflict with the design and correct them.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

SPAN-NOT-MEASURED

SPAN-NOT-MEASURED is a transient condition.

SQUELCHED

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: 2R, ESCON, FC, GE, ISC, OCN/STMN, TRUNK

The Client Signal Squelched condition is raised by a card 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 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 a SIGLOSS, Ethernet CARLOSS, LOS, or LOS (TRUNK) alarm. In some transparent modes, the client is squelched if the trunk detects an AIS condition or a TIM alarm.
- The client will squelch if the upstream client receive (on the card at the other end of the DWDM span) experiences CARLOSS, SIGLOSS, or LOS.

The local client raises a SQUELCHED condition if the local trunk raises one of the following alarms:

-
-
-
-
-
-
-
- LOF (OCN/STMN) alarm
- LOS (OCN/STMN) alarm
-
-

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 previously listed
- Local trunk alarms, as previously listed
- Remote (upstream) client receive alarms, as previously listed

Note If you see a SQUELCHED condition on the trunk, this can only be caused by a transponder (TXP) card.

Clear the SQUELCHED Condition

Procedure

Step 1 If the object is reported against any object besides ESCON, determine whether the remote node and local node reports and LOF or the LOS alarm (for the client trunk, as listed here). If it does, turn to the relevant section in this chapter and complete the troubleshooting procedure.

Step 2 If no LOF or LOS is reported, determine whether any other listed remote node or local node conditions as listed here have occurred. If so, turn to the relevant section of this chapter and complete the troubleshooting procedure.

Step 3 If none of these alarms is reported, determine whether the local port reporting the SQUELCHED condition is in loopback. If it is in loopback, complete the following steps:

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

SSM-DUS

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The Synchronization Status (SSM) Message Quality Changed to Do Not Use (DUS) condition occurs on MXP trunk ports 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)

Logical Object: TRUNK

The SSM Failed alarm occurs on MXP trunk ports when the synchronization status messaging received by the system fails. The problem is external to the NCS system. This alarm indicates that although the NCS system is set up to receive SSM, the timing source is not delivering valid SSM messages.

Clear the SSM-FAIL Alarm

Procedure

Step 1 Verify that SSM is enabled on the external timing source.

Step 2 If timing is enabled, use an optical test set to determine that the external timing source is delivering SSM. For specific procedures to use the test set equipment, consult the manufacturer.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

SSM-LNC

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

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)

Logical Object: TRUNK

The SSM Off condition applies to references used for timing related to the MXP trunk ports. 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

Procedure

Complete the Clear the SSM-FAIL Alarm, on page 271 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

SSM-PRC

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The SSM Primary Reference Clock (PRC) Traceable condition occurs when the SONET transmission level for MXP trunk ports 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)

Logical Object: TRUNK

The SSM Primary Reference Source (PRS) Traceable condition occurs when the SSM transmission level for MXP trunk ports is 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)

Logical Object: TRUNK

The SSM Reserved (RES) For Network Synchronization Use condition occurs when the synchronization message quality level for MXP trunk ports is RES.

Note SSM-RES is an informational condition and does not require troubleshooting.

SSM-SMC

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The SSM SONET Minimum Clock (SMC) Traceable condition occurs when the synchronization message quality level for MXP trunk ports is 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)

Logical Object: TRUNK

The SSM Stratum 2 (ST2) Traceable condition occurs when the synchronization message quality level for MXP trunk ports is ST2.

Note SSM-ST2 is an informational condition and does not require troubleshooting.

SSM-ST3

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The SSM Stratum 3 (ST3) Traceable condition occurs when the synchronization message quality level for MXP trunk ports is ST3.

Note SSM-ST3 is an informational condition and does not require troubleshooting.

SSM-ST3E

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The SSM Stratum 3E (ST3E) Traceable condition indicates that the synchronization message quality level for MXP trunk ports is ST3E. 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)

Logical Object: TRUNK

The SSM Stratum 4 (ST4) Traceable condition occurs when the synchronization message quality level is ST4 for MXP trunk ports. 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)

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 NCS system has SSM support enabled (MXP trunk ports).

SSM-STU can also occur if the timing source is sending out SSM messages but SSM is not enabled on the NCS system.

Clear the SSM-STU Condition

Procedure

Step 1 In node view (single-shelf mode) or shelf view (multishelf mode), click the **Provisioning** > **Timing** > **BITS Facilities** tabs.

Step 2 Complete one of the following depending upon the status of the Sync Messaging Enabled check box:

- If the **Sync. Messaging Enabled** check box for the BITS source is checked, uncheck the box.
- If the **Sync. Messaging Enabled** check box for the BITS source is not checked, check the box.

Step 3 Click **Apply**.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

SSM-TNC

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The SSM Transit Node Clock (TNC) Traceable condition occurs when the synchronization message quality level is TNC for MXP trunk ports.

Note SSM-TNC is an informational condition and does not require troubleshooting.

SW-MISMATCH

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Software Mismatch condition occurs during software upgrade when there is a mismatch between software versions.

Clear the SW-MISMATCH Condition

Procedure

Complete the procedure for the errored card.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

SWTOPRI

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: EXT-SREF, NE-SREF

The Synchronization Switch to Primary Reference condition occurs when the NCS system switches to the primary timing source (reference 1). The NCS system 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)

Logical Objects: EXT-SREF, NE-SREF

The Synchronization Switch to Secondary Reference condition occurs when the NCS system has switched to a secondary timing source (reference 2).

Clear the SWTOSEC Condition

Procedure

To clear the condition, clear alarms related to failures of the primary source, such as the SYNCPRI , on page 278 alarm.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

SWTOTHIRD

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: EXT-SREF, NE-SREF

The Synchronization Switch to Third Reference condition occurs when the NCS system has switched to a third timing source (reference 3).

Clear the SWTOTHIRD Condition

Procedure

To clear the condition, clear alarms related to failures of the primary source, such as the SYNCPRI , on page 278 alarm or the SYNCSEC , on page 279 alarm.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

SYNC-FREQ

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

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

Procedure

Step 1 Use an optical test set to verify the timing frequency of the line or BITS timing source and ensure that it falls within the proper frequency. For specific procedures to use the test set equipment, consult the manufacturer.

For BITS, the proper timing frequency range is approximately 15 PPM to 15 PPM. For optical line timing, the proper frequency range is approximately 16 PPM to 16 PPM.

Step 2 If the reference source frequency is not outside of bounds, complete the Physically Replace a Card, on page 313 procedure for the control card.

Note It takes up to 30 minutes for the control card to transfer the system software to the newly installed control card. Software transfer occurs in instances where different software versions exist on the two cards. When the transfer completes, the active control card reboots and goes into standby mode after approximately three minutes.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

SYNCLOSS

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Objects: FC, GE, ISC, TRUNK, EQPT

The Loss of Synchronization on Data Interface alarm is raised on MXP card client and 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

Procedure

Step 1 Ensure that the data port connection at the near end of the SONET or SDH (ETSI) link is operational.

Step 2 Verify fiber continuity to the port. To do this, follow site practices.

Step 3 View the physical port LED to determine whether the alarm has cleared.

- If the LED is green, the alarm has cleared.
- If the port LED is clear (that is, not lit green), the link is not connected and the alarm has not cleared.
- If the LED is red, this indicates that the fiber is pulled.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

SYNCPRI

Default Severity:

Minor (MN), Non-Service-Affecting (NSA) for EXT-SREF; Major (MJ), Service-Affecting (SA) for NE-SREF (For SONET)

Minor (MN), Non-Service-Affecting (NSA) for EXT-SREF; Major (MJ), Non-Service-Affecting (NSA) for NE-SREF (For SDH)

Logical Objects: EXT-SREF, NE-SREF

A Loss of Timing on Primary Reference alarm occurs when the NCS system loses the primary timing source (reference 1). The NCS system 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 NCS system should switch to its secondary timing source (reference 2). Switching to the secondary timing source also triggers the SWTOSEC , on page 276 alarm.

Clear the SYNCPRI Alarm

Procedure

Step 1 In node view (single-shelf mode) or shelf view (multishelf mode), click the **Provisioning** > **Timing** > **General** tabs.

Step 2 Verify the current configuration for REF-1 of the NE Reference.

Step 3 If the primary timing reference is a BITS input, complete the Clear the LOS (BITS) Alarm, on page 158 procedure.

Step 4 If the primary reference clock is an incoming port on the NCS system, complete the Clear the LOS (OCN/STMN) Alarm procedure located in the Alarm Troubleshooting chapter of the Troubleshooting guide.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

SYNCSEC

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Objects: EXT-SREF, NE-SREF

A Loss of Timing on Secondary Reference alarm occurs when the system loses the secondary timing source (reference 2). If SYNCSEC occurs, the system should switch to a third timing source (reference 3) to obtain valid timing for the system. Switching to a third timing source also triggers the SWTOTHIRD , on page 277 alarm.

Clear the SYNCSEC Alarm

Procedure

Step 1 In node view (single-shelf mode) or shelf view (multishelf mode), click the **Provisioning** > **Timing** > **General** tabs.

Step 2 Verify the current configuration of REF-2 for the NE Reference.

Step 3 If the secondary reference is a BITS input, complete the Clear the LOS (BITS) Alarm, on page 158 procedure.

Step 4 Verify that the BITS clock is operating properly.

Step 5 If the secondary timing source is an incoming port on the system, complete the Clear the LOS (OCN/STMN) Alarm procedure located in the Alarm Troubleshooting chapter of the Troubleshooting guide.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

SYNCTHIRD

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Objects: EXT-SREF, NE-SREF

A Loss of Timing on Third Reference alarm occurs when the NCS system loses the third timing source (reference 3). If SYNCTHIRD occurs and the NCS system uses an internal reference for source three, the control card could have failed. The NCS system often reports either the FRNGSYNC , on page 99 condition or the HLDOVRSYNC , on page 116 condition after a SYNCTHIRD alarm.

Clear the SYNCTHIRD Alarm

Procedure

Step 1 In node view (single-shelf mode) or shelf view (multishelf mode), click the **Provisioning** > **Timing** > **General** tabs.

Step 2 Verify that the current configuration of REF-3 for the NE Reference. For more information about references, refer to the Timing chapter in the Configuration guide.

Step 3 If the third timing source is a BITS input, complete the Clear the LOS (BITS) Alarm, on page 158 procedure.

Step 4 If the third timing source is an incoming port on the system, complete the Clear the LOS (OCN/STMN) Alarm procedure located in the Alarm Troubleshooting chapter of the Troubleshooting guide.

Caution Always use the supplied electrostatic discharge wristband when working with a powered system. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 5 Wait ten minutes to verify that the control card you reset completely reboots and becomes the standby card.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

SYSBOOT

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: NE

The System Reboot alarm indicates that new software is booting on the control card. No action is required to clear the alarm. The alarm clears when all cards finish rebooting the new software. The reboot takes up to 30 minutes. However, if several line cards are present on the nodes in the network or if the line cards reboot many times, the alarm clears before all the line cards reboot completely.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

Note SYSBOOT is an informational alarm. It only requires troubleshooting if it does not clear.

TEMP-LIC

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Temporary License (TEMP-LIC) alarm is raised to indicate that a valid temporary license is in use.

Clear the TEMP-LIC Alarm

Procedure

Procure and install a permanent license.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

TEMP-MISM

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: NE

Temperature Reading Mismatch Between Control Cards is raised when the temperature readings on the two control cards 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 control cards, allowing the values to be compared. The temperature of each control card 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

Procedure

Step 1 Complete the Inspect, Clean, and Replace the Air Filter, on page 316 procedure.

Step 2 If the condition does not clear, complete the Remove and Reinsert a Fan-Tray Assembly, on page 318 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

TIM

Default Severity: Critical (CR), Service-Affecting (SA)

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, 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/STMN) or UNEQ-P (or HP-UNEQ) alarms. 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

Procedure

Step 1 Ensure that the physical fibers are correctly configured and attached. To do this, consult site documents.

Step 2 If the alarm does not clear, ensure that the signal has not been incorrectly routed.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

TIM-MON

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The TIM Section Monitor TIM alarm is similar to the TIM , on page 282 alarm, but it applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, TXP_MR_10E_C, TXP_MR_10E_L, 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.)

Clear the TIM-MON Alarm

Procedure

Complete the Clear the TIM Alarm, on page 282 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html 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

Logical Object: 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

Procedure

Complete the Clear the TIM Alarm, on page 282 procedure. (The option will say Edit J1 Path Trace rather than Edit J0 Path Trace.)

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

TIM-S

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: 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 , on page 18 alarm can be raised downstream and the RFI-L , on page 252 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

Procedure

Step 1 Double-click the DS3/EC1-48 card to open the card view.

Step 2 Click the **Provisioning** > **EC1** > **Section Trace** tabs.

Step 3 Choose the port from the **Port** pull-down.

Step 4 In the Expected area, enter the correct string into the **Current Expected String** field.

Step 5 Click **Apply**.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

TRAF-AFFECT-RESET-REQUIRED

Default Severity: Minor (MN) and Non-Service affecting (NSA)

Logical Object: CARD

The Traffic Affecting Reset Required alarm is raised when you have to reset the MR-MXP cards. This reset impacts the traffic.

When you downgrade the WSE card from Release 11.12 to older releases such as R11.1.1.2, R11.0, R10 and so on, the Traffic Affecting Reset Required alarm is raised and does not clear.

The Traffic Affecting Reset Required alarm is raised when you have to upgrade the SMR 20 or SMR 20 FS CV cards.

Clear the TRAF-AFFECT-RESET-REQUIRED Alarm

Procedure

Step 1 Display the MR-MXP card in the card view.

Step 2 Click the **Provisioning > Card > Operating Modes** tabs.

Step 3 Click the **FGPA/FIRWAREUpgrade/TrafficAffectingReset** button.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

Clear the TRAF-AFFECT-RESET-REQUIRED Alarm for SMR 20 and SMR 20 FS CV Cards

Procedure

Step 1 Display the SMR 20 or SMR20 FS CV card in the card view.

Step 2 Click the **Maintenance> Firmware** tabs.

Step 3 Click the **FIRMWARE Upgrade** button.

Step 4 Click **Yes**.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

TRAF-AFFECT-SEC-UPG-REQUIRED

Default Severity: Not Reported (NR), Non Service Affecting (NSA)

Logical Object: EQUIPMENT

The TRAF-AFFECT-SEC-UPG-REQUIRED alarm occurs when there is a control FPGA version mismatch and the control FPGA flash partition is not locked.

Clear the TRAF-AFFECT-SEC-UPG-REQUIRED alarm

Procedure

Upgrade the FPGA image and lock the partition of the control FPGA.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

TRAIL-SIGNAL-FAIL

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: OCH, TRUNK

The Trail Signal Fail condition is raised on a DWDM trunk port or OCH port to correlate with the LOS-P (TRUNK) , on page 170 alarm when the trunk port administrative state is set to OOS,DSBLD (or Locked,disabled).

Clear the TRAIL-SIGNAL-FAIL Condition

Procedure

Switch the OCHNC administrative state of the errored OCH or trunk port to **IS** (or **Unlocked**).

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

TRUNK-ODU-AIS

Default Severity: Not Reported (NR)

Logical Object: OCN, OTU, GE, FC

The TRUNK-ODU-AIS condition is raised on the 100G-LC-C or 10x10G-LC card when the node detects the optical data unit (ODU) alarm indication signal (AIS) from the trunk port. This condition is raised to indicate a signal failure.

Clear the TRUNK-ODU-AIS Condition

Procedure

Remove the far-end fault causing the remote ODU-AIS insertion and bring up the traffic between the two ports.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

TRAIL-SIGNAL-FAIL

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: OCH, TRUNK

The Trail Signal Fail condition is raised on a DWDM trunk port or OCH port to correlate with the LOS-P (TRUNK) , on page 170 alarm when the trunk port administrative state is set to OOS,DSBLD (or Locked,disabled).

Clear the TRAIL-SIGNAL-FAIL Condition

Procedure

Switch the OCHNC administrative state of the errored OCH or trunk port to **IS** (or **Unlocked**).

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OPU-CSF

Default Severity: Not Reported (NR)

Logical Objects: GE

The Optical Payload Unit Client Signal Fail (OPU-CSF) alarm indicates a remote client signal failure on the node.

Clear the OPU-CSF Alarm

Procedure

Clear the remote client signal on the node.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

TRUNK-PAYLOAD-MISM

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: OCN, OTN, GE, FC

The TRUNK-PAYLOAD-MISM alarm is raised on the 10x10G-LC card, which is configured in the 10x10G muxponder mode. This occurs when the payload types configured at the near-end and far-end nodes are different.

Clear the TRUNK-PAYLOAD-MISM Alarm

Configure the same payload type at both near-end and far-end nodes.

Procedure

Step 1 Log in to a node on the network.

Step 2 In node view (single-shelf mode) or shelf view (multishelf mode), double-click the reporting card in CTC to open the card view.

Step 3 Click the **Provisioning** > **Pluggable Port Modules** tabs.

Step 4 In the Pluggable Port Modules area, click **Create**.

Step 5 Choose the same payload type from the Port Type drop-down list and click **OK**.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

TX-OFF-NON-CISCO-PPM

Default Severity: Major (MJ), Non-Service-Affecting (NSA)

Logical Object: PPM

The Laser Off Non Cisco PPM (TX-OFF-NON-CISCO-PPM) alarm occurs when the PPM plugged into a card's port fails the security code check and laser is shutdown. The check fails when the PPM used is not a Cisco PPM.

Clear the TX-OFF-NON-CISCO-PPM Condition

Procedure

Obtain the correct Cisco PPM and replace the existing PPM with the new one.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

UNC-WORD

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The Uncorrected FEC Word condition indicates that the FEC capability could not sufficiently correct the frame.

Clear the UNC-WORD Condition

Procedure

Step 1 Ensure that the fiber connector for the card is completely plugged in.

Step 2 Ensure that the ports on the far end and near end nodes have the same port rates and FEC settings.

Step 3 If the BER threshold is correct and at the expected level, use an optical test set to measure the power level of the line to ensure it is within guidelines. For specific procedures to use the test set equipment, consult the manufacturer.

Step 4 If the optical power level is good, verify that optical receive levels are within the acceptable range.

Step 5 If receive levels are good, clean the fibers at both ends according to site practice.

Step 6 If the condition does not clear, verify that single-mode fiber is used.

Step 7 If the fiber is of the correct type, verify that a single-mode laser is used at the far-end node.

Step 8 Clean the fiber connectors at both ends for a signal degrade according to site practice.

Step 9 Verify that a single-mode laser is used at the far end.

Step 10 If the problem does not clear, the transmitter at the other end of the optical line could be failing and require replacement. Refer to the Physical Card Reseating, Resetting, and Replacement, on page 312 section.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

UNEQ-P

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: 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.

Clear the UNEQ-P Alarm

Procedure

Step 1 In node view, choose **Go to Network View** from the View menu.

Step 2 Right-click the alarm to display the Select Affected Circuits shortcut menu.

Step 3 Click **Select Affected Circuits**.

Step 4 When the affected circuits appear, look in the Type column for VTT, which indicates a VT tunnel circuit. A VT tunnel with no VTs assigned could be the cause of an UNEQ-P alarm.

Step 5 If the Type column does not contain VTT, there are no VT tunnels connected with the alarm. Go to Step 7, on page 290.

Step 6 If the Type column does contain VTT, attempt to delete these rows:

Note The node does not allow you to delete a valid VT tunnel or one with a valid VT circuit inside.

a) Click the VT tunnel circuit row to highlight it. Complete the Delete a Circuit, on page 314 procedure.
b) If an error message dialog box appears, the VT tunnel is valid and not the cause of the alarm.
c) If any other rows contain VTT, repeat Step 6, on page 290.

Step 7 If all nodes in the ring appear in the CTC network view, determine whether the circuits are complete:

a) Click the **Circuits** tab.
b) Verify that PARTIAL is not listed in the Status column of any circuits.

Step 8 If you find circuits listed as PARTIAL, use an optical test set to verify that these circuits are not working circuits that continue to pass traffic. For specific procedures to use the test set equipment, consult the manufacturer.

Step 9 If the PARTIAL circuits are not needed or are not passing traffic, delete the PARTIAL circuits.

Complete the Delete a Circuit, on page 314 procedure.

Step 10 Recreate the circuit with the correct circuit size. Refer to the Create Circuits and VT Tunnels chapter in the Configuration guide.

Step 11 Log back in and verify that all circuits terminating in the reporting card are active:

a) Click the **Circuits** tab.

b) Verify that the **Status** column lists all circuits as active.

Step 12 If the alarm does not clear, clean the far-end optical fiber according to site practice. If no site practice exists, complete the procedure in the Maintain the Node chapter of the Configuration guide.

On the OC-192 card:

Warning **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 system. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 13 If the alarm does not clear, complete the Physically Replace a Card, on page 313 procedure for the OC-N and electrical cards.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

UNIT-HIGH-TEMP

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: EQPT

The UNIT-HIGH-TEMP alarm applies to the 100G-LC-C, 10x10G-LC, or CFP-LC cards. The alarm occurs when the temperature of any one of the internal measurement points exceeds its predefined threshold. It indicates that the card is functioning in abnormal conditions that could jeopardize its reliability in the long term. The alarm is raised because of one of these reasons:

- An improper rack installation
- Abnormally high environmental temperature
- An unclean air filter
- A hardware failure of the card

Clearing the UNIT-HIGH-TEMP Alarm

Procedure

Step 1 Verify that the rack is installed properly. For proper airflow and cooling of the shelf, the shape of the vertical posts of the rack should be such that the airflow vents are not covered. For more information about the installation, refer to the *Hardware Installation Guide*.

Step 2 If the rack installation is proper, verify that the environmental temperature of the room is not abnormally high.

Step 3 If the room temperature is not abnormally high, ensure that nothing prevents the fan-tray assembly from passing air through the system shelf.

Step 4 If the airflow is not blocked, determine whether the air filter needs replacement. Refer to the Inspect, Clean, and Replace the Air Filter, on page 316 procedure.

Step 5 If the air filter is clean, ensure all empty slots are installed with filler cards.

Step 6 If all the slots are installed with cards, check the cooling profile settings for the shelf and ensure it is set to high.

Step 7 If the cooling profile settings are proper, complete the Physically Replace a Card, on page 313 procedure for the 100G-LC-C , 10x10G-LC, or CFP-LC card.

Note When you replace a card an identical card, you do not need to make any changes to the database.

If the troubleshooting procedure does not clear the alarm, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html or call the Cisco Technical Assistance Center (1 800 553-2447) to report the problem.

UNQUAL-PPM

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

Logical Objects: PPM

The Unqualified PPM Inserted condition occurs when a PPM with a nonqualified product ID is plugged into the card 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

Procedure

Obtain the correct Cisco PPM and replace the existing PPM with the new one.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

UNREACHABLE-TARGET-POWER

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: OCH

The Unreachable Port Target Power alarm occurs on WSS32 cards during startup as the card laser attains its correct power level. The condition disappears when the card successfully boots.

Note Card power levels are listed in the "Hardware Specifications" appendix of the *Cisco ONS 15454 DWDM Reference Manual*Hardware Specifications document.

Note UNREACHABLE-TARGET-POWER is an informational condition. It only requires troubleshooting if it does not clear.

USB-EMPTY-CODE-VOL

Default Severity: Critital (CR) for M2, M6, and M15 chassis, Minor (MN) for Stand-alone control card, Service-Affecting (SA)

Logical Object: USB MODULE

The USB-EMPTY-CODE-VOL alarm occurs when USB gets formatted during a control card software upgrade.

Clearing the USB-EMPTY-CODE-VOL Alarm

The USB-EMPTY-CODE-VOL alarm clears without user intervention as soon as the USBSYNC operation between the control card and the USB interface is successful.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

USBSYNC

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: USB

The USB Synchronization (USB-SYNC) alarm is raised during the sync operation between the control card and the USB interface.

Clear the USB-SYNC Alarm

Procedure

The USB-SYNC alarm clears without user intervention as soon as synchronization between the control card and the USB interface completes.

USB-MOUNT-FAIL Alarm

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Objects: USB

The USB Mount Fail (USB-MOUNT-FAIL) alarm is raised when the USB flash is not mounted.

Clearing the USB-MOUNT-FAIL Alarm

Procedure

Step 1 Back up the database of the active control card.

Step 2 Remove the standby control card.

Step 3 Reboot the active control card.

Step 4 After the active control card is rebooted, reinsert the standby control card.

If the troubleshooting procedure does not clear the alarm, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html or call the Cisco Technical Assistance Center (1 800 553-2447) to report the problem.

USB PORTS DOWN

Default Severity: Major (MJ), Non-Service-Affecting (NSA)

Logical Object: ECU

The USB Ports Down alarm is raised when the USB enumeration fails to detect the external connection unit (ECU) hubs and passive devices.

Clear the USB PORTS DOWN Alarm

Procedure

Perform soft reset or hard reboot of the controller card.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

USB-WRITE-FAIL

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: USB

The USB Write Fail (USB-WRITE-FAIL) alarm is raised when a write operation on the USB interface fails due to communication disruptions.

Clear the USB-WRITE-FAIL Alarm

Procedure

Step 1 Verify that both the control cards are powered and enabled by confirming lighted ACT/SBY LEDs.

Step 2 If both the control cards are powered and enabled, reset the active control card.

Step 3 Wait ten minutes to verify that the card you reset completely reboots.

Step 4 If the control card you reset does not reboot successfully, or the alarm has not cleared, call Cisco TAC 1 800 553-2447.

UT-COMM-FAIL

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: TRUNK

The Universal Transponder (UT) Module Communication Failure alarm is raised on MXP_2.5G_10E and TXP_MR_10E cards when there is a universal transponder communication failure because the universal transponder (UT) has stopped responding to the control card.

Clear the UT-COMM-FAIL Alarm

Procedure

Step 1 In node view (single-shelf mode) or shelf view (multishelf mode), double-click the card to open the card view.

Step 2 Request a laser restart:

a) Click the **Maintenance** > **ALS** tabs.
b) Check the **Request Laser Restart** check box.
c) Click Apply.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

UT-FAIL

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: TRUNK

The Universal Transponder Module Hardware Failure alarm is raised against MXP_2.5G_10E and TXP_MR_10E cards when a UT-COMM-FAIL alarm persists despite being reset.

Clear the UT-FAIL Alarm

Procedure

Complete the Physically Replace a Card, on page 313 procedure for the alarmed card.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

VOA-DISABLED

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: EQPT

The VOA Disabled alarm indicates that the VOA control loop is disabled due to excessive counter-propagation light. This alarm is raised when there is a mis-cabling of interface cards, that is, when the interface trunk TX port is connected to DMX drop-TX port through the patch-panel.

Clear the VOA-DISABLED Condition

Procedure

To clear the alarm, check and ensure that the patchcords connection to and from the interfaces trunk ports are proper.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

VOA-HDEG

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Objects: AOTS, OCH, OMS, OTS

The VOA High Degrade alarm is raised on DWDM cards when an equipped VOA exceeds the setpoint due to an internal problem. The alarm indicates that the attenuation has crossed the high degrade threshold.

Clear the VOA-HDEG Alarm

Procedure

Complete the Physically Replace a Card, on page 313 procedure for the alarmed card.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

VOA-HFAIL

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Objects: AOTS, OCH, OMS, OTS

The VOA High Fail alarm is raised on DWDM cards when an equipped VOA exceeds the setpoint due to an internal problem. The alarm indicates that the attenuation has crossed the high fail threshold. The card must be replaced.

Clear the VOA-HFAIL Alarm

Procedure

Complete the Physically Replace a Card, on page 313 procedure for the alarmed card.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

VOA-LMDEG

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Objects: AOTS, OCH, OMS, OTS

The VOA Low Degrade alarm is raised on DWDM cards when an equipped VOA does not reach the setpoint due to an internal problem. The alarm indicates that the attenuation has crossed the low degrade threshold.

Clear the VOA-LDEG Alarm

Procedure

Complete the Physically Replace a Card, on page 313 procedure for the alarmed card.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

VOA-LFAIL

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Objects: AOTS, OCH, OMS, OTS

The VOA Low Fail alarm is raised on DWDM cards when an equipped VOA does not reach the setpoint due to an internal problem. The alarm indicates that the attenuation has crossed the low fail threshold. The card must be replaced.

Clear the VOA-LFAIL Alarm

Procedure

Complete the Physically Replace a Card, on page 313 procedure for the alarmed card.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

VOLT-MISM

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: PWR

The Power Monitoring Mismatch Between Control Cards alarm is raised against the shelf when the power voltages of both the control cards are out of range of each other by more than 3V DC.

Clear the VOLT-MISM Condition

Procedure

Step 1 Check the incoming voltage level to the shelf using a voltmeter. Follow site practices.

Step 2 Correct any incoming voltage issues.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

WAITING-TO-START

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: OTS

The WAITING-TO-START condition is raised on the COM-TX and EXP-TX ports of 16-WXC-FS, 17 SMR9 FS, 24 SMR9 FS, 34 SMR9 FS, and SMR20 FS cards by the control cards when a cross-connection is ready to start and/or waiting for other transient conditions to clear. The condition clears when cross-connection is running in In-Service administrative state .

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

WAN-SYNCLOSS

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Objects: STSMON, STSTRM

The WAN-SYNCLOSS condition is raised when GE-Syncloss condition is detected on a STS payloads (STS-192c).

Clear the WAN-SYNCLOSS Condition

Procedure

Set a valid GE frame and payload inside the affected STS.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

WKSWPR (2R, EQPT, ESCON, FC, GE, ISC, OTS)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: 2R, EQPT, ESCON, FC, GE, ISC, OTS

This condition is raised when you use the FORCE SPAN, FORCE RING, or MANUAL SPAN command at for a Y-Cable-protected MXP or TXP client port (set for one the above-listed client configurations). WKSWPR is visible on the network view Alarms, Conditions, and History tabs.

This condition is raised when traffic is manually or automatically switched from the working to the protect path on the 200G-CK-LC card. Reset the control card to clear the WKSWPR alarm.

Note For more information about protection schemes, refer to the Manage the Node chapter of the *Cisco ONS 15454 DWDM Procedure Guide*Manage the Node document.

WKSWPR (TRUNK)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: TRUNK

This condition is raised when you use the FORCE SPAN, FORCE RING, or MANUAL SPAN command at for a splitter-protection enabled MXP or TXP trunk port.

WRK-PATH-RECOVERY-CHECK

Default Severity: Non-Alarming (NA), Non-Service Affecting (NSA)

Logical Objects: OTS

The Working Path Recovery Check (WRK-PATH-RECOVERY-CHECK) alarm is raised against PSM cards when traffic switches to the protection path and that is revertive. This alarm is raised only when the protection path is configured as revertive.

Clear the WRK-PATH-RECOVERY-CHECK Alarm

Procedure

WRK-PATH-RECOVERY-CHECK alarm clears in one of these scenarios:

a) The alarm clears automatically when the Wait To Restore (WTR) timer starts. The traffic reverts to working path at the end of the timer.
b) The alarm clears when traffic switches to the working path.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

Wait to Restore Condition

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: 2R, ESCON, FC, GE, ISC, PSM

The Wait To Restore condition occurs:

- On the client ports in the 2R, ESCON, FC, GE, and ISC configurations, in a Y-cable protection group when the WKSWPR (TRUNK), on page 300 condition, is raised. The condition occurs when the wait-to-restore time has not expired; this meas 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.
- On PSM cards, when the WTR timer starts. The timer starts before the traffic is switched from the protection path to the working path. The condition clears when the timer expires and traffic switches back to the working path.

Note WTR is an informational condition and does not require troubleshooting.

WTR (TRUNK)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The Wait To Restore condition occurs when the WKSWPR (TRUNK), on page 300 condition, is raised for MXP or TXP splitter protection scheme ports. The condition occurs when 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.

Note WTR is an informational condition and does not require troubleshooting.

WVL-DRIFT-CHAN-OFF

Default Severity: Not Reported (NR), Service-Affecting (SA)

Logical Object: OCH

The Wavelength Channel OFF (WVL_CHAN_OFF) condition occurs in 40-SMR1-C, 40-SMR2-C, 80-WXC-C, 40-WXC-C, or 40-WSS-C cards. The condition detects slow variation in wavelength or optical power of a TXP Trunk-TX port connected to an MSTP multiplexer.

WVL-DRIFT-CHAN-OFF alarm occurs in different ports depending on the type of card:

- In the 80-WXC-C or 40-WXC-C cards, COM-TX port for ADD/DROP and EXP/PT circuits.
- In the 40-SMR1-C or 40-SMR2-C cards, LINE-TX port for ADD/DROP and EXP/PT circuits.
- In the 40-WSS-C card, CHAN-RX port for ADD/DROP circuits and PT port for pass through circuits.

Clear the WVL-DRIFT-CHAN-OFF Condition

Procedure

WVL-DRIFT-CHAN-OFF condition clears in the following scenarios:

- OCH port is forced OOS.
- OCH-circuit associated to the port is deleted or set to OOS state.
- Hardware reset or card removal.
- Software reset of the card.

Note Although the WVL-DRIFT-CHAN-OFF condition is raised in the optical card, make sure that the laser source connected to the MSTP equipment is investigated to isolate the origin of the issue. Laser is likely affected by wavelength instability or wavelength drift causing this condition to occur.

WVL-MISMATCH

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: TRUNK

Clear the WVL-MISMATCH alarm

WVL-UNLOCKED Alarm

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Objects: TRUNK

The Wavelength Unlocked (WVL-UNLOCKED) alarm occurs when the laser cannot be tuned at the required wavelength. This is a normal condition during laser frequency requests.

The alarm is cleared when the laser wavelength locker detects a lock condition during which the laser is steadily tuned at the required wavelength.

DWDM Card LED Activity

The following sections list the DWDM card LED sequences during card insertion and reset.

DWDM Card LED Activity After Insertion

When an DWDM card is inserted in the shelf, the following LED activities occur:

1. The FAIL LED illuminates for approximately 35 seconds.
2. The FAIL LED blinks for approximately 40 seconds.
3. All LEDs illuminate and then turn off within 5 seconds.
4. If new software is being downloaded to the card, the ACT and SF LEDs blink for 20 seconds to 3.5 minutes, depending on the card type.
5. The ACT LED illuminates.
6. The SF LED stays illuminated until all card ports connect to their far-end counterparts and a signal is present.

DWDM Card LED Activity During Reset

When an DWDM card resets (by software or hardware), the following LED activities occur:

1. The FAIL LED switches on for few seconds.
2. The FAIL LED on the physical card blinks and turns off.
3. The white LED with the letters LDG appears on the reset card in CTC.
4. The green ACT LED appears in CTC.

Traffic Card LED Activity

System 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 non-DWDM 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 non-DWDM 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 non-DWDM card successfully resets, the following LED states are present:

- If you are looking at the physical NCS system, the ACT/SBY LED is illuminated.
- If you are looking at node view (single-shelf mode) or shelf view (multishelf mode) of the NCS system, 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 (single-shelf mode) or shelf view (multishelf mode) of the NCS system, 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.

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 system documentation. They are included in this chapter for the user convenience. For further information, please refer to the Configuration guide as appropriate to your purpose

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

Procedure

Step 1 Log into a node on the network.

Step 2 In node view, choose **Go to Network View** from the View menu.

Step 3 Click the **Provisioning** > **BLSR** tabs.

Step 4 From the Ring Name column, record the ring name, or in the Nodes column, record the Node IDs in the BLSR. The Node IDs are the numbers in parentheses next to the node name.

Change a BLSR Ring Name

Procedure

Step 1 Log into a node on the network.

Step 2 In node view, choose **Go to Network View** from the View menu.

Step 3 Click the **Provisioning** > **BLSR** tabs.

Step 4 Highlight the ring and click **Edit.**

Step 5 In the BLSR window, enter the new name in the Ring Name field.

Step 6 Click **Apply.**

Step 7 Click **Yes** in the Changing Ring Name dialog box.

Change a BLSR Node ID Number

Procedure

Step 1 Log into a node on the network.
Step 2 In node view, choose **Go to Network View** from the View menu.
Step 3 Click the **Provisioning** > **BLSR** tabs.
Step 4 Highlight the ring and click **Edit.**
Step 5 In the BLSR window, right-click the node on the ring map.
Step 6 Select **Set Node ID** from the shortcut menu.
Step 7 In the Edit Node ID dialog box, enter the new ID. The Node ID is the number in parentheses after the Node Name.
Step 8 Click **OK.**

Verify Node Visibility for Other Nodes

Procedure

Step 1 Log into a node on the network.
Step 2 In node view, click the **Provisioning** > **BLSR** tabs.
Step 3 Highlight a BLSR.
Step 4 Click **Ring Map**.
Step 5 In the BLSR Ring Map window, verify that each node in the ring appears on the ring map with a node ID and IP address.
Step 6 Click **Close**.

Protection Switching, Lock Initiation, and Clearing

The following sections give instructions for port, ring, and span switching and switch-clearing commands, as well as lock-ons and lockouts.

Initiate a 1+1 Protection Port Force Switch Command

The following sections give instructions for port switching and switch-clearing commands.

Procedure

Step 1 In node view (single-shelf mode) or shelf view (multishelf mode), click the **Maintenance** > **Protection** tabs.
Step 2 In the Protection Groups area, select the protection group with the port you want to switch.

Step 3 In the Selected Groups area, select the port belonging to the card you are replacing. You can carry out this command for the working or protect port. For example, if you need to replace the card with the Protect/Standby port, click this port.

Step 4 In the Switch Commands area, click **Force**.

Step 5 Click **Yes** in the Confirm Force Operation dialog box.

Step 6 If the switch is successful, the group says Force to working in the Selected Groups area.

Initiate a 1+1 Manual Switch Command

This procedure switches 1+1 protection group traffic from one port in the group to the other using a Manual switch.

Note A Manual command switches traffic if the path has an error rate less than the signal degrade. A Manual switch is preempted by a Force switch.

Procedure

Step 1 In node view (single-shelf mode) or shelf view (multishelf mode), click the **Maintenance** > **Protection** tabs.

Step 2 In the Protection Groups area, select the protection group with the port you want to switch.

Step 3 In the Selected Groups area, select the port belonging to the card you are replacing. You can carry out this command for the working or protect port. For example, if you need to replace the card with the protect/standby port, click this port.

Step 4 In the Switch Commands area, click **Manual**.

Step 5 Click **Yes** in the Confirm Force Operation dialog box.

Step 6 If the switch is successful, the group now says Manual to working in the Selected Groups area.

Initiate a 1:1 Card Switch Command

Note The Switch command only works on the active card, whether this card is working or protect. It does not work on the standby card.

Procedure

Step 1 In node view, click the **Maintenance** > **Protection** tabs.

Step 2 Click the protection group that contains the card you want to switch.

Step 3 Under Selected Group, click the active card.

Step 4 Next to Switch Commands, click **Switch**.

The working slot should change to Working/Active and the protect slot should change to Protect/Standby.

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.

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.

Procedure

Step 1 In node view (single-shelf mode) or shelf view (multishelf mode), click the **Maintenance** > **Protection** tabs.

Step 2 In the Protection Groups area, choose the protection group containing the port you want to clear.

Step 3 In the Selected Group area, choose the port you want to clear.

Step 4 In the Switching Commands area, click **Clear.**

Step 5 Click **Yes** in the Confirmation Dialog box.

The Force switch is cleared. Traffic immediately reverts to the working port if the group was configured for revertive switching.

Initiate a Lock-On Command

Note For 1:1 and 1:N electrical protection groups, working or protect cards can be placed in the Lock On state. For a 1+1 optical protection group, only the working port can be placed in the Lock On state.

Procedure

Step 1 In node view (single-shelf mode) or shelf view (multishelf mode), click the **Maintenance** > **Protection** tabs.

Step 2 In the Protection Groups list, click the protection group where you want to apply a lock-on.

Step 3 If you determine that the protect card is in standby mode and you want to apply the lock-on to the protect card, make the protect card active if necessary:

a) In the Selected Group list, click the protect card.

b) In the Switch Commands area, click **Force**.

Step 4 In the Selected Group list, click the active card where you want to lock traffic.

Step 5 In the Inhibit Switching area, click **Lock On**.

Step 6 Click **Yes** in the confirmation dialog box.

Initiate a Card or Port Lockout Command

Note For 1:1 or 1:N electrical protection groups, working or protect cards can be placed in the Lock Out state. For a 1+1 optical protection group, only the protect port can be placed in the Lock Out state.

Procedure

Step 1 In node view (single-shelf mode) or shelf view (multishelf mode), click the **Maintenance** > **Protection** tabs.

Step 2 In the Protection Groups list, click the protection group that contains the card you want to lockout.

Step 3 In the Selected Group list, click the card where you want to lock out traffic.

Step 4 In the Inhibit Switching area, click **Lock Out**.

Step 5 Click **Yes** in the confirmation dialog box.

The lockout has been applied and traffic is switched to the opposite card.

Clear a Lock-On or Lockout Command

Procedure

Step 1 In node view (single-shelf mode) or shelf view (multishelf mode), click the **Maintenance** > **Protection** tabs.

Step 2 In the Protection Groups list, click the protection group that contains the card you want to clear.

Step 3 In the Selected Group list, click the card you want to clear.

Step 4 In the Inhibit Switching area, click **Unlock**.

Step 5 Click **Yes** in the confirmation dialog box.

The lock-on or lockout is cleared.

Initiate a Lockout on a BLSR Protect Span

Procedure

Step 1 From the View menu choose **Go to Network View**.

Step 2 Click the **Provisioning** > **BLSR** tabs.

Step 3 Choose the BLSR and click **Edit**.

Step 4 Right-click the BLSR node channel (port) and choose **Set West Protection Operation** (if you chose a west channel) or **Set East Protection Operation** (if you chose an east channel).

Step 5 In the Set West Protection Operation dialog box or the Set East Protection Operation dialog box, choose **Lockout Protect Span** from the drop-down list.

Step 6 Click **OK**.

Step 7 Click **Yes** in the two Confirm BLSR Operation dialog boxes.

Clear a BLSR External Switching Command

Procedure

Step 1 Log into a node on the network.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 Click the **Provisioning** > **BLSR** tabs.

Step 4 Click the BLSR you want to clear.

Step 5 Right-click the west port of the BLSR node where you invoked the switch and choose **Set West Protection Operation**.

Step 6 In the Set West Protection Operation dialog box, choose **Clear** from the drop-down list.

Step 7 Click **OK**.

Step 8 Click **Yes** in the Confirm BLSR Operation dialog box.

Card Resetting and Switching

This section gives instructions for resetting traffic cards and control 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 Configuration 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.

Reset a Card in CTC

Procedure

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2, on page 311.

Step 2 In node view (single-shelf mode) or shelf view (multishelf mode), position the cursor over the optical or electrical traffic card slot reporting the alarm.

Step 3 Right-click the card. Choose **Reset Card** from the shortcut menu.

Step 4 Click **Yes** in the Resetting Card dialog box.

Reset an Active Control Card and Activate the Standby Card

Note Before you reset the control card, you should wait at least 60 seconds after the last provisioning change you made to avoid losing any changes to the database.

Before you begin

Caution Resetting an active control card can be service-affecting.

Procedure

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 Identify the active control card:

If you are looking at the physical ONS system shelf, the ACT/SBY LED of the active card is green. The ACT/STBLY LED of the standby card is amber.

Step 3 In node view (single-shelf mode) or shelf view (multishelf mode), right-click the active control card in CTC.

Step 4 Choose **Reset Card** from the shortcut menu.

Step 5 Click **Yes** in the Confirmation Dialog box.

The card resets, the FAIL LED blinks on the physical card, and connection to the node is lost. CTC switches to network view.

Step 6 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. For LED appearance, see the Typical Card LED State After Successful Reset, on page 304 section.

Step 7 Double-click the node and ensure that the reset control card is in standby mode and that the other control card is active. Verify the following:

- If you are looking at the physical ONS system 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.

Physical Card Reseating, Resetting, and Replacement

This section gives instructions for physically reseating and replacing control cards and line cards.

Caution Do not physically replace a card without first making provisions to switch or move traffic to a different card or circuit..

Remove and Reinsert (Reseat) the Standby Control Card

Note Before you reset the control card, you should wait at least 60 seconds after the last provisioning change you made to avoid losing any changes to the database.

When a standby control card is removed and reinserted (reseated), all three fan lights could momentarily turn on, indicating that the fans have also reset.

Before you begin

Warning **High-performance devices on this card can get hot during operation. To remove the card, hold it by the faceplate and bottom edge. Allow the card to cool before touching any other part of it or before placing it in an antistatic bag.** Statement 201

Caution Always use the supplied electrostatic discharge wristband when working with a powered system. 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 control card reseat could be service-affecting. Refer to the Protection Switching, Lock Initiation, and Clearing, on page 306 section for traffic-switching procedures.

Procedure

Step 1 Log into a node on the network.

Ensure that the control card you want to reseat is in standby mode. A standby card has an amber ACT/SBY (Active/Standby) LED illuminated.

Step 2 When the control card is in standby mode, unlatch both the top and bottom ejectors on the control card.

Step 3 Physically pull the card at least partly out of the slot until the lighted LEDs turn off.

Step 4 Wait 30 seconds. Reinsert the card and close the ejectors.

Note The control card requires several minutes to reboot and display the amber standby LED after rebooting. Refer to the Configuration guide for more information about LED behavior during a card reboot.

Remove and Reinsert (Reseat) Any Card

Before you begin

Warning Warning: High-performance devices on this card can get hot during operation. To remove the card, hold it by the faceplate and bottom edge. Allow the card to cool before touching any other part of it or before placing it in an antistatic bag. Statement 201

Caution Always use the supplied electrostatic discharge wristband when working with a powered NCS system. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Procedure

Step 1 Open the card ejectors.

Step 2 Slide the card halfway out of the slot along the guide rails.

Step 3 Slide the card all the way back into the slot along the guide rails.

Step 4 Close the ejectors.

Physically Replace a Card

When you replace a card with the identical type of card, you do not need to make any changes to the database.

Before you begin

Warning **High-performance devices on this card can get hot during operation. To remove the card, hold it by the faceplate and bottom edge. Allow the card to cool before touching any other part of it or before placing it in an antistatic bag.** Statement 201

Caution Always use the supplied electrostatic discharge wristband when working with a powered NCS system. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Caution Removing an active card can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the Protection Switching, Lock Initiation, and Clearing, on page 306 section for commonly used traffic-switching procedures.

Procedure

Step 1 Open the card ejectors.
Step 2 Slide the card out of the slot.
Step 3 Open the ejectors on the replacement card.
Step 4 Slide the replacement card into the slot along the guide rails.
Step 5 Close the ejectors.

Generic Signal and Circuit Procedures

This section gives instructions for verify BER thresholds, deleting circuits, provisioning SDCC (or MS DCC) terminations, and clearing loopbacks.

Verify the Signal BER Threshold Level

This procedure is used for MXP or TXP cards.

Procedure

Step 1 Log into a node on the network.
Step 2 In node view (single-shelf mode) or shelf view (multishelf mode), double-click the card reporting the alarm to open the card view.
Step 3 Click the **Provisioning** > **Line** > **SONET** (or **SDH**) tabs.
Step 4 Under the **SD BER** (or **SF BER**) column in the Provisioning window, verify that the cell entry is consistent with the originally provisioned threshold. The default setting is 1E-7.
Step 5 If the entry is consistent with the original provisioning, go back to your original procedure.
Step 6 If the entry is not consistent with what the system was originally provisioned for, click the cell to reveal the range of choices and click the original entry.
Step 7 Click **Apply**.

Delete a Circuit

Procedure

Step 1 Log into a node on the network.

Step 2 In node view (single-shelf mode) or shelf view (multishelf mode), click the **Circuits** tab.

Step 3 Click the circuit row to highlight it and click **Delete.**

Step 4 Click **Yes** in the Delete Circuits dialog box.

Verify or Create Node Section DCC Terminations

Procedure

Step 1 Log into a node on the network.

Step 2 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **Comm Channels** > **SDCC** (or **Provisioning** > **Comm Channels** > **MS DCC**) tab.

Step 3 View the Port column entries to see where terminations are present for a node. If terminations are missing, proceed to Step 4.

Step 4 If necessary, create a DCC termination:

a) Click **Create**.

b) In the Create SDCC Terminations (or Create MS DCC Terminations) dialog box, click the ports where you want to create the DCC termination. To select more than one port, press the Shift key.

c) In the port state area, click the **Set to IS** (or **Set to Unlocked**) radio button.

d) Verify that the Disable OSPF on Link check box is unchecked.

e) Click **OK**.

Clear an MXP, TXP, GE-XP, 10GE-XP, and ADM-10G Card Loopback Circuit

Procedure

Step 1 Log into a node on the network.

Step 2 In node view (single-shelf mode) or shelf view (multishelf mode), double-click the reporting card in CTC to open the card view.

Step 3 Click the **Maintenance** > **Loopback** tabs.

Step 4 In the Loopback Type column, determine whether any port row shows a state other than None.

Step 5 If a row contains another state besides None, click in the column cell to display the drop-down list and select **None.**

Step 6 In the Admin State column, determine whether any port row shows an administrative state other than IS, for example, OOS,MT.

Step 7 If a row shows an administrative state other than IS, click in the column cell to display the drop-down list and select **IS** or **Unlocked.**

Note If ports managed into IS (or Unlocked) administrative state are not receiving signals, the LOS alarm is either raised or remains, and the port service state transitions to OOS-AU,FLT (or Locked-disabled, automaticInService & failed).

Step 8 Click **Apply**.

Verify or Create Node RS-DCC Terminations

Procedure

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 In node view, click the **Provisioning** > **Comm Channels** > **RS-DCC** tab.

Step 3 View the Port column entries to see where terminations are present for a node. If terminations are missing, proceed to Step 4.

Step 4 If necessary, create a DCC termination by completing the following steps:

a) Click **Create**.

b) In the Create RS-DCC Terminations dialog box, click the ports where you want to create the DCC termination. To select more than one port, press the Shift key.

c) In the port state area, click the **Set to Unlocked** radio button.

d) Verify that the Disable OSPF on Link check box is unchecked.

e) Click **OK**.

Clear an STM-N Card XC Loopback Circuit

Procedure

Step 1 Log into a node on the network. If you are already logged in, continue with Clear an STM-N Card XC Loopback Circuit, on page 316.

Step 2 Double-click the reporting card in CTC to display the card view.

Step 3 Click the **Maintenance** > **Loopback** > **VC4** tabs.

Step 4 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 Air Filter

Before you begin

To complete this task, you need a replacement air 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 system. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Procedure

Step 1 If the air filter is installed in the external filter brackets, slide the filter out of the brackets while being careful not to dislodge any dust that could have collected on the filter. If the filter is installed beneath the fan tray and not in the external filter brackets, open and remove the front door assembly by completing the following steps:

a) Open the front door of the shelf assembly by completing the following substeps.(If it is already open or if the shelf assembly does not have a front door, continue with Step 2, on page 317.)

- Open the front door lock.
- Press the door button to release the latch.
- Swing the door open.

b) Remove the front door by completing the following substeps (optional):

- Detach the ground strap from either the door or the chassis by removing one of the Kepnuts.
- Place the Kepnut back on the stud after the ground strap is removed to avoid misplacement.
- Secure the dangling end of the ground strap to the door or chassis with tape.

Step 2 Push the outer side of the handles on the fan-tray assembly to expose the handles.

Step 3 Pull the handles and slide the fan-tray assembly one inch (25.4 mm) out of the shelf assembly and wait until the fans stop.

Step 4 When the fans have stopped, pull the fan-tray assembly completely out of the shelf assembly.

Step 5 Gently remove the air filter from the shelf assembly. Be careful not to dislodge any dust that could have collected on the filter.

Step 6 Visually inspect the air filter material for dirt and dust.

Step 7 If the air filter has a concentration of dirt and dust, replace the unclean air filter with a clean air filter and reinsert the fan-tray assembly.

Step 8 If the air filter should be installed in the external filter brackets, slide the air filter all the way to the back of the brackets to complete the procedure.

Step 9 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 filter until the fan tray fits correctly.

Note On a powered-up NCS system, the fans start immediately after the fan-tray assembly is correctly inserted.

Step 10 To verify that the tray is plugged into the backplane, ensure that the LCD on the front of the fan-tray assembly is activated and displays node information.

Step 11 Rotate the retractable handles back into their compartments.

Step 12 Replace the door and reattach the ground strap.

Remove and Reinsert a Fan-Tray Assembly

Procedure

Step 1 Use the retractable handles embedded in the front of the fan-tray assembly to pull it forward several inches.

Step 2 Push the fan-tray assembly firmly back into the NCS system.

Step 3 Close the retractable handles.

Replace the Fan-Tray Assembly

Before you begin

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 NCS system. 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.

Procedure

Step 1 Open the front door of the shelf assembly by completing the following steps. If the shelf assembly does not have a front door, continue with Step 3, on page 319.

a) Open the front door lock.
b) Press the door button to release the latch.
c) Swing the door open.

Step 2 Remove the front door (optional):

a) Detach the ground strap from either the door or the chassis by removing one of the Kepnuts.
b) Place the Kepnut back on the stud after the ground strap is removed to avoid misplacement.
c) Secure the dangling end of the ground strap to the door or chassis with tape.

Step 3 Push the outer side of the handles on the fan-tray assembly to expose the handles.

Step 4 Fold out the retractable handles at the outside edges of the fan tray.

Step 5 Pull the handles and slide the fan-tray assembly one inch (25.4 mm) out of the shelf assembly and wait until the fans stop.

Step 6 When the fans have stopped, pull the fan-tray assembly completely out of the shelf assembly.

Step 7 If you are replacing the fan-tray air filter and it is installed beneath the fan-tray assembly, slide the existing air filter out of the shelf assembly and replace it before replacing the fan-tray assembly.

If you are replacing the fan-tray air filter and it is installed in the external bottom bracket, you can slide the existing air filter out of the bracket and replace it at anytime. For more information on the fan-tray air filter, see the Inspect, Clean, and Replace the Air Filter, on page 316 section.

Step 8 Slide the new fan tray into the shelf assembly until the electrical plug at the rear of the tray plugs into the corresponding receptacle on the backplane.

Step 9 To verify that the tray has plugged into the backplane, check that the LCD on the front of the fan tray is activated.

Step 10 If you replace the door, be sure to reattach the ground strap.

Interface Procedures

This section includes instructions for replacing an AIP.

Replace the Alarm Interface Panel

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.

Before you begin

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 control card can cause a service disruption of less then 50 ms to OC-N or DS-N traffic. Resetting the active control card 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 system. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

You need a #2 Phillips screwdriver.

Procedure

Step 1 Ensure that all nodes in the affected network are running the same software version before replacing the AIP and repairing circuits:

a) In network view, click the **Maintenance** > **Software** tabs. The working software version for each node is listed in the Working Version column.

b) If you need to upgrade the software on a node, refer to the release-specific software upgrade document for procedures. No hardware should be changed or circuit repair performed until after the software upgrade is complete. If you do not need to upgrade software or have completed the software upgrade, proceed to Step 2, on page 320.

Step 2 Record the MAC address of the old AIP:

a) Log into the node where you are replacing the AIP. For login procedures, refer to the Connect the PC and Log into the GUI chapter in the Configuration guide.

b) In node view, click the **Provisioning** > **Network** > **General** tabs.

c) Record the MAC address.

Step 3 Call Cisco TAC (1 800 553-2447) for assistance in replacing the AIP and maintaining the original MAC address.

Step 4 Unscrew the five screws that hold the lower backplane cover in place.

Step 5 Grip the lower backplane cover and gently pull it away from the backplane.

Step 6 Unscrew the two screws that hold the AIP cover in place.

Step 7 Grip the cover and gently pull away from the backplane.

Note On the 15454-SA-HD (P/N: 800-24848), 15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1 (P/N: 800-07149) shelves the AIP cover is clear plastic. On the 15454-SA-ANSI shelf (P/N: 800-19857), the AIP cover is metal.

Step 8 Grip the AIP and gently pull it away from the backplane.

Step 9 Disconnect the fan-tray assembly power cable from the AIP.

Step 10 Set the old AIP aside for return to Cisco.

Caution The type of shelf the AIP resides in determines the version of AIP that should replace the failed AIP. The 15454-SA-ANSI shelf (P/N: 800-19857) and 15454-SA-HD (P/N: 800-24848) currently use the 5A AIP, (P/N: 73-7665-01). The 15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1 (P/N: 800-07149) shelves and earlier use the 2A AIP (P/N: 73-5262-01).

Caution Do not put a 2A AIP (P/N: 73-5262-01) into a 15454-SA-ANSI (P/N: 800-19857) or 15454-SA-HD (P/N: 800-24848) shelf; doing so causes a blown fuse on the AIP.

Step 11 Attach the fan-tray assembly power cable to the new AIP.

Step 12 Place the new AIP on the backplane by plugging the panel into the backplane using the DIN connector.

Step 13 Replace the AIP cover over the AIP and secure the cover with the two screws.

Step 14 Replace the lower backplane cover and secure the cover with the five screws.

Step 15 In node view, click the **Provisioning** > **Network** tabs.

Caution Cisco recommends control card resets be performed in a maintenance window to avoid any potential service disruptions.

Step 16 Reset the standby control card:

a) Right-click the standby control card and choose **Reset Card**.

b) Click **Yes** in the Resetting Card dialog box. As the card resets, a loading (Ldg) indication appears on the card in CTC.The reset takes approximately five minutes. Do not perform any other steps until the reset is complete.

Step 17 Reset the active control card:

a) Right click the active control card and choose **Reset Card**.

b) Click **Yes** in the Resetting Card dialog box. As the card resets, a Ldg indication appears on the card in CTC. The reset takes approximately five minutes and CTC loses its connection with the node.

Step 18 From the **File** drop-down list, choose Exit to exit the CTC session.

Step 19 Log back into the node. At the Login dialog box, choose **(None)** from the Additional Nodes drop-down list.

Step 20 Record the new MAC address:

a) In node view, click the **Provisioning** > **Network** > **General** tabs.

b) Record the MAC address.

Step 21 In node view, click the **Circuits** tab. Note that all circuits listed are PARTIAL.

Step 22 In node view, choose **Repair Circuits** from the **Tools** drop-down list. The Circuit Repair dialog box appears.

Step 23 Read the instructions in the Circuit Repair dialog box. If all the steps in the dialog box have been completed, click **Next**. Ensure that you have the old and new MAC addresses.

Step 24 The Node MAC Addresses dialog box appears. Complete the following steps:

a) From the Node drop-down list, choose the name of the node where you replaced the AIP.

b) In the Old MAC Address field, enter the old MAC address that was recorded in Step 2, on page 320.

c) Click **Next**.

Step 25 The Repair Circuits dialog box appears. Read the information in the dialog box and click **Finish**.

The CTC session freezes until all circuits are repaired. Circuit repair can take up to five minutes or more depending on the number of circuits provisioned on it.

When the circuit repair is complete, the Circuits Repaired dialog box appears.

Step 26 Click **OK**.

Step 27 In the node view of the new node, click the **Circuits** tab. Note that all circuits listed are DISCOVERED. If all circuits listed do not have a DISCOVERED status, call the Cisco TAC (1 800 553-2447) to open a Return Material Authorization (RMA).