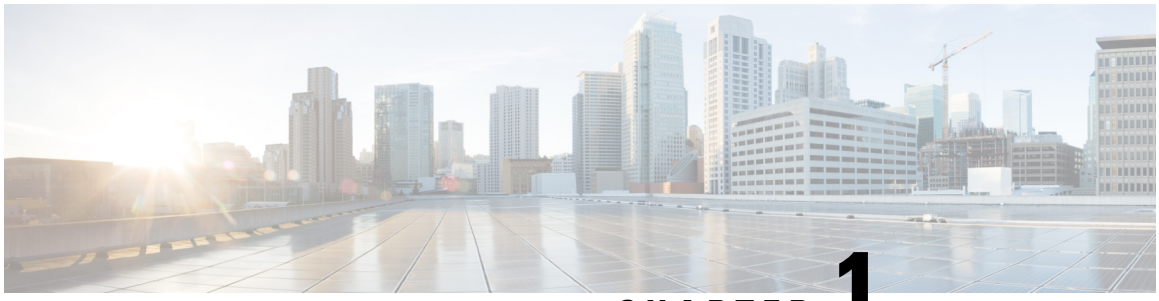
# Cisco NCS 2000 Series SVO Troubleshooting Guide, Release 12.2

**First Published:** 2021-04-29

**Last Modified:** 2021-04-29

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CHAPTER 1

# Alarms

This chapter provides description, severity, and troubleshooting procedure for each commonly encountered alarm.

# Fault Monitoring

The Fault Monitoring pane provides an alarm summary for all alarms and conditions that are encountered. It displays the number of Critical (CR), Major (MJ), Minor (MN), Warnings (W), and Non-applicable (NA) alarms. It displays the alarms, transient conditions, and historical alarms that are related to chassis, passive devices, pluggables, line cards, amplifier cards, and control cards. You can also create custom alarm profiles and apply them on the node using this pane.

# Display Alarms

Use this task to display the alarms raised on a rack, chassis, or card.

### Before you begin

Log into the SVO Web Interface, on page 15

### Procedure

**Step 1** Perform this step, as needed.

a) To view the alarms raised on the specific rack, perform these steps:

1. Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

   The SVO Topology page appears.

2. Click the rack in the left panel.

   The rack view appears.

   From R12.0.1 onwards, the alarm severities are displayed with alarm icons that are based on the alarm severity colors along with alarms. The expanded rack view on the left panel displays the highest alarm severity for each chassis.

3. Click the **Alarms** tab.

   In the rack view, the alarms that are related to the rack are displayed. The alarms with several severities such as Critical, Major, Minor, and Not Alarmed are displayed. The alarm severities are indicated by different colors.

b) To view the alarms raised on the specific chassis, perform these steps:

1. Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

   The SVO Topology page appears.

2. Click the rack in the left panel.

   The rack view appears.

3. Left-click the chassis and select **Open**.

   The chassis view appears.

4. Click the **Alarms** tab.

   In the chassis view, the alarms that are related to chassis and ancillaries of NCS 2006 and NCS 2015, control cards, line cards, amplifier cards, and pluggables are displayed. The alarms with several severities such as Critical, Major, Minor, and Not Alarmed are displayed. The alarm severities are indicated by different colors.

   In the chassis view, you can view borders with maximum alarm severity. For example, if critical alarms are raised for ports, then the borders of the ports section along with the chassis display with the designated alarm severity color.

c) To view the alarms raised on the specific card, perform these steps:

1. Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

   The SVO Topology page appears.

2. Click the rack in the left panel.

   The rack view appears.

3. Left-click the chassis and select **Open**.

   The chassis view appears.

4. Left-click the card and select **Open Card**.

   The card view appears.

5. Click the **Alarms** tab.

   In the card view, the alarms that are related to the card are displayed. The alarms with several severities such as Critical, Major, Minor, and Not Alarmed are displayed. The alarm severities are indicated by different colors. The color of the card is the same as that of the highest severity alarm.

**Step 2** Click the **Auto delete cleared alarms** check box to automatically delete the cleared alarms.

**Step 3** Click **Export to Excel** to export the alarms to the excel sheet.

**Step 4** From the **Severity** drop-down list, choose a severity to filter the alarms based on severity.

# Display Transient Conditions

Use this task to display the transient conditions raised on a rack, chassis, or card.

### Before you begin

Log into the SVO Web Interface, on page 15

### Procedure

**Step 1** Perform this step, as needed.

a) To view the transient conditions raised on the specific rack, perform these steps:

1. Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

   The SVO Topology page appears.

2. Click the rack in the left panel.

   The rack view appears.

3. Click the **Conditions** tab.

b) To view the transient conditions raised on the specific chassis, perform these steps:

1. Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

   The SVO Topology page appears.

2. Click the rack in the left panel.

   The rack view appears.

3. Left-click the chassis and select **Open**.

   The chassis view appears.

4. Click the **Conditions** tab.

c) To view the transient conditions raised on the specific card, perform these steps:

1. Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

   The SVO Topology page appears.

2. Click the rack in the left panel.

   The rack view appears.

3. Left-click the chassis and select **Open**.

The chassis view appears.

4. Left-click the card and select **Open Card**.

   The card view appears.

5. Click the **Conditions** tab.

**Step 2** Click **Fetch Conditions** to display the transient conditions.

**Step 3** Click **Export to Excel** to export the transient conditions to the excel sheet.

# Display Historical Alarms

Use this task to display the historical alarms raised on a rack, chassis, or card.

### Before you begin

Log into the SVO Web Interface, on page 15

### Procedure

**Step 1** Perform this step, as needed.

a) To view the historical alarms raised on the specific rack, perform these steps:

1. Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

   The SVO Topology page appears.

2. Click the rack in the left panel.

   The rack view appears.

3. Click the **History** tab.

b) To view the historical alarms raised on the specific chassis, perform these steps:

1. Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

   The SVO Topology page appears.

2. Click the rack in the left panel.

   The rack view appears.

3. Left-click the chassis and select **Open**.

   The chassis view appears.

4. Click the **History** tab.

c) To view the historical alarms raised on the specific card, perform these steps:

1. Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

The SVO Topology page appears.

2. Click the rack in the left panel.

   The rack view appears.

3. Left-click the chassis and select **Open**.

   The chassis view appears.

4. Left-click the card and select **Open Card**.

   The card view appears.

5. Click the **History** tab.

**Step 2** Click **Export to Excel** to export the historical alarms to the excel sheet.

**Step 3** From the **Severity** drop-down list, choose a severity to filter the alarms based on severity.

# Sensor Alarms Supported by NCS2K-SVO-K9 Card

The following sensor alarms are supported by the NCS2K-SVO-9K card. All the sensor alarms are cleared when the sensor value reverts to normal or within the expected range. The default severity of all these alarms is Minor (MN), Non-Service-Affecting (NSA).

- SENSOR_HIGH_0_6V_CPU_B
- SENSOR_LOW_0_6V_CPU_B
- SENSOR_HIGH_1_2V_CPU
- SENSOR_LOW_1_2V_CPU
- SENSOR_HIGH_1_5V_CPU
- SENSOR_LOW_1_5V_CPU
- SENSOR_HIGH_1_7V_CPU
- SENSOR_LOW_1_7V_CPU
- SENSOR_HIGH_3_3V_CPU
- SENSOR_LOW_3_3V_CPU
- SENSOR_HIGH_1_05V_CPU
- SENSOR_LOW_1_05V_CPU
- SENSOR_HIGH_1_82V_CPU
- SENSOR_LOW_1_82V_CPU
- SENSOR_HIGH_1_3V_CPU
- SENSOR_LOW_1_3V_CPU

- SENSOR_HIGH_0_6V_CPU_A
- SENSOR_LOW_0_6V_CPU_A
- SENSOR_HIGH_5_0V_STDBY
- SENSOR_LOW_5_0V_STDBY
- SENSOR_HIGH_3_3V_STDBY
- SENSOR_LOW_3_3V_STDBY
- SENSOR_HIGH_3_3V
- SENSOR_LOW_3_3V
- SENSOR_HIGH_2_5V
- SENSOR_LOW_2_5V
- SENSOR_HIGH_1_8V
- SENSOR_LOW_1_8V
- SENSOR_HIGH_1_2V
- SENSOR_LOW_1_2V
- SENSOR_HIGH_1_0V_PHY
- SENSOR_LOW_1_0V_PHY
- SENSOR_HIGH_1_0V
- SENSOR_LOW_1_0V
- SENSOR_HIGH_BP_48V
- SENSOR_LOW_BP_48V
- SENSOR_HIGH_HOTSPOT2
- SENSOR_LOW_HOTSPOT2
- SENSOR_HIGH_HOTSPOT1
- SENSOR_LOW_HOTSPOT1
- SENSOR_HIGH_INLET_AIR
- SENSOR_LOW_INLET_AIR
- SENSOR_HIGH_OUTLER_AIR
- OUTLER_AIR_SENSOR_LOW
- SENSOR_HIGH_ETH_SWITCH_TEMP
- SENSOR_LOW_ETH_SWITCH_TEMP
- SENSOR_HIGH_CPU_TEMP
- SENSOR_LOW_CPU_TEMP

- SENSOR_HIGH_DDR_CH0_TEMP
- SENSOR_LOW_DDR_CH0_TEMP
- SENSOR_HIGH_DDR_CH1_TEMP
- SENSOR_LOW_DDR_CH1_TEMP

# Troubleshooting MXP, TXP, XP, or ADM-10G Circuit Paths With Loopbacks

Facility loopbacks and terminal loopbacks are often used together to test the circuit path through the network or to logically isolate a fault. Performing a loopback test at each point along the circuit path systematically isolates possible points of failure. MXP, TXP, XP, or ADM-10G card loopback tests differ from other testing in that loopback testing does not require circuit creation. MXP, TXP, and XP client ports are statically mapped to the trunk ports so no signal needs to traverse the cross-connect card (in a circuit) to test the loopback.

You can use these procedures on transponder cards (TXP, TXPP, ADM-10G), muxponder, or xponder cards (MXP, MXPP, XP, ADM-10G) cards. The example in this section tests an MXP or TXP circuit on a three-node bidirectional line switched ring (BLSR) or multiplex section-shared protection ring (MS-SPRing). Using a series of facility loopbacks and terminal loopbacks, the example scenario traces the circuit path, tests the possible failure points, and eliminates them. The logical progression contains six network test procedures:

**Note** MXP, TXP, XP, or ADM-10G card client ports do not appear when you click the **Maintenance** > **Loopback** tab unless they have been provisioned. Do this in the card view by clicking the **Provisioning** > **Pluggable** Port Modules tab.

**Note** The test sequence for your circuits will differ according to the type of circuit and network topology.

1. A facility loopback on the source-node MXP, TXP, XP, or ADM-10G port
2. A terminal loopback on the source-node MXP, TXP, XP, or ADM-10G port
3. A facility loopback on the intermediate-node MXP, TXP, XP, or ADM-10G port
4. A terminal loopback on the intermediate-node MXP, TXP, XP, or ADM-10G port
5. A facility loopback on the destination-node MXP, TXP, XP, or ADM-10G port
6. A terminal loopback on the destination-node MXP, TXP, XP, or ADM-10G port

**Note** Facility and terminal loopback tests require on-site personnel.

# Log into the SVO Web Interface

Use this task to log into the SVO web interface (SVO instance).

### Procedure

**Step 1** In the browser URL field, enter the IP address of the SVO instance.

The IP address to be used is the management IP address that is configured in the Create an SVO Instance, on page 15 task.

The SVO login page appears.

**Step 2** Enter the username and password.

**Note** Use the credentials (configured in the Create an SVO Instance, on page 15 task) to log into a SVO instance.

**Step 3** Click **Login**.

# Create an SVO Instance

Use this task to configure an SVO instance.

### Before you begin

Log into the Cisco SVO Admin Plane, on page 16

### Procedure

**Step 1** Click the + button at the top-left of the SVO Instances page.

The SVO Instance Configuration page appears.

**Step 2** In the **General Info** area, perform these steps:

a) Enter the name for the new SVO instance in the **Name** field.

The name is mandatory and must be unique among the SVO instances managed by the admin plane. It can contain a minimum of two characters and a maximum of 64 characters. It can include numbers, uppercase letters, lowercase letters, dashes (-), or underscores (_).

b) Choose the version from the **Software Version** drop-down list.

c) Choose the type of the SVO instance from the **TDM Terminology** drop-down list.

The two options are ANSI and ETSI.

d) Choose the label of the SVO instance from the **Type** drop-down list.

The four options are ROADM, OLA, DGE, and TXP. The type indicates the role of the SVO instance in the network.

**Note** When Type is selected, a default value for memory size is displayed in the **Reserved Memory GB** field.

e) Choose the memory size to be allocated to the SVO instance from the **Reserved Memory GB** field.

The user is allowed to reserve the SVO container memory in steps of 1GB. This value is visible and summarized at server level in the SVO instances table.

**Step 3** In the **Admin User** area, perform these steps:

a) Enter the username in the **Username** field.

The values "admin," "oper," "private," or, "public" cannot be used as the admin username.

b) Enter the password in the **Password** field.

The password must be a minimum of eight characters. The password must contain at least an uppercase letter a number, and a special character. The special characters supported are ! $ % ^ ( ) [ ] _ - ~ { } . +

c) Enter the password again in the **Retype Password** field.

**Step 4** In the **Management Network** area, the system suggests the management subnets to be used in the **IPv4 Address** or the **IPv6 Address** fields, depending on the type of addressing defined during the installation. The system checks for constraints defined in the network configuration file and ensures that the IP addresses that are assigned are not in use.

a) Enter the IPv4 Address in the **IPv4 Address** field in a SVO card model.

or

b) Enter the IPv4 or the IPv6 Address in the **IPv4 Address** or **IPv6 Address** field respectively in an external server model.

**Step 5** Click **Create**.

**Step 6** A message is displayed indicating the creation of the SVO instance.

**Step 7** Click **OK**.

The SVO Instances page appears. The table displays the new SVO instance.

The SVO instance can now be accessed through a web browser.

# Log into the Cisco SVO Admin Plane

Use this task to log in to the Cisco SVO admin plane.

### Procedure

**Step 1** In the browser URL field, enter the IP address of the admin plane (https://*IP_address*/login).

The login page appears.

**Step 2** Enter the username and password.

In an SVO card system, only the superuser is allowed to log in to the Cisco SVO admin plane.

**Step 3** Click **Login**.

The SVO Instances page is displayed.

# 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

Resource Type: CARD

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

Resource Type: OCn, STMn

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).

# ALS

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

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

Resource Type: OPT, OCH, ETH

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

Resource Type: OPT, OCH

The Automatic Laser Shutdown (ALS) condition occurs when an 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 chassis view, click the slot that contains the card, and click **Open Card**.

The card view appears.

**Step 2** Click **Maintenance** > **Optical Safety**.

**Step 3** In the **ALS Mode** column, choose **ALS-Disabled** 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).

# AMPLI-INIT

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

Logical Object: AOTS

Resource Type: OPT

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**

Remove most recently created circuit using EPNM.

If the condition does not clear, log into the Technical 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-CORR-SKIPPED

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

Logical Objects: AOTS, OCH, OMS, OTS

Resource Type: OPT

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

Resource Type: OPT

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, delete the circuit using EPNM.

If the condition does not clear, log into the Technical 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

Resource Type: 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

Resource Type: OPT

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

Resource Type: OPT

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 OPT-AMP-C 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).

# APS-NO-RESPONSE

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

Logical Object: ODU

Resource Type: ODUk

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

Resource Type: ODUk

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

Resource Type: ALL

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

# 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

Resource Type: ALL

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

**Before you begin**

**Procedure**

**Step 1** In chassis view, click the slot that contains the card, and click **Open Card**.

The card view appears.

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

**Step 3** In the Loopback Type drop-down list, determine whether any port row shows a state other than Disabled.

**Step 4** If a row contains another state besides Disabled, click in the column cell to display the drop-down list and select Disabled.

**Step 5** Click **Apply**.

**Step 6** Click the **Provisioning** > **Pluggable Port Modules** tabs.

**Step 7** In the Admin State column, determine whether any port row shows an administrative state other than IS, for example, OOS,MT.

**Step 8** 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.

# 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.

# AUTH-EC

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

Logical Objects: OTU

Resource Type: ODUk

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).

# AUTOLSROFF

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

Logical Object: STMN

Resource Type: OCn, STMn

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

On the 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

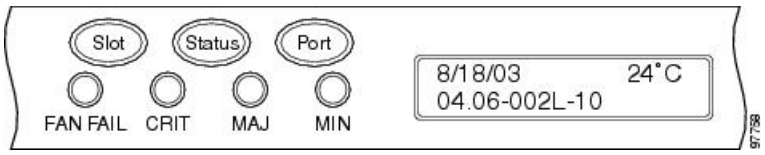
# Clear the AUTOLSROFF Alarm

**Procedure**

**Step 1** View the temperature displayed on the NCS LCD front panel (Figure 3: Shelf LCD Panel, on page 76).

Figure 3: Shelf LCD Panel, on page 76 shows the shelf LCD panel.

***Figure 1: Shelf LCD Panel***




**Step 2** If the temperature of the shelf exceeds 194 degrees F (90 degrees C), the alarm should clear if you solve the NCS temperature problem.

**Step 3** If the temperature of the shelf is under 194 degrees F (90 degrees C), the HITEMP alarm is not the cause of the AUTOLSROFF alarm. Complete the Physically Replace a Card, on page 188 procedure for the OC-192 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.

# AUTH-EC

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

Logical Objects: OTU

Resource Type: ODUk

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).

# AUTOLSROFF

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

Logical Object: STMN

Resource Type: OCn, STMn

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

On the 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

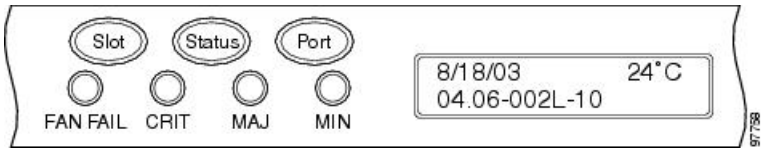
# Clear the AUTOLSROFF Alarm

### Procedure

**Step 1** View the temperature displayed on the NCS LCD front panel (Figure 3: Shelf LCD Panel, on page 76).

Figure 3: Shelf LCD Panel, on page 76 shows the shelf LCD panel.

***Figure 2: Shelf LCD Panel***




**Step 2** If the temperature of the shelf exceeds 194 degrees F (90 degrees C), the alarm should clear if you solve the NCS temperature problem.

**Step 3** If the temperature of the shelf is under 194 degrees F (90 degrees C), the HITEMP alarm is not the cause of the AUTOLSROFF alarm. Complete the Physically Replace a Card, on page 188 procedure for the OC-192 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.

# AUTORESET

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

Logical Object: EQPT

Resource Type: CARD

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 188 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).

# AWG-DEG

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

Logical Object: OTS

Resource Type: OPT

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 188 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

Resource Type: OPT

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 188 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

Resource Type: OPT

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 30 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

Resource Type: OPT

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

Resource Type: 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

Resource Type: 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.

# BKUPMEMP

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

Logical Object: EQPT

Resource Type: CARD, USB_FLASH

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

- Flash manager fails to format a flash partition.

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

**Caution** A software update on a standby control card can take up to 30 minutes.

## Clear the BKUPMEMP Alarm

**Procedure**

**Step 1** Determine the control card that has the alarm.

**Step 2** Reset the control card where the alarm is raised using the procedure Reset a Card, on page 186

**Step 3** If the control card you reset does not reboot successfully, or the alarm has not cleared, call Cisco TAC (1 800 553-2447). If the Cisco TAC technician tells you to reset the card, complete the Remove and Reinsert (Reseat) the Standby Control Card, on page 186 procedure. If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the Physically Replace a Card, on page 188 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

# BP-LPBKFACILITY

Default Severity: Not alarmed (NA)

Logical Object: EQPT

Resource Type: CARD

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** In chassis view, click the slot that contains the 100G-LC-C or 10x10G-LC card, and click **Open Card**.

The card view appears.

**Step 2** Click the **Provisioning > Pluggable Port Modules** tab.

Only the admin state of each port can be changed.

**Step 3** Click on the card port that is in Unlocked state in the Admin State column, and change the state to locked, Maintenance.

**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).

# BP-LPBKTERMINAL

Default Severity: Not alarmed (NA)

Logical Object: EQPT

Resource Type: CARD

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** In chassis view, click the slot that contains the 100G-LC-C or 10x10G-LC card, and click **Open Card**.

The card view appears.

**Step 2** Click the **Provisioning > Pluggable Port Modules** tab.

Only the admin state of each port can be changed.

**Step 3** Click on the card port that is in Unlocked state in the Admin State column, and change the state to locked, Maintenance.

**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).

# CARLOSS (EQPT)

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

Logical Object: EQPT

Resource Type: ETH

A Carrier Loss on the LAN Equipment alarm generally occurs on MXP, TXP cards when the system and the workstation hosting SVO 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 SVO 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.

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

# CARLOSS (FC)

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

Logical Object: FC

Resource Type: ETH

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.

# CARLOSS (GE)

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

Logical Object: GE

Resource Type: ETH

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) In node view (single-shelf mode) or shelf view (multishelf mode), double-click the card to open the card view.

The card view appears.

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

c) View the Pluggable Port Modules area port listing in the **Actual Equipment Type** column and compare this with the client equipment. If no 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.

d) 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

Resource Type: ETH

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.

# CARLOSS (TRUNK)

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

Logical Object: TRUNK

Resource Type: ETH

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.

# CASETEMP-DEG

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

Logical Object: AOTS

Resource Type: OPT

**Note** For specific temperature and environmental information about each DWDM card, refer to the .

## 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 189 procedure.

**Step 2** If the filter is clean, complete the Remove and Reinsert a Fan-Tray Assembly, on page 190 procedure.

**Step 3** If the fan does not run or the alarm persists, complete the Replace the Fan-Tray Assembly, on page 190 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)

Resource Type: OCH

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.

# CHAN-PWR-THRESHOLD-CHECK

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

Logical Objects: OTS

Resource Type: OPT

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

Resource Type: CARD

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 187 procedure.

**Step 3** If the condition does not clear, complete the Physically Replace a Card, on page 188 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).

# COMM-FAIL

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

Logical Object: EQPT

Resource Type: CARD

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 187 procedure for the reporting card.

**Step 2** If the alarm does not clear, complete the Physically Replace a Card, on page 188 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

Resource Type: CARD

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 28
  - MANRESET , on page 106
  - CLDRESTART , on page 39
  - PROV-MISMATCH, on page 145

## 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 29
- Clear the CLDRESTART Condition, on page 39

If the condition does not clear, log into the Technical 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-DISABLED

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

Logical Object: EQPT

Resource Type: CARD

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

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

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

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

CONTBUS-DISABLED overrides the IMPROPRMVL alarm during the one-minute wait period, but afterward IMPROPRMVL can be raised because it is no longer suppressed. IMPROPRMVL is raised after CONTBUS-DISABLED clears if the card is in the node database. If CONTBUS-DISABLED has cleared but IMPROPRMVL is still active, inserting a card will clear the IMPROPRMVL alarm.

## Clear the CONTBUS-DISABLED Alarm

**Procedure**

If the IMPROPRMVL alarm is raised, complete the Physically Replace a Card, on page 188 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).

# CONTBUS-IO-A

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

Logical Object: EQPT

Resource Type: CARD

A TCCA to Shelf A Slot Communication Failure alarm occurs when the active Slot 7 TCC2/TCC2P/TCC3 (TCC A) has lost communication with another card in the shelf.

The CONTBUS-IO-A alarm can appear briefly when the NCS switches to the protect TCC2/TCC2P/TCC3. In the case of a TCC2/TCC2P/TCC3 protection switch, the alarm clears after the other cards establish communication with the newly active TCC2/TCC2P/TCC3. If the alarm persists, the problem lies with the physical path of communication from the TCC2/TCC2P/TCC3 to the reporting card. The physical path of communication includes the TCC2/TCC2P/TCC3, the other card, and the backplane.

## Clear the CONTBUS-IO-A Alarm

**Procedure**

**Step 1** Determine the control card that has the alarm.

**Step 2** Reset the control card where the alarm is raised using the procedure Reset a Card, on page 186

**Step 3** If the reset does not clear the alarm, complete the Remove and Reinsert (Reseat) Any Card , on page 187 procedure for the reporting card.

**Caution** Always use the supplied electrostatic discharge wristband when working with a powered NCS. Plug the wristband cable into the ESD jack located 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).

If the Technical Support technician tells you to reseat the card, complete the Remove and Reinsert (Reseat) the Standby Control Card, on page 186 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 188 procedure.

# CONTBUS-IO-B

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

Logical Object: EQPT

Resource Type: CARD

A TCC B to Shelf Communication Failure alarm occurs when the active Slot 11 TCC2/TCC2P/TCC3 (TCC B) has lost communication with another card in the shelf.

The CONTBUS-IO-B alarm could appear briefly when the NCS switches to the protect TCC2/TCC2P/TCC3. In the case of a TCC2/TCC2P/TCC3 protection switch, the alarm clears after the other cards establish communication with the newly active TCC2/TCC2P/TCC3. If the alarm persists, the problem lies with the physical path of communication from the TCC2/TCC2P/TCC3 to the reporting card. The physical path of communication includes the TCC2/TCC2P/TCC3, the other card, and the backplane.

## Clear the CONTBUS-IO-B Alarm

**Procedure**

**Step 1** Determine the control card that has the alarm.

**Step 2** Reset the control card where the alarm is raised using the procedure Reset a Card, on page 186

**Step 3** If the reset does not clear the alarm, complete the Remove and Reinsert (Reseat) Any Card , on page 187 procedure for the reporting card.

**Caution** Always use the supplied electrostatic discharge wristband when working with a powered NCS. Plug the wristband cable into the ESD jack located 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).

If the Technical Support technician tells you to reseat the card, complete the Remove and Reinsert (Reseat) the Standby Control Card, on page 186 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 188 procedure.

# COOL-MISM

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

Logical Object: FAN

Resource Type: FAN_TRAY

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

**Procedure**

**Step 1** Click the hamburger icon at the top-left of the page, and select **Device Configuration**.

**Step 2** Click the **Configuration** > **Device Settings** tabs.

**Step 3** Choose the control from the **Cooling Profile Control** drop-downlist.

**Step 4** Click **Apply**.

A confirmation message appears.

**Step 5** 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).

# DATAFLT

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

Logical Object: NE

Resource Type: NE

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

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

## Clear the DATAFLT Alarm

**Procedure**

Complete the Reset a Card, on page 186 procedure, and rebbot 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).

# DBOSYNC

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

Logical Object: NE

Resource Type: 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.

# DCU-LOSS-FAIL

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

Logical Object: OTS

Resource Type: OPT

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).

# DSP-COMM-FAIL

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

Logical Object: TRUNK

Resource Type: CARD

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 46 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

Resource Type: CARD

The DSP Failure alarm indicates that a DSP-COMM-FAIL , on page 45, 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 188 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

Resource Type: 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, SVO 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 SVO 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** Click the hamburger icon at the top-left of the page, and select **Device Configuration**.

**Step 2** Click the **Configuration** > **IPv4 Settings** tabs.

**Step 3** Click **Edit** against the alarmed node.

**Step 4** In the **IP Address** field, change the IP address to a unique number.

**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).

# DUP-NODENAME

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

Logical Object: NE

Resource Type: NE

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

# DUP-SHELF-ID

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

Logical Object: SHELF

Resource Type: 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.

# EHIBATVG

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

Logical Object: PWR

Resource Type: 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

Resource Type: 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.

# ENC-CERT-EXP

Default Severity: Minor

Logical Object: NearEnd

Resource Type: ODUK

The Encryption Certificate Expired alarm is raised on line cards such as 400G-XP-LC, WSE, and MR-MXP when the SUDI 2029 MIC encryption certificate expires.

## Clear the ENC-CERT-EXP Alarm

**Procedure**

Perform one of the following :

- Change the encryption certificate type to LSC
- Disable the Encryption

- Verify if both the near-end and far-end line cards have the software package as release 11.12 and above

# EOC

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

Logical Objects: OCN, STMN, TRUNK

Resource Type: OPT, OCn, STMn

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

The SDCC consists of three bytes, D1 through D3, in the SONET overhead. The bytes convey information about operation, administration, maintenance, and provisioning (OAM&P). The NCS 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.

# EOC-E

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

Logical Objects: OCN, STMN, FE, GE

Resource Type: ETH

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.

# EPROM-SUDI-SN-MISMATCH

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

Logical Object: EQPT

Resource Type: CARD

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).

# EQPT-DEGRADE

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

Logical Objects: EQPT

Resource Type: CARD

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 188 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

Resource Type: CARD

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 187 procedure for the alarmed card

**Step 2** If the alarm does not clear, complete the Physically Replace a Card, on page 188 procedure if it is raised against a traffic card, or complete the Generic Signal and Circuit Procedures, on page 191 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

Resource Type: CARD

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 Reset a Card, on page 186procedure for the reporting card.

**Step 2** Verify that the reset is complete and error-free and that no new related alarms appear in SVO . 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 187 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 188 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

Resource Type: CARD

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

Resource Type: CARD/FAN_TRAY/ECU/LCD_FLASH/PWR

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 190 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.

# ETH-LINKLOSS

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

Logical Object: NE

Resource Type: 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

Resource Type: CARD

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).

# EXT

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

Logical Object: ENVALRM

Resource Type: 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

Resource Type: OPT, ODUk, OTUk, OCn, STMn, ETH

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 Hardware Specification 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 188 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

Resource Type: OPT, ODUk, OTUk, OCn, STMn, ETH

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 .

## 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 188 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

Resource Type: OPT, ODUk, OTUk, OCn, STMn, ETH

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 56 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

Resource Type: OPT, ODUk, OTUk, OCn, STMn, ETH

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.

# FAN

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

Logical Object: FAN

Resource Type: FAN_TRAY

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 189 procedure.

**Step 2** If the filter is clean, complete the Remove and Reinsert a Fan-Tray Assembly, on page 190 procedure.

**Step 3** If the fan does not run or the alarm persists, complete the Replace the Fan-Tray Assembly, on page 190 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.

# FC-NO-CREDITS

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

Logical Objects: Client port

Resource Type: FC

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.)

# FC-DE-NES

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

SONET Logical Object: FCMR

DWDM Logical Objects: FC, TRUNK

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

## Clear the FC-DE-NES Alarm

**Procedure**

Ensure that the FC client setup and distance extension configuration is correct.

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).

# FDI

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

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

Resource Type: OXC

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 98
- Clear the LOS (TRUNK) Alarm, on page 97
- Clear the LOS-P (OCH) Alarm, on page 99
- Clear the LOS-P (AOTS, OMS, OTS) Alarm
- Clear the LOS-P (TRUNK) Alarm, on page 102
- Clear the OPWR-LFAIL Alarm, on page 126

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

# FEED-MISMATCH

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

Logical Objects: EQPT

Resource Type: PWR

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 .

# FIBERTEMP-DEG

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

Logical Object: AOTS

Resource Type: OPT

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.

## Clear the FIBERTEMP-DEG Alarm

**Procedure**

For the alarmed card, complete the Physically Replace a Card, on page 188 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).

# FOIC Group ID Mismatch

Default Severity: Major

Logical Object: Standing

Resource Type: zrPlus

The FOIC (FlexO-SR Interface) Group ID Mismatch alarm is raised due to one of the following conditions:

- When configurations of the system are incorrect
- When unsupported trunks with the same rate are reconnected back to back

## Clear the FOIC Group ID Mismatch Alarm

**Procedure**

The alarm clears when configurations are correct or supported trunk is connected back.

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).

# FOIC-LDI-LD

Default Severity: Minor

Logical Object: Standing

Resource Type: zrPlus

The FOIC Link Degrade Indicator-Local Degrade (FOIC-LDI-LD) alarm is raised due to one of the following conditions:

- When Local Degrade Indicator CA is inserted
- When Pre-FEC degrade is detected at the near end

## Clear the FOIC-LDI-LD Alarm

**Procedure**

The FOIC Link Degrade Indicator-Local Degrade (FOIC-LDI-LD) alarm clears due to one of the following conditions:

- When Local Degrade Indicator CA is removed
- When no Pre-FEC degrade is detected at the near end

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).

# FOIC-LDI-RD

Default Severity: Minor

Logical Object: Standing

Resource Type: zrPlus

The FOIC Link Degrade Indicator-Remote Degrade (FOIC-LDI-RD) alarm is raised due to one of the following conditions:

- When Local Degrade Indicator CA is detected at the far end
- When Pre-FEC degrade is detected at the near end

## Clear the FOIC-LDI-RD Alarm

**Procedure**

The alarm clears due to one of the following conditions:

- When Local Degrade CA is not detected at the far end.
- When Pre-FEC degrade is not detected at the near end.

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).

# FOIC-LOF-LOM

Default Severity: Critical

Logical Object: Standing

Resource Type: zrPlus

The FOIC Loss of Frame-Loss of Multi-frame (FOIC-LOF-LOM) alarm is raised due to one of the following conditions:

- High FEC error due to very low OSNR on the trunk Side
- Out of range of the OSNR
- Misconstructed or different modulation

## Clear the FOIC-LOF-LOM Alarm

**Procedure**

The alarm clears due to one of the following conditions:

- No High FEC error due to very low OSNR on the trunk Side
- The OSNR is not out of range
- No misconstructed or different modulation

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).

# FOIC-LOL

Default Severity: Critical

Logical Object: Standing

Resource Type: zrPlus

The FOIC Loss of Lock alarm is raised due to one of the following:

- High FEC error due to very low OSNR on the Trunk side
- Out of range of the OSNR
- Misconstructed or different modulation

## Clear the FOIC-LOL Alarm

**Procedure**

The alarm clears when clearing the HIGH FEC error due to very low OSNR on the trunk side or out of range of the OSNR or misconstructed or different Modulation.

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).

# FOIC-LOM

Default Severity: Critical

Logical Object: Standing

Resource Type: zrPlus

The FOIC Loss of Multi-frame alarm is raised due to one of the following:

- High FEC error due to very low OSNR on the Trunk side
- Out of range of the OSNR
- Misconstructed or different Modulation

## Clear the FOIC-LOM Alarm

**Procedure**

The alarm clears after clearing the HIGH FEC error due to very low OSNR on the Trunk side or out of range of the OSNR or misconstructed or different Modulation.

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).

# FOIC-PMM

Default Severity: Minor

Logical Object: Standing

Resource Type: zrPlus

The FOIC Phy Map Mismatch (FOIC-PMM) alarm is raised due to one of the following conditions:

- Misconfiguration of the system.
- When unsupported trunks with the same rate are reconnected back to back.

## Clear the FOIC-PMM Alarm

**Procedure**

The alarm clears due to correct configuration or when the supported Trunk is connected back.

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).

# FOIC-RPF

Default Severity: Minor

Logical Object: Standing

Resource Type: zrPlus

The FOIC Remote Phy Fault (FOIC-RPF) alarm is raised to inform the far-end node about the locally detected failure of the PHY.

## Clear the FOIC-RPF Alarm

**Procedure**

The alarm clears when clearing the locally detected failure of the PHY.

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).

# FOIC-TIM

Default Severity: Critical

Logical Object: Standing

Resource Type: zrPlus

The FOIC Trail Trace Identifier Mismatch (FOIC-TIM) alarm is raised when there is a mismatch between the expected TTI string that is provisioned and the received TTI string from the far-end.

## Clear the FOIC-TIM Alarm

**Procedure**

The alarm clears when there is no mismatch between the expected TTI string that is provisioned and the received TTI String from the far-end.

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).

# 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

Resource Type: OPT

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.

# FORCED-REQ-SPAN (TRUNK)

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

Logical Object: TRUNK

Resource Type: OPT

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.

# FPGA-UPGRADE-FAILED

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

Logical Object: Equipment

Resource Type: Card

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

Resource Type: NE_SYNCHREF

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

Resource Type: EXT_SYNCHREF/NE_SYNCHREF

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

Resource Type: EXT_SYNCHREF/NE_SYNCHREF

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

Resource Type: EXT_SYNCHREF/NE_SYNCHREF

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

Resource Type: NE_SYNCHREF

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 172 alarm and the SYNCSEC , on page 173 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.

# GAIN-LDEG

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

Logical Object: AOTS

Resource Type: OPT

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.

# GAIN-HDEG

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

Logical Object: AOTS

Resource Type: OPT

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 Reset a Card, on page 186procedure 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 188 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

Resource Type: OPT

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 70 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-LFAIL

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

Logical Object: AOTS

Resource Type: OPT

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.

# GAIN-NEAR-LIMIT

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

Logical Objects: AOTS

Resource Type: OPT

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 **SVO Web User Inferface** > **Node Configuration** > **ANS Parameters** > **Amplifiers**.
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).

# GFP Extension Header Mismatch

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

SONET Logical Objects: CE1000, FCMR, GFP-FAC

Resource Type: PORT/ODUK

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

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

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

## Clear the GFP Extension Header Mismatch Alarm

**Procedure**

Ensure that the vendor equipment is provisioned to send a null extension header in order to interoperate with the FC_MR-4 card. (The FC_MR-4 card always sends a null extension header.)

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).

# GFP-NO-BUFFERS

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

SONET Logical Objects: FCMR, GFP-FAC

Resource Type: PORT/ODUK

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

This alarm is raised in conjunction with the FC-NO-CREDITS. For example, if the FC-NO-CREDITS alarm is generated at an FC_MR-4 data port, a GFP-NO-BUFFERS alarm is raised at the upstream remote FC_MR-4 data port.

## Clear the GFP-NO-BUFFERS Alarm

**Procedure**

Clear the FC-NO-CREDITS Alarm.

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).

# GFP-LFD

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

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

Resource Type: PORT/ODUk

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 25 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.

# HIBATVG

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

Logical Object: PWR

Resource Type: 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-CCVOLT

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

Logical Object: BITS

Resource Type: 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.

# HITEMP

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

Logical Objects: EQPT, NE

Resource Type: CARD, NE

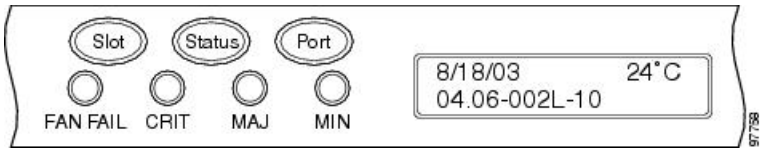
The High Temperature alarm occurs when the temperature of the ONS system is above 122 degrees F (50 degrees C).

## 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 3: Shelf LCD Panel, on page 76.

***Figure 3: 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 189 procedure.

**Step 6** If the fan does not run or the alarm persists, complete the Replace the Fan-Tray Assembly, on page 190 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.

# HLDOVRSYNC

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

Logical Object: NE-SREF

Resource Type: NE-SYNCHREF

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 68
- FSTSYNC , on page 69
- LOF (BITS) , on page 93
- LOS (BITS) , on page 95
- MANSWTOINT, on page 106
- MANSWTOPRI , on page 107
- MANSWTOSEC , on page 107
- MANSWTOTHIRD , on page 107
- SWTOPRI , on page 169
- SWTOSEC , on page 170
- SWTOTHIRD , on page 170
- SYNC-FREQ , on page 171
- SYNCPRI , on page 172
- SYNCSEC , on page 173
- SYNCTHIRD , on page 173

**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).

# I-HITEMP

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

Logical Object: NE

Resource Type: 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 76 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 76 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-FS

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

Logical Objects: PSHELF

Resource Type: 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.

# 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 79 procedure.

**Step 2** If it is raised against a 1:1 card, complete the Initiate a 1:1 Card Switch Command, on page 80 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).

# 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.

# 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 .)

**Step 2** In node view (single-shelf mode) or multishelf view (multishelf mode), click the **SVO Web Interface** > **Device Configuration** > **Devices** > **Authorization Group**.

**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

Resource Type: CARD

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).

# INVMACADR

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

Logical Objects: AIP, BP

Resource Type: BLACKPLANE

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. Complete the Reset a Card, on page 186 procedure after selecting the control card from the **Rack View** in the SVO Web Application and performing a **Soft Reset** on the card.

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).

# IPC-LASER-FAIL

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

Logical Objects: EQPT

Resource Type: CARD

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

Resource Type: OPT

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 **SVO Web Interface** > **SVO Topology** > **Rack View** > **Maintenance Tab** > **Loopback Tab**.

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

Resource Type: 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

Resource Type: 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.

# IPC-VERIFICATION-RUNNING

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

Logical Objects: EQPT

Resource Type: NE

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).

# LASER-APR

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

Logical Object: AOTS

Resource Type: OPT

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.

# LASERBIAS-FAIL

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

Logical Object: AOTS

Resource Type: OCH

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 188 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).

# LASERTEMP-DEG

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

Logical Object: AOTS

Resource Type: OCH

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 188 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

Resource Type: CARD

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 . 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

Resource Type: CARD

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

Resource Type: CARD

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

Resource Type: CARD

The License Missing (LIC-MISSING) alarm is raised when a valid license on the expires.

## Clear the LIC-MISSING Alarm

**Procedure**

Procure and install a valid license for the . 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.

# LOCAL-CERT-CHAIN-VERIFICATION-FAILED

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

Logical Object: EQPT

Resource Type: CARD

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-EXPIRED

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

Logical Object: EQPT

Resource Type: CARD

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-CERT-EXPIRING-WITHIN-30-DAYS

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

Logical Object: EQPT

Resource Type: CARD

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-CERT-ISSUED-FOR-FUTURE-DATE

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

Logical Object: EQPT

Resource Type: CARD

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-SUDI-CERT-VERIFICATION-FAILED

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

Logical Object: EQPT

Resource Type: CARD

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).

# LOCKOUT-REQ

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

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

Resource Type: OPT, ODUk, OTUk, OCn, STMn, ETH

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 92 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).

# 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.

# LO-LASERBIAS

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

Logical Objects: EQPT, OCN/STMN, PPM

Resource Type: OCH

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 188 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

Resource Type: OCH

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 46 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 Reset a Card in CTC procedure for the reporting MXP or TXP card.

**Step 2** If the alarm does not clear, complete the Physically Replace a Card, on page 188 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).

# LOF (BITS)

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

Logical Object: BITS

Resource Type: OCn

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 188 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 (BITS)

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

Logical Object: BITS

Resource Type: OCn

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 188 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).

# 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-O

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

Logical Objects: OCH, OMS, OTS

Resource Type: OPT

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, go to **SVO Web Interface** > **SVO Topology** > **Rack View** > **Select Card** > **Provisioning Tab** > **Optics Thresholds Tab**.

**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), go to **SVO Web Interface** > **Node Configuration** > **ANS Paramaters** > **Amplifiers**.

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 188 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).

# 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 70 alarm, the GAIN-HFAIL , on page 71 alarm, the GAIN-LDEG , on page 70 alarm or GAIN-LFAIL , on page 72 alarm); APC alarms (the APC-CORR-SKIPPED , on page 19 alarm and APC-OUT-OF-RANGE , on page 21 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.

# 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.

# 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 188 procedure and continue with Step 9, on page 102.

**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 100.
- 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 procedure for the card.

If the alarm does not clear, complete the Physically Replace a Card, on page 188 procedure and continue to Step 9, on page 102.

**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 102.

**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 102. If the actual power value is outside the specification range, complete the Physically Replace a Card, on page 188. 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 102.

**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.

# 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 188 procedure and continue to Step 7, on page 103.

**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 102.
- 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 procedure for the card.

**Step 3** If the alarm does not clear, complete the Physically Replace a Card, on page 188 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.

# 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, on page 14 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 193 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, on page 14 section.

# 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, on page 14 section.

# LSC-NOT-PRESENT-MIC-IN-USE

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

Logical Object: EQPT

Resource Type: CARD

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

Resource Type: 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

Resource Type: OPT, OCH

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

Resource Type: CARD

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 79 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

Resource Type: CARD

A User-Initiated Manual Reset condition occurs when you click a card on SVO web interface and choose **Soft Reset**.

**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

Resource Type: 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

Resource Type: 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

Resource Type: 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

Resource Type: 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.

# MAX-AUTH-LIST

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

Logical Object:

Resource Type: OTUk

The Max Authentication List alarm is raised when

# MEA (PPM)

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

Logical Object: PPM

Resource Type: 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**

Complete the Provision PPM and Provision Pluggable Ports procedures in the *Cisco NCS 2000 Series SVO 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.

# MEA (SHELF)

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

Logical Object: SHELF

Resource Type: 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

Resource Type: CARD

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

Resource Type: CARD

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

Resource Type: FAN_TRAY, ECU, LCD_FLASH, PWR, BACKPLANE, PPM

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).

# MT-OCHNC

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

Logical Object: OTS

Resource Type: OXC

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).

# RESOURCES-GONE

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

Logical Object: EQPT

Resource Type: CARD

The No More Resources Available (RESOURCES-GONE) alarm is raised, if any of the following condition is there:

- If the resource memory is used completely.
- When resources cannot be configured.
- When SEU FPGA bit error detected on the PTF card. To confirm the SEU FPGA bit error, connect to the respective PTF card using IOS command and check for any alarm on LEONE FPGA using the command “fmea alarm”.

## Clear the RESOURCES-GONE Alarm

**Procedure**

Perform any of the following, as appropriate:

- Find the resources that are using more memory and free up memory.
- In case of SEU FPGA bit error, reset the PTF card.

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-SHARED-CIPHERS Alarm

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

Logical Object: OTS

Resource Type: ODUk

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).

# NODE-FACTORY-MODE

Default Severity: Critical (CR)

Logical Object: NE

Resource Type: 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.

# NON-CISCO-PPM

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

Logical Object: PPM

Resource Type: 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

Resource Type: CARD

The NON-TRAF-AFFECT-SEC-UPG-REQUIRED alarm is raised when the partition of the control FPGA is not locked.

## 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).

# OCHNC-BDI

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

Logical Objects: OTS

Resource Type: OXC

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

Resource Type: OXC

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

Resource Type: OXC

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

Resource Type: OXC

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-AIS-PM

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

Logical Object: TRUNK

Resource Type: ODUk

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 118.

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

Resource Type: ODUk

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 134 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

Resource Type: ODUk

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

Resource Type: ODUk

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 117 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

Resource Type: ODUk

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 137 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

Resource Type: ODUk

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

Resource Type: ODUk

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 117, 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

Resource Type: CARD/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).

# OPU-CSF

Default Severity: Not Reported (NR)

Logical Objects: GE

Resource Type: ODU, ODUk

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).

# OPWR-HDEG

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

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

Resource Type: OPT/OXC

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 amplifier cards, click the **Provisioning** > **Optics Thresholds** tabs in card view.

**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.

**Step 7** Repeat Steps 1 to 6 for any other port on the card reporting the OPWR-HDEG alarm.

**Step 8** 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 9** Complete the Physically Replace a Card 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

Resource Type: OPT/OXC

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.

The Output Power Failure alarm occurs on an amplifier card and 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** → **Amplifier** 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 clicking the hamburger icon at the top-left of the page, and selecting the **Node Configuration** → **ANS Parameters** → **Amplifiers** tab. Validate if it is correct.

**Step 3** Set the OSC PPM mode in the TNCS-O card view by navigating to **Provisioning** → **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

Resource Type: OPT/OXC

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 124 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).

# 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 99 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 145 section. For more detailed protection switching information, refer to the Configuration guide.

**Step 9** Repeat Steps Step 1, on page 124 to Step 8, on page 125 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 188 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-LFAIL

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

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

Resource Type: OPT/OXC

The Output Power Failure alarm applies to the card transmit ports. The alarm is raised when the monitored input power crosses the low fail threshold.

## Clear the OPWR-LFAIL Alarm

**Procedure**

Complete the Clear the OPWR-HDEG Alarm, on page 124 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

Resource Type: OPT

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 126 alarm, which is also reported on the same port.

## Clear the OSRION Condition

**Procedure**

Turn the OSRI off:

a) In card view, click the **Maintenance** > **Optical Safety** tabs.
b) From the OSRI drop-down list, choose **OSRI-OFF**.

If the condition does not clear, log into the Technical 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

Resource Type: PPM

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.

# OTDR-ABSOLUTE-A-EXCEEDED-TX

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

Logical Object: EQPT

Resource Type: PPM

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.

# OTDR-ABSOLUTE-R-EXCEEDED-RX

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

Logical Object: EQPT

Resource Type: PPM

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.

# OTDR-ABSOLUTE-R-EXCEEDED-TX

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

Logical Object: EQPT

Resource Type: PPM

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.

# OTDR-BASELINE-A-EXCEEDED-RX

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

Logical Object: EQPT

Resource Type: PPM

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.

# OTDR-BASELINE-A-EXCEEDED-TX

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

Logical Objects: EQPT

Resource Type: PPM

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.

# OTDR-BASELINE-R-EXCEEDED-RX

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

Logical Objects: PPM

Resource Type: 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.

# OTDR-BASELINE-R-EXCEEDED-TX

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

Logical Object: PPM

Resource Type: 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.

# OTDR-FAST-FAR-END-IN-PROGRESS

Default Severity: Minor (MN)

Logical Object: EQUIPMENT

Resource Type: PPM

The OTDR-FAST-FAR-END-IN-PROGRESS alarm is raised when a fast scan is started on the remote side.

# OTDR-FAST-SCAN-IN-PROGRESS-RX

Default Severities: Minor (MI), Non-Service-Affecting (NSA)

Logical Object: EQPT

Resource Type: PPM

The Optical Time Domain Reflectometer (OTDR) Fast Scan In Progress Rx alarm is raised when the fast OTDR scan starts in the Rx direction.

# OTDR-FAST-SCAN-IN-PROGRESS-TX

Default Severities: Minor (MI), Non-Service-Affecting (NSA)

Logical Object: EQPT

Resource Type: PPM

The Optical Time Domain Reflectometer (OTDR) Fast Scan In Progress TX alarm is raised when the fast OTDR scan starts in the TX direction.

# OTDR-FIBER-END-NOT-DETECTED-RX

Default Severity: NA

Logical Object: EQUIPMENT

Resource Type: PPM

The OTDR-FIBER-END-NOT-DETECTED-RX alarm is raised when the OTDR module cannot return a valid fiber end.

# OTDR-FIBER-END-NOT-DETECTED-TX

Default Severity: NA

Logical Object: EQUIPMENT

Resource Type: PPM

The OTDR-FIBER-END-NOT-DETECTED-TX alarm is raised when the OTDR module cannot return a valid fiber end.

# OTDR-HYBRID-FAR-END-IN-PROGRESS

Default Severity: NA

Logical Object: EQUIPMENT

Resource Type: PPM

The OTDR-HYBRID-FAR-END-IN-PROGRESS alarm is raised when a hybrid scan is started on the remote side.

# OTDR-HYBRID-SCAN-IN-PROGRESS-RX

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

Logical Objects: PPM

Resource Type: PPM

The Optical Time Domain Reflectometer (OTDR) Hybrid Scan In Progress RX condition occurs when a hybrid OTDR scan starts in the RX direction.

# OTDR-HYBRID-SCAN-IN-PROGRESS-TX

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

Logical Objects: PPM

Resource Type: PPM

The Optical Time Domain Reflectometer (OTDR) Hybrid Scan In Progress TX condition occurs when a hybrid OTDR scan starts in the TX direction.

# OTDR-ORL-THRESHOLD-EXCEEDED-RX

Default Severity: Minor (MN)

Logical Object: EQUIPMENT

Resource Type: PPM

The OTDR-ORL-THRESHOLD-EXCEEDED-RX alarm is raised if the current ORL value crosses its threshold value.

# OTDR-ORL-THRESHOLD-EXCEEDED-TX

Default Severity: Minor (MN),

Logical Object: EQUIPMENT

Resource Type: PPM

The OTDR-ORL-THRESHOLD-EXCEEDED-TX alarm is raised if the current ORL value crosses its threshold value.

# OTDR-ORL-TRAINING-FAILED-RX

Default Severity: Minor (MN)

Logical Object: EQUIPMENT

Resource Type: PPM

The OTDR-ORL-TRAINING-FAILED-RX alarm is raised if the training phase cannot find valid calibration data.

# OTDR-ORL-TRAINING-FAILED-TX

Default Severity: Minor (MN)

Logical Object: EQUIPMENT

Resource Type: PPM

The OTDR-ORL-TRAINING-FAILED-TX alarm is raised if the training phase cannot find valid calibration data.

# OTDR-ORL-TRAINING-IN-PROGRESS-RX

Default Severity: NA

Logical Object: EQUIPMENT

Resource Type: PPM

The OTDR-ORL-TRAINING-IN-PROGRESS-RX alarm is raised if the ORL is started in the fast mode on the Rx side.

# OTDR-ORL-TRAINING-IN-PROGRESS-TX

Default Severity: NA

Logical Object: EQUIPMENT

Resource Type: PPM

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.

# OTDR-OTDR-TRAINING-FAILED-RX

Default Severity: NA

Logical Object: EQUIPMENT

Resource Type: PPM

The OTDR-OTDR-TRAINING-FAILED-RX alarm is raised if the training phase cannot find valid calibration data.

# OTDR-OTDR-TRAINING-FAILED-TX

Default Severity: NA

Logical Object: EQUIPMENT

Resource Type: PPM

The OTDR-OTDR-TRAINING-FAILED-TX alarm is raised if the training phase cannot find valid calibration data.

# OTDR-SCAN-FAILED

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

Logical Object: EQPT

Resource Type: PPM

The Optical Time Domain Reflectometer (OTDR) scan failed alarm is raised when the OTDR scan fails and no result is sent to the user.

# OTDR-SCAN-IN-PROGRESS

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

Logical Objects: PPM

Resource Type: 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

Resource Type: PPM

The OTDR-SCAN-NOT-COMPLETED alarm is raised when the scan has not been executed on the span in the TX direction.

# OTUK-AIS

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

Logical Object: TRUNK

Resource Type: OTUk

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

Resource Type: OTUk

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 133 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 135 condition or OTUK-SD , on page 136 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-BIAE

Default Severity: Non-Service-Affecting (NSA)

Logical Object:

Resource Type: OTUk

The OTUk-SM Backward Incoming Alignment Error alarm is raised when

# OTUK-IAE

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

Logical Object: TRUNK

Resource Type: OTUk

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 135 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 135 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

Resource Type: OTUk

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

Resource Type: OTUk

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 186 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

Resource Type: OTUk

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 137 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

Resource Type: OTUk

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 133 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 175 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).

# OVER-TEMP-UNIT-PROT

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

Logical Object: EQPT

Resource Type: CARD

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 189 procedure.

**Step 5** If the air filter is clean, complete the Remove and Reinsert (Reseat) Any Card , on page 187 procedure.

**Step 6** If the alarm fails to get cleared, complete the Physically Replace a Card, on page 188 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

Resource Type: OPT

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

Resource Type: CARD

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

Resource Type: 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).

# PEER-CERT-VERIFICATION-FAILED

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

Logical Object: OTN

Resource Type: OTUk/ODUk

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

Resource Type: ODUK

The Peer Client Signal Fail alarm 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/cisco/web/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)

Resource Type: OCH

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.

The PMD Degrade alarm is raised when the device experiences PMD in excess of 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

Resource Type: OPT

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 98 procedure
- Clear the LOS (TRUNK) Alarm, on page 97 procedure
- Clear the LOS-P (OCH) Alarm, on page 99 procedure
- Clear the LOS-P (AOTS, OMS, OTS) Alarm procedure

- Clear the LOS-P (TRUNK) Alarm, on page 102 procedure
- Clear the OPWR-LFAIL Alarm, on page 126 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

Resource Type: PORT

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.

The port module communication failure (PORT-COMM-FAIL) alarm is raised on the 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.

# PRBS-ENABLED

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

Logical Objects: OCH

Resource Type: ODUk

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-CONFIG-MISMATCH

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

Logical Object: EQPT

Resource Type: CARD

The Protection Card Configuration Mismatch alarm is raised when

# 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

Resource Type: CARD

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.

# 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.

# PROV-MISMATCH

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

Logical Object: EQPT and control cards

Resource Type: PPM

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 the line cards, perform the following steps:

a) Determine range of PPM wavelength range by viewing the frequency provisioned for the card:

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 the TNC, TNCS, TNCE, or TNCS-O cards, do the steps that follow:

a) To clear the alarm when the card mode is TNC with OC3 or GE ports provisioned and the plugged card is a TNCS-O, do the steps that follow:

1. Login to the SVO web user interface.
2. Open the TNCS-O card view.
3. Delete the provisioned OC3 or GE ports.
4. Click the **Provisioning** > **Card Mode** tabs.
5. Set mode to TNCO-MODE.
6. Click **Apply**.

b) To clear the alarm when the card mode is TNCO and the plugged card is a TNC, TNCS, or TNCE, do the steps that follow:

1. Login to the SVO web user interface.
2. Open the TNC, TNCS, or TNCE card view where you want to clear the alarm.
3. Click the **Provisioning** > **Card Mode** tabs.
4. Set Mode to TNC-MODE.
5. Click **Apply**.

**Step 3** 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.
c) Insert the TNCS card.

**Step 4** To clear the PROV-MISMATCH alarm on the 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.
c) Insert the TNCS-O card.

**Note** On the MR-MXP and 400G-XP 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

Resource Type: ODUk

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**

Complete the Provision G.709 Thresholds procedure in the *Cisco NCS 2000 Series SVO Configuration Guide*.

# PWR

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

Logical Object: EQPT

Resource Type: PWR

The Power Failure at Connector alarm is raised when

# PWR-CON-LMT

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

Logical Object: EQPT

Resource Type: SHELF

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

The PWR-CON-LMT condition is also raised when you install the SVO card.

## 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

Resource Type: PWR

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 145 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 187 procedure.

**Step 3** If the alarm does not clear, complete the Physically Replace a Card, on page 188 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

Resource Type: PWR

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 149 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

Resource Type: PWR

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 149 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

Resource Type: PWR

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.

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 control card.

## Clear the PWR-FAIL-RET-B Alarm

**Procedure**

Complete the Clear the PWR-FAIL-A Alarm, on page 149 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).

# Powerfail Restart

Default Severity: warning

Logical Object: Standing

not-applicable

## Clear the Powerfail Restart Alarm

**Procedure**

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).

# PWR-PROT-ON

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

SONET Logical Objects: OTS

Resource Type: OPT

The Raman Power Protection On alarm occurs when the Raman amplifier is used on fiber span that is too short for Raman power.

# RESOURCE-ALLOC-FAIL

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

Logical Object: EQPT

Resource Type: CARD

The Resource Allocation Failed (RESOURCE-ALLOC-FAIL) alarm is raised when Quality of Service (QoS) cannot be configured due to lack of resources.

## Clear the RESOURCE-ALLOC-FAIL Alarm

**Procedure**

Find the resources that are using more memory and free up the memory.

If the alarm does not get cleared, you must 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.

# RESOURCES-GONE

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

Logical Object: EQPT

Resource Type: CARD

The No More Resources Available (RESOURCES-GONE) alarm is raised, if any of the following condition is there:

- If the resource memory is used completely.
- When resources cannot be configured.
- When SEU FPGA bit error detected on the PTF card. To confirm the SEU FPGA bit error, connect to the respective PTF card using IOS command and check for any alarm on LEONE FPGA using the command “fmea alarm”.

# Clear the RESOURCES-GONE Alarm

**Procedure**

Perform any of the following, as appropriate:

- Find the resources that are using more memory and free up memory.
- In case of SEU FPGA bit error, reset the PTF card.

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).

# Running Low On Resources

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

Logical Object: EQPT

Resource Type: CARD

The Running Low on Resources (RESOURCES-LOW) alarm is raised if the resource memory is very low or when more resources cannot be configured.

## Clear the Running Low On Resources Alarm

**Procedure**

Find the resources that are using more memory and free up the memory.

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).

# Remote Alarm Indication

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

Logical Object: TDM

Resource Type: OXC/STMn/OCn

The Remote Alarm Indication (RAI) alarm is raised when the received signal is degraded.

## Clear the Remote Alarm Indication Alarm

**Procedure**

The alarm is cleared when the high frequency signals are received.

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).

# REMOTE-FAULT

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

SONET Logical Objects: ETH

Resource Type: ETH

The REMOTE-FAULT alarm is raised on the card under the following conditions:

- 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.

# REROUTE-IN-PROG

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

Logical Objects: OTS

Resource Type: OXC

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

Resource Type: OXC

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

Resource Type: OPT

The Remote Failure Indication condition is raised against a TXP or MXP card when the card has an AIS condition. 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.

# ROUTE-OVERFLOW

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

Logical Object: NE regardless of MSTP or MSPP

Resource Type: NE

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.

# Running Low On Resources

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

Logical Object: EQPT

Resource Type: CARD

The Running Low on Resources (RESOURCES-LOW) alarm is raised if the resource memory is very low or when more resources cannot be configured.

## Clear the Running Low On Resources Alarm

**Procedure**

Find the resources that are using more memory and free up the memory.

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).

# SD (TRUNK)

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

Logical Object: TRUNK

Resource Type: OCn, STMn

A Signal Degrade (SD) condition on 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 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 186 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).

# SF (TRUNK)

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

Logical Object: TRUNK

Resource Type: OCn, STMn

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 157 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).

# SFTWDOWN

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

Logical Object: EQPT

Resource Type: NE

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.

# SHELF-COMM-FAIL

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

Logical Object: SHELF

Resource Type: 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.

# SIGLOSS

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

Logical Objects: FC, GE, ISC, TRUNK

Resource Type: ETH, OCH

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

Resource Type: 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.

**Step 3** If no network problems exist, ensure the system proxy is provisioned correctly:

a) Log into the SVO web interface.

b) Click the hamburger icon at the top-left of the page, and select **SVO Configuration**.

c) Click the **SVO Configuration** > **Time Settings** tabs.

d) Perform the following steps:

1. **Enable Date and Time**—Check this check box to enable the synchronization of SVO card with network time.

2. **Server Address**—Type the IP address of the primary NTP server.
3. **Backup Server Address**—Type the IP address of the secondary NTP server.

   When the primary NTP server fails or is not reachable, the node uses the secondary NTP server to synchronize its date and time. If both the primary and secondary NTP servers fail or are not reachable, an SNTP-FAIL alarm is raised. The node checks for the availability of the primary or secondary NTP server at regular intervals until it can get the time from any one of the NTP servers. After the node gets the time from any one server, it synchronizes its date and time with the server's date and time and the SNTP-FAIL alarm is cleared. For each retry and resynchronization, the node checks the availability of the primary NTP server first, followed by the secondary NTP server. The node synchronizes its date and time every hour.
4. **Date and Time**—Choose the date and time.
5. **Time Zone**—Choose a city within your time zone from the drop-down list.

e) Click **Apply**.

A confirmation message appears.

f) 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).

# SOFT-VERIF-FAIL

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

Logical Object: EQPT

Resource Type: NE

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

Resource Type: OPT

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 entered in the SVO web interface are correct. Follow these steps:

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

Resource Type: OCH, ODUk

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:

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

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

- Local client alarms, as 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:

a) Log into the SVO web interface.
b) Click the hamburger icon at the top-left of the page, and select **SVO Topology**.
c) Navigate to the chassis view.
d) Click the slot that contains the card, and click **Open Card**.
e) Click the **Provisioning** > **Optical Channel** tabs.
f) If the port Admin State field displays OOS,MT (or Locked,maintenance) or OOS,DSBLD (or Locked,disabled), click the cell to highlight it and choose IS (or Unlocked), from the drop-down list. Changing the state to **IS** (or **Unlocked**) also clears any loopback provisioned on the port.
g) 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-DUS

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

Logical Object: TRUNK

Resource Type: OCn, STMn, OTUk

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

Resource Type: OCn, STMn, OTUk

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

Resource Type: OCn, STMn, OTUk

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

Resource Type: OCn, STMn, OTUk

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 165 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

Resource Type: OCn, STMn, OTUk

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

Resource Type: OCn, STMn, OTUk

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

Resource Type: OCn, STMn, OTUk

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

Resource Type: OCn, STMn, OTUk

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

Resource Type: OCn, STMn, OTUk

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

Resource Type: OCn, STMn, OTUk

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

Resource Type: OCn, STMn, OTUk

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

Resource Type: OCn, STMn, OTUk

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

Resource Type: OCn, STMn, OTUk

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.

# SSM-TNC

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

Logical Object: TRUNK

Resource Type: OCn, STMn, OTUk

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

Resource Type: CARD

The Software Mismatch condition occurs during software upgrade when there is a mismatch between software versions.

## Clear the SW-MISMATCH Condition

**Procedure**

Complete the Reset a Card, on page 186 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

Resource Type: EXT_SYNCHREF, NE_SYNCHCREF

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

Resource Type: EXT_SYNCHREF, NE_SYNCHCREF

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 172 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

Resource Type: EXT_SYNCHREF, NE_SYNCHCREF

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 172 alarm or the SYNCSEC , on page 173 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

Resource Type: OTUk, BITS

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 188 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

Resource Type: ETH

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

Resource Type: EXT_SYNCHREF, NE_SYNCHCREF

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 170 alarm.

# SYNCSEC

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

Logical Objects: EXT-SREF, NE-SREF

Resource Type: EXT_SYNCHREF, NE_SYNCHCREF

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 170 alarm.

# SYNCTHIRD

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

Logical Objects: EXT-SREF, NE-SREF

Resource Type: EXT_SYNCHREF, NE_SYNCHCREF

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 68 condition or the HLDOVRSYNC , on page 77 condition after a SYNCTHIRD alarm.

# SYSBOOT

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

Logical Object: NE

Resource Type: 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

Resource Type: CARD

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

Resource Type: 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 189 procedure.

**Step 2** If the condition does not clear, complete the Remove and Reinsert a Fan-Tray Assembly, on page 190 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

Resource Type: OCn, STMn

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.

# TRAF-AFFECT-RESET-REQUIRED

Default Severity: Minor (MN) and Non-Service affecting (NSA)

Logical Object: CARD

Resource Type: CARD

The Traffic Affecting Reset Required alarm is raised when you have to reset the MR-MXP cards. This reset impacts the traffic.

# TRAF-AFFECT-SEC-UPG-REQUIRED

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

Logical Object: EQUIPMENT

Resource Type: CARD

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).

# 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

**Procedure**

**Step 1** Log in to a node with Cisco SVO web user interface.

**Step 2** In the rack view, click the line card.

A menu appears.

**Step 3** From the menu, click **Open Card**.

**Step 4** In the card slot view, Click the **Provisioning** tab.

**Step 5** Click the **Pluggable Port Modules** tab.

**Step 6** In the **Pluggable Port Modules** tab, click the plus (+) sign.

**Step 7** Select the **Port ID**.

**Step 8** Choose the same payload type from the **Port Type** drop-down list.

**Step 9** Click **OK**.

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).

# 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.

# 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 177 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.

# UNC-WORD

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

Logical Object: TRUNK

Resource Type: OCH, OTUk

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 186 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).

# UNQUAL-PPM

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

Logical Objects: PPM

Resource Type: 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).

# USB-MOUNT-FAIL Alarm

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

Logical Objects: USB

Resource Type: USB_FLASH

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

Resource Type: 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

Resource Type: USB_FLASH

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.

# USBSYNC

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

Logical Object: USB

Resource Type: USB_FLASH

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.

# VOA-DISABLED

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

Logical Object: EQPT

Resource Type: CARD

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

Resource Type: OPT, OXC

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 188 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

Resource Type: OPT, OXC

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 188 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

Resource Type: OPT, OXC

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 188 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

Resource Type: OPT, OXC

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 188 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

Resource Type: 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).

# WKSWPR (TRUNK)

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

Logical Object: TRUNK

Resource Type: OCn, STMn, ODUk, OTUk, ETH

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

Resource Type: OPT

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).

# WTR (TRUNK)

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

Logical Object: TRUNK

Resource Type: OCn, STMn, ODUk

The Wait To Restore condition occurs when the WKSWPR (TRUNK), on page 184 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-MISMATCH

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

Logical Object: TRUNK

Resource Type: OCH

The Equipment Wavelength Mismatch alarm applies to the TXP and MXP cards when you provision a wavelength that the card does not support.

## Clear the WVL-MISMATCH alarm

**Procedure**

**Step 1** Log into the SVO web interface.

**Step 2** Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

**Step 3** Navigate to the chassis view.

**Step 4** Click the slot that contains the card, and click **Open Card**.

**Step 5** Click the **Provisioning** > **Optical Channel** tabs.

**Step 6** Set the frequency in THz in the **Frequency** field.

The wavelength is automatically set based on the frequency.

**Step 7** 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.

# Reset a Card

**Procedure**

**Step 1** Log into the SVO web interface.

**Step 2** Click the hamburger icon at the top-left of the page, and select **SVO Topology**. The SVO Topology page appears.

**Step 3** Click the rack in the left panel. The rack view appears.

**Step 4** Click the chassis and select **Open**. The chassis view appears.

**Step 5** Left-click the card, and choose **Soft Reset** .

**Step 6** Click **Yes**.

# 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 145 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 145 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.

# 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 189.)

- 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 191.

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 189 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.

# 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 194.

**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**.

# NE-VER-NOT-SUPP

Default Severity: Major (MJ)

Logical Object: NE

Resource Type: NE

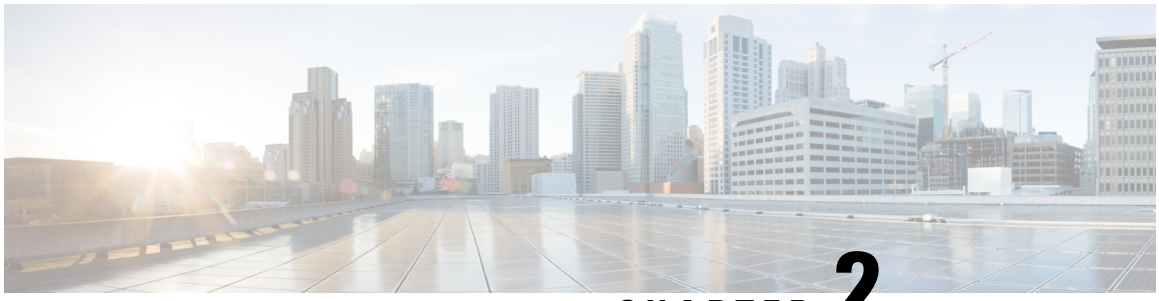
The NE-VER-NOT-SUPP alarm is raised when the managed NE version is not supported.

## Clear the NE-VER-NOT-SUPP Alarm

**Procedure**

Upgrade the device with a supported version.

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).



CHAPTER 2

# Transient Conditions

This chapter provides description for each commonly encountered transient condition.

# ADMIN-DISABLE

The Disable Inactive User (ADMIN-DISABLE) condition occurs when the administrator disables a user or when a account is inactive for a specified period.

This transient condition does not result in a standing condition.

# ADMIN-DISABLE-CLR

The Disable Inactive Clear (ADMIN-DISABLE-CLR) condition occurs when the administrator clears the disable flag on a user account.

This transient condition does not result in a standing condition.

# ADMIN-LOCKOUT

The Admin Lockout of User (ADMIN-LOCKOUT) condition occurs when the administrator locks a user account.

This transient condition does not result in a standing condition.

# ADMIN-LOCKOUT-CLR

The Admin Lockout Clear (ADMIN-LOCKOUT-CLR) condition occurs when the administrator unlocks a user account or when the lockout time expires.

This transient condition does not result in a standing condition.

# ADMIN-LOGOUT

The Admin Logout of User (ADMIN-LOGOUT) condition occurs when the administrator logs off a user session.

This transient condition does not result in a standing condition.

# ADMIN-SUSPEND

The Suspend User (ADMIN-SUSPEND) condition occurs when the password for a user account expires.

This transient condition does not result in a standing condition.

# ADMIN-SUSPEND-CLR

The Suspend User Clear (ADMIN-SUSPEND-CLR) condition occurs when the user or administrator changes the password.

This transient condition does not result in a standing condition.

# AUD-ARCHIVE-FAIL

The Archive of Audit Log Failed (AUD-ARCHIVE-FAIL) condition occurs when the software fails to archive the audit log. The condition normally occurs when the user refers to an FTP server that does not exist, or uses an invalid login while trying to archive. The user must log in again with correct user name, password, and FTP server details.

This transient condition does not lead to a standing condition.

# AUTOWDMANS

The Automatic WDM ANS Finish (AUTOWDMANS) condition indicates that an automatic node setup (ANS) command has been initiated. It normally occurs when you replace dense wavelength division multiplexing (DWDM) cards; the condition is an indication that the system has regulated the card.

This transient condition does not result in a standing condition.

# DBBACKUP-FAIL

The Database Backup Failed (DBBACKUP-FAIL) condition occurs when the system fails to back up the database when the backup command is initiated.

This condition can occur when the server is not able to handle the backup operation due to network or server issues. Repeat the same operation again and check to see if it is successful. If the backup fails, it could be due to a network issue or software program failure. Contact the Cisco Technical Assistance Center (TAC) (1 800 553-2447) for assistance.

# DBRESTORE-FAIL

The Database Restore Failed (DBRESTORE-FAIL) condition occurs when the system fails to restore the backed up database when the restore command is initiated.

This condition can be due to server issues, network issues, or human error (pointing to a file that does not exist, wrong file name, etc.). Retrying the database restore with the correct file will usually succeed. If the network issue persists, you must contact network lab support. If the condition is caused by a network element (NE) failure, contact the Cisco Technical Assistance Center (TAC) (1 800 553-2447) for assistance.

# FIRMWARE-DOWNLOAD

The Firmware Download (FIRMWARE-DOWNLOAD) condition occurs when the firmware is being downloaded during the firmware upgrade. The firmware upgrade initiates when the download is complete.

This transient condition does not result in a standing condition.

# FIRMWARE-UPG

The Firmware Upgrade (FIRMWARE-UPG) condition occurs when the firmware is being upgraded. This condition reflects the upgrade status.

This transient condition does not result in a standing condition.

# FIRMWARE-UPG-COMPLETE

The Firmware Upgrade Complete (FIRMWARE-UPG-COMPLETE) condition occurs when the firmware upgrade is successfully completed.

This transient condition does not result in a standing condition.

# FIRMWARE-UPG-FAIL

The Firmware Upgrade Fail (FIRMWARE-UPG-FAIL) condition occurs when the firmware upgrade fails. The user must start the firmware upgrade again.

This transient condition does not result in a standing condition.

# LOGIN-FAIL-LOCKOUT

The Invalid LoginLocked Out (LOGIN-FAIL-LOCKOUT) condition occurs when you attempt to log into a locked account.

This transient condition does not result in a standing condition.

# LOGIN-FAIL-ONALRDY

The Security: Invalid LoginAlready Logged On (LOGIN-FAIL-ONALRDY) condition occurs when a user attempts to log into a node where the user already has an existing session and a Single-User-Per-Node (SUPN) policy exists.

This transient condition does not result in a standing condition.

# LOGIN-FAILURE-PSWD

The Invalid LoginPassword (LOGIN-FAILURE-PSWD) condition occurs when you attempt to log in with an invalid password.

This transient condition does not result in a standing condition.

# LOGIN-FAILURE-USERID

The Invalid LoginUsername (LOGIN-FAILURE-USERID) condition occurs when a user login ( SVO web interface) fails because the login username is not present on the node database. You must log in again with an existing user ID.

This transient condition is equivalent to a security warning. You must check the security log (audit log) for other security-related actions that have occurred.

# LOGOUT-IDLE-USER

The Automatic Logout of Idle User (LOGOUT-IDLE-USER) condition occurs when a user session is idle for too long (the idle timeout expires) and the session terminates as a result. You must log in again to restart your session.

# MASTERKEY-SUCCESS

The Master Key Exchange Success condition occurs when the primary key is successfully reset and the Threshold Crossing Alert (TCA) has provisioned.

This transient condition does not result in a standing condition.

# PM-TCA

The Performance Monitoring Threshold Crossing Alert (PM-TCA) condition occurs when network collisions cross the rising threshold for the first time.

# PSWD-CHG-REQUIRED

The Password Change Required condition occurs when the user password needs to be changed.

This transient condition does not result in a standing condition.

# RMON-ALARM

The Remote Monitoring Threshold Crossing Alarm (RMON-ALARM) condition occurs when the remote monitoring (RMON) variable crosses the threshold.

# RMON-RESET

The RMON Histories and Alarms Reset Reboot (RMON-RESET) condition occurs when the time-of-day settings on the control card are increased or decreased by more than five seconds. This invalidates all the history data, and RMON must restart. It can also occur when you reset a card.

# SESSION-TIME-LIMIT

The Session Time Limit Expired (SESSION-TIME-LIMIT) condition occurs when a login session exceeds the time limit and you are logged out of the session. You must log in again.

# USER-LOCKOUT

The User Locked Out (USER-LOCKOUT) condition occurs when the system locks an account because of a failed login attempt. To proceed, the administrator must unlock the account or the lockout time must expire.

# USER-LOGIN

The Login of User (USER-LOGIN) occurs when you begin a new session by verifying your user ID and password.

This transient condition does not result in a standing condition.

# USER-LOGOUT

The Logout of User (USER-LOGOUT) condition occurs when you stop a login session by logging out of your account.

This transient condition does not result in a standing condition.

# WRMRESTART

The Warm Restart (WRMRESTART) condition occurs when the node restarts while it is powered up. A restart can be caused by provisioning, such as a database restore or IP changes, or by software defects. A WRMRESTART is normally accompanied by MANRESET or AUTORESET to indicate whether the reset was initiated manually (MAN) or automatically (AUTO).

This is the first condition that appears after a control card is powered up. The condition changes to COLD-START if the control card is restarted from a physical reseat or a power loss.

# WKSWBK

Default Severity: Warning

Logical Object: Transient

Resource Type: OPT ODUk

The WKSWBK alarm is raised when the protection switch returns the traffic to the nominal working resource.

## Clear the WKSWBK Alarm

### Procedure

The alarm never clears as it is a transient condition.

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).