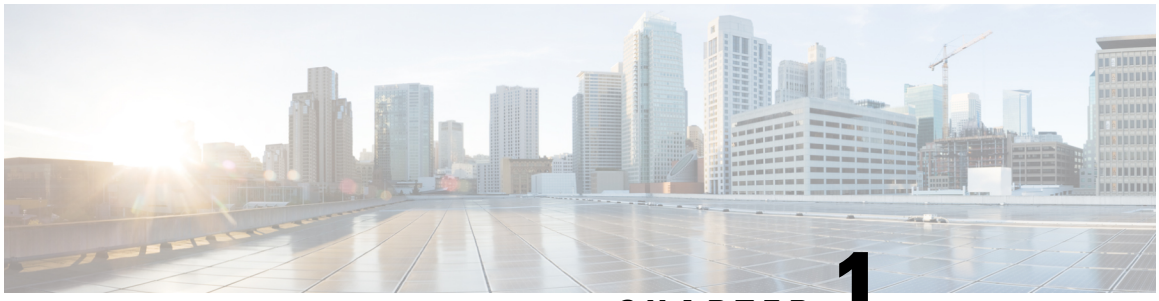
Troubleshooting Guide for Cisco NCS 1014, IOS XR Release 26.x.x

First Published: 2026-03-02

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

Alarm Troubleshooting

This chapter provides a description, severity, and troubleshooting procedure for each commonly encountered Cisco NCS 1014 alarm and condition. To clear an alarm when it is raised, refer to its clearing procedure.

CD Alarm

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

Logical Object: TRUNK

The Chromatic Dispersion (CD) alarm is raised when the detected chromatic dispersion value is above or below the configured threshold values.

Clear the CD Alarm

Procedure

Configure the threshold value within range.

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).

CRYPTO_HW_FAILURE

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

Logical Object: Shelf

Supported from release: R25.2.1

The CRYPTO_HW_FAILURE alarm is raised when a KAT associated with any line card port fails. As a result, the line card is locked, preventing further configuration or operational use until the issue is resolved.

Clear the CRYPTO_HW_FAILURE Alarm

Follow these steps to clear the alarm:

Procedure

Step 1 Check if the line card is in a locked and failed state due to KAT errors.

Step 2 Power-cycle the affected line card to restart the KAT process and attempt recovery, if KAT errors are confirmed.

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).

CRYPTO-INDEX-MISMATCH

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

Logical Object: OTN

Supported from release: R25.2.1

The *OTN-Sec-Association-Mismatch* (CRYPTO-INDEX-MISMATCH) alarm is raised when the AN# of Rx on the near end node does not match the AN# of Tx on the far end node, or the AN# of Tx on the near end node does not match with the AN# of Rx on the far end node.

Clear the CRYPTO-INDEX-MISMATCH Alarm

Follow these steps to clear the alarm:

Procedure

Step 1 Verify the key synchronization mechanism is working.

Step 2 Verify the AN and key status on both sides.
The alarm is cleared when the index AN numbers match with the peer node.

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).

CRYPTO-KEY-EXPIRING

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

Logical Object: OTN

Supported from release: R25.2.1

The *OTN Sec Association current key will expire soon* (CRYPTO-KEY-EXPIRING) alarm is raised when all rekey attempts have failed after exceeding 70% of the key's lifetime. This alarm is typically triggered approximately 5 hours after the system crosses the 70% volume-based rekeying threshold.

Clear the CRYPTO-KEY-EXPIRING Alarm

Procedure

Step 1 Verify that the automatic rekey is enabled and correctly configured.

Step 2 Verify that the key lifetimes and rollover windows are overlapping properly.

The alarm is cleared automatically when the key rollover completes successfully. If the alarm is not resolved in time, the system raises the **CRYPTO-KEY-EXPIRED** alarm, potentially disrupting future traffic.

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).

CRYPTO-KEY-EXPIRED

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

Logical Object: OTN

Supported from release: R25.2.1

The *OTN Sec Encryption Key Expired* (CRYPTO-KEY-EXPIRED) alarm is raised when a hardware programmed key expires and there is no new key available for rollover.

Clear the CRYPTO-KEY-EXPIRED Alarm

Procedure

The alarm is cleared after the new sak key is made available.

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).

DGD Alarm

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

Logical Object: TRUNK

The Differential Group Delay (DGD) alarm is raised when the value of the differential group delay read by the pluggable port module exceeds the configured threshold value.

Clear the DGD Alarm

Procedure

Configure the threshold value within range if DGD value is not within the threshold range.

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).

DISASTER_RECOVERY_UNAVAILABLE_ALARM

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

Logical Object: Instorch

The DISASTER_RECOVERY_UNAVAILABLE_ALARM is raised when the chassis SSD image is corrupted or system is running with a software not committed.

Clear the Disaster Recovery Unavailable Alarm

Procedure

This alarm clears automatically after the upgrade from a lower release to a higher release. The upgrade process completes after running the **install commit** command. It syncs the image with the local repository every 12 hours. For more details about software upgrade, see the Upgrade Software section of the *System Setup and Software Installation Guide for Cisco NCS 1014*.

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

EGRESS-AMPLI-GAIN-HIGH

Default Severity: Non Service-Affecting (NSA)

Logical Object: Controller OTS

Supported from release: R25.1.1

The EGRESS-AMPLI-GAIN-HIGH alarm is raised when the EGRESS EDFA module cannot reach the gain setpoint. This condition occurs if the amplifier reaches its range boundaries and the Egress Amplifier Gain Degrade is high.

Clear the EGRESS-AMPLI-GAIN-HIGH Alarm

Procedure

Step 1 Adjust the gain setting to a correct value using the **controller ots egress-ampli-gain** command.

Step 2 Check the overall system settings, performance, and the configured EDFA Gain using the **show configuration commit changes all** command.

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).

EGRESS-AMPLI-GAIN-LOW

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

Logical Object: Controller OTS

Supported from release: R25.1.1

The EGRESS-AMPLI-GAIN-LOW alarm is raised when the Egress Amplifier Gain Degrade is Low.

Clear the EGRESS-AMPLI-GAIN-LOW Alarm

Procedure

Step 1 Adjust the gain setting to a correct value using the **controller ots egress-ampli-gain** command.

Step 2 Check the overall system settings, performance, and the configured EDFA Gain using the **show configuration commit changes all** command.

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).

EGRESS-AUTO-LASER-SHUT

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

Logical Object: Controller OTS

Supported from release: R25.1.1

The EGRESS-AUTO-LASER-SHUT alarm is raised when the Egress EDFA shuts down its Tx power if it is not receiving any input power on the Line Rx port due to a fiber cut. This alarm is raised if the safety-control-mode is set to the auto state on line OTS controller.

Clear the EGRESS-AUTO-LASER-SHUT Alarm

Procedure

Step 1 Check and clear the RX-LOC alarm by repairing any cut in fiber cable.

Step 2 Check and clear the RX-LOS-P alarm by adjusting the threshold setting.

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).

EGRESS-AUTO-POW-RED

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

Logical Object: Controller OTS

Supported from release: R25.1.1

The EGRESS-AUTO-POW-RED alarm is raised when LOS is detected on the line RX, the line TX normalizes the signal output power. In this case, if safety-control-mode set to auto, the egress amplifier goes into power reduction mode for safety reasons.

Clear the EGRESS-AUTO-POW-RED Alarm

Procedure

Step 1 Check if the egress amplifier automatic power reduction is active using the **show controllers** *Controller-type R/S/I/P* command.

Step 2 Check if the safety conditions of the Egress EDFA are active using the **show controllers** *Controller-type R/S/I/P* command.

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).

EQUIPMENT_FAILURE

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

Logical Object: LC

The EQUIPMENT_FAILURE alarm is raised when any of the following equipment fails:

- Optical module
- Phase Lock Loop (PLL)
- Cloud Detection and Response (CDR)
- Line Card
- Field Programmable Gate Array (FPGA)
- Line card RAM or Disk
- META-DX2
- I/O Expander

Clear the EQUIPMENT_FAILURE Alarm

Procedure

Step 1 Collect logs to gather detailed diagnostic information. Use the **show tech-support** command in privileged EXEC mode:

Example:

```
RP/0/RP0/CPU0:ios#show tech-support
```

Step 2 Check for any active alarms or syslogs to identify unexpected alarms that may have triggered the failure. If there are any alarms, clear the active alarms.

Step 3 Examine the following parameters related to the failed equipment or line card.

- Ambient temperature
- Voltage
- Current
- Power supply

Step 4 (Optional) If the alarm was raised for a CIM8 module in a 2.4T or 2.4TX line card, perform the following checks.

a) If there was an ambient temperature issue, perform the following steps.
b) Ensure that all fan trays are operational and the chassis and line card temperatures are within the recommended range.
c) After the chassis and line card temperatures are optimal, perform a CIM8 Online Insertion and Removal.
d) If the alarm is still active, conduct a cold reload of the Line Card using the **reload** *location Rack/Slot* **noprompt** command.

Step 5 Attempt the following workarounds in sequence to resolve the issue:

a) Perform online insertion and removal of the failed module.
b) Conduct a warm reload of the Line Card using the **reload** *location* **0/1/NXR0 noprompt** command.
c) Conduct a cold reload of the Line Card using the **reload** *location Rack/Slot* command.

Warning
A cold reload of the line card affects traffic on the other slice of the line card.

Step 6 If the alarm is still active after trying the workarounds in the previous steps, replace the faulty equipment.

For more details, refer to the Cisco Returns Portal or log in to the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

FAM_FAULT_TAG_CTRLR_MAINTENANCE_MODE

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

Logical Object: Controller

Supported from release: R25.3.1

The *In Maintenance Mode* (FAM_FAULT_TAG_CTRLR_MAINTENANCE_MODE) alarm is raised when the controller is set to maintenance mode.

Note This alarm is suppressed if PRBS or Loopback is configured on the controller.

Clear the FAM_FAULT_TAG_CTRLR_MAINTENANCE_MODE Alarm

Procedure

Remove the maintenance mode configuration using the **no sec-admin-state maintenance** command.

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).

FAM_FAULT_TAG_CTRLR_PRBS_PROVISIONED

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

Logical Object: Controller

Supported from release: R25.3.1

The *PRBS Provisioned* (FAM_FAULT_TAG_CTRLR_PRBS_PROVISIONED) alarm is raised when the user configures PRBS.

Note PRBS can only be configured when the controller is in maintenance mode.

Clear the FAM_FAULT_TAG_CTRLR_PRBS_PROVISIONED alarm

SUMMARY STEPS

1. This alarm is cleared when the user removes the PRBS configuration.

DETAILED STEPS

Procedure

This alarm is cleared when the user removes the PRBS configuration.

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).

ESD_INIT_ERR_E

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

Logical Object: ESD

The ESD_INIT_ERR_E alarm is raised when the Ethernet Switch Driver (ESD) initialization fails.

Clear the ESD_INIT_ERR_E Alarm

Procedure

Cisco IOS XR automatically detects and clears this alarm by resetting the switch.

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).

FAM_FAULT_TAG_LC_CIM_PCI_FAIL_PORT

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

Logical Object: Shelf

Supported from release: R24.3.1

The *CIM8 PCI Failed, Impacted ports: 0,1,2,3* (FAM_FAULT_TAG_LC_CIM_PCI_FAIL_PORT) alarm is raised when CIM8 PCI fails.

Clear the FAM_FAULT_TAG_LC_CIM_PCI_FAIL_PORT Alarm

To clear this alarm:

Procedure

Step 1 Reload the line card using the **reload location location** command.

Step 2 Perform an Online Insertion and Removal (OIR) of CIM

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).

FAM_FAULT_TAG_LC_CIM_SCREW_OPEN_PORT

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

Logical Object: Shelf

Supported from release: R24.3.1

The *CIM screw not closed on Port<number>, Impacted ports: 0,1,2,3* (FAM_FAULT_TAG_LC_CIM_SCREW_OPEN_PORT) alarm is raised when both CIM8 screws on the port are not properly tightened.

Clear the FAM_FAULT_TAG_LC_CIM_SCREW_OPEN_PORT Alarm

To clear this alarm:

Procedure

Verify that the screws on the trunk module are properly tightened.

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).

FAM_FAULT_TAG_LC_CIM8_UPGRADE_FAILED_PORT

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

Logical Object: Shelf

Supported from release: R24.3.1

The *CIM8 Upgrade failed for Port<number>, retry with LC warm reboot* (FAM_FAULT_TAG_LC_CIM8_UPGRADE_FAILED_PORT) alarm is raised when CIM8 upgrade fails.

Clear the FAM_FAULT_TAG_LC_CIM8_UPGRADE_FAILED_PORT Alarm

To clear this alarm:

Procedure

Retry the CIM8 upgrade using the line card warm reload command **reload location 0/slot/NXR0**.

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).

FAM_FAULT_TAG_LC_PORT_SUDI0_FAILURE

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

Logical Object: Shelf

Supported from release: R25.4.1

The *Port Secure ID Validation failed*(FAM_FAULT_TAG_LC_PORT_SUDI0_FAILURE) alarm is raised when the SUDI certificate validation on a CIM8 module does not succeed. This failure typically occurs when the SUDI certificates have not been programmed.

Clear the FAM_FAULT_TAG_LC_PORT_SUDI0_FAILURE alarm

Procedure

Replace the faulty module with a working CIM8 module

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).

FAM_FAULT_TAG_LC_PORT_SUDI0_UNSUPPORTED

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

Logical Object: Shelf

Supported from release: R25.4.1

The *Port SecureID validation not done*(FAM_FAULT_TAG_LC_PORT_SUDI0_UNSUPPORTED) alarm is raised when the module does not support the SUDI certificate.

Clear the FAM_FAULT_TAG_LC_PORT_SUDI0_UNSUPPORTED alarm

Procedure

Replace the module with the appropriate CIM8 module that supports SUDI certificates.

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).

FAN FAIL

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

Logical Object: SPI-ENVMON

The FAN FAIL alarm is raised when one of the two fans stops spinning or fails. If a fan stops working properly, the temperature can increase beyond the usual operating range, which might also trigger the TEMPERATURE alarm to activate.

Clear the FAN FAIL Alarm

Procedure

To clear this alarm, replace the faulty fan in the chassis.

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

FAN SPEED SENSOR 0: OUT OF TOLERANCE FAULT

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

Logical Object: SPI-ENVMON

The FAN SPEED SENSOR 0: OUT OF TOLERANCE FAULT alarm is raised when one or more fans in the fan tray are faulty.

Clear the FAN SPEED SENSOR 0: OUT OF TOLERANCE FAULT Alarm

Procedure

To clear this alarm, replace the faulty fans in 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).

FAN-POWER-ERROR

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

Logical Object: SPI-ENVMON

The FAN-POWER-ERROR alarm is raised when the power supply to the fan tray fails.

Clear the FAN-POWER-ERROR Alarm

Procedure

This alarm is cleared when:

- The power supply to the fan tray is restored.
- Online Insertion and Removal (OIR) of the fan tray is performed.

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).

FAN-TRAY-ABSENT

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

Logical Object: SPI-ENVMON

The FAN-TRAY-ABSENT alarm is raised when one or more fan trays are absent or removed from the chassis.

Clear the FAN-TRAY-REMOVAL Alarm

Procedure

Insert the fan trays into 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).

Flexo-LOF Alarm

Default Severity: Critical

Logical Object: TRUNK

Flexo LOF alarm is raised when loss of alignment is detected on the Flexo frame for more than 3ms.

Clear the Flexo-LOF Alarm

Procedure

Identify and correct the underlying cause of mis-alignment. The Flexo LOF (Loss of Frame) alarm is cleared when good alignment is detected on the Flexo frame for more than 3ms.

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).

Flexo-LOM Alarm

Default Severity: Critical

Logical Object: TRUNK

Flexo LOM (Loss of Multi-Frame) is raised when loss of multi-frame alignment is detected on the Flexo multi-frame for more than 10ms

Clear the Flexo-LOM Alarm

Procedure

Identify and correct the underlying cause of mis-alignment. The Flexo LOM alarm is cleared when good multi-frame alignment is detected on the Flexo multi-frame.

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).

Flexo-RDI Alarm

Default Severity: Not Reported

Logical Object: TRUNK

Flexo RDI is raised when trunk detected an incoming fault signal.

Clear the Flexo-RDI

Procedure

The Flexo-RDI alarm is cleared when `transmit-power` is than -40.00 dBm on trunk.

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).

FPD IN NEED UPGD

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

Logical Object: SPI-FPD

The FPD IN NEED UPGD alarm is raised when a newer FPD version in the FPD package is available on the FPD boot disk and the its internal memory has an outdated FPD version. A FPD package is stored on the boot disk and contains all the FPD images for each FPD on the platform for that Cisco IOS XR version. The FPDs run from images stored in its internal memory and not from the images inside the FPD package.

Clear the FPD IN NEED UPGD Alarm

Procedure

This alarm is cleared when the correct FPD is upgraded using the **upgrade hw-module location** *location-id* **fpd** *fpd name* command. For more details, see the Manual FPD Upgrade section of the *System Setup and Software Installation Guide for Cisco NCS 1014*.

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).

GIDM Alarm

Default Severity: Critical

Logical Object: TRUNK

The GIDM (Group ID Mismatch) alarm is raised when the received GID is not equal to the expcted GID.

Clear the GIDM Alarm

Procedure

The GIDM alarm is cleared when the received GID is equal to the expected GID on all the flexo group members. Ensure that the GID programmed on the remote trunk and local trunk ports 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).

HIBER Alarm

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

Logical Object: CLIENT

The High Bit Error Rate (HIBER) alarm is raised when the client ports receive 16 or more invalid sync-headers in 125 microseconds.

Clear the HIBER Alarm

Procedure

Step 1 Ensure the card port does not receive a high bit error rate.

Step 2 Clean the optical connectors.

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).

HI-LASERBIAS Alarm

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

Logical Object: PPM

The HI-LASERBIAS alarm is raised when the physical pluggable port laser detects a laser bias value beyond the configured high threshold.

Clear the HI-LASERBIAS Alarm

Procedure

Configure the threshold value within range if high laser bias threshold value is not within the threshold range.

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).

HI-RXPOWER Alarm

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

Logical Object: PPM

The HI-RXPOWER alarm occurs on the client optics controller when the measured individual lane optical signal power of the received signal exceeds the default or user-defined threshold. The HI-RXPOWER alarm occurs on the trunk optics controller when the total optical signal power of the received signal exceeds the default or user-defined threshold.

Clear the HI-RXPOWER Alarm

Procedure

Configure the high receive power threshold value in range. If the value is within the range of the high receive power threshold, physically verify, that the optical input power is overcoming the expected power threshold using a standard power meter.

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).

HI-SER Alarm

Default Severity: Major

Logical Object: CLIENT

The High Symbol Error Rate alarm is raised when 5560 or more errored FEC symbols are present in 8000 codewords.

Clear the HI-SER Alarm

Procedure

Identify the cause of high FEC errors and clear them.

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).

HIGH-TX-BR-PWR

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

Logical Object: Controller OTS

Supported from release: R25.1.1

The HI-TX-BR-PWR alarm is raised when there is a high back reflection power at the ingress port due to a poor fiber connection.

Clear the HIGH-TX-BR-PWR Alarm

Procedure

Ensure that the span fiber is thoroughly clean and properly connected.

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).

HI-TXPOWER Alarm

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

Logical Object: PPM

The HI-TXPOWER alarm occurs on the client optics controller when the measured individual lane optical signal power of the transmitted signal exceeds the default or user-defined threshold. The HI-TXPOWER alarm occurs on the trunk optics controller when the total optical signal power of the transmitted signal exceeds the default or user-defined threshold.

Clear the HI-TXPOWER Alarm

Procedure

Configure the high transmit power threshold in range. If the value is within the range of the high transmit power threshold, physically verify, that the optical output power is overcoming the expected power threshold using a standard power meter .

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).

IMPROPRMVL

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

Logical Object: LC/PPM

The IMPROPRMVL alarm is raised when a line card or PPM is removed without deleting its configuration.

Clear the IMPROPRMVL Alarm

To clear this alarm:

Procedure

Step 1 Re-insert the line card or PPM.

Step 2 Delete the line card configuration.

Step 3 Remove the line 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).

INGRESS-AMPLI-GAIN-HIGH

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

Logical Object: Controller OTS

Supported from release: R25.1.1

The INGRESS-AMPLI-GAIN-HIGH alarm is raised when the Ingress EDFA module cannot reach the gain setpoint. This condition occurs if the amplifier reaches its range boundaries.

Clear the INGRESS-AMPLI-GAIN-HIGH Alarm

Procedure

Step 1 Adjust the ingress amplification gain to a correct value using the **controller ots ingress-ampli-gain** command.

Step 2 Check the overall system settings, performance, and the configured EDFA Gain using the **show configuration commit changes all** command.

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).

INGRESS-AMPLI-GAIN-LOW

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

Logical Object: Controller OTS

Supported from release: R25.1.1

The INGRESS-AMPLI-GAIN-LOW alarm is raised when the Ingress EDFA module cannot reach the gain setpoint. This condition occurs if the amplifier reaches its range boundaries.

Clear the INGRESS-AMPLI-GAIN-LOW Alarm

Procedure

Step 1 Adjust the ingress amplification gain to a correct value using the **controller ots ingress-ampli-gain** command.

Step 2 Check the overall system settings, performance, and the configured EDFA Gain using the **show configuration commit changes all** command.

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).

INGRESS-AUTO-LASER-SHUT

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

Logical Object: Controller OTS

Supported from release: R25.1.1

The INGRESS-AUTO-LASER-SHUT alarm is raised when the ingress amplifier is off for safety Reasons.

Clear the INGRESS-AUTO-LASER-SHUT Alarm

Procedure

Step 1 For the controller OTS, check the RX-LOC or RX-LOSP alarm.

Step 2 Check if the safety conditions of the Ingress EDFA ALS are active.

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).

INGRESS-AUTO-POW-RED

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

Logical Object: Controller OTS

Supported from release: R25.1.1

The INGRESS-AUTO-POW-RED alarm is raised when the ingress amplifier is in power reduction mode for safety reasons.

Clear the INGRESS-AUTO-POW-RED Alarm

Procedure

Step 1 For controller OTS, check if the APR configuration is active.

Step 2 Check if the safety conditions of the Ingress EDFA for APR are active.

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).

FAM_FAULT_TAG_INTERNAL_LOOPBACK_PROVISIONED

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

Logical Object: Controller

The *Internal Loopback Configured* (FAM_FAULT_TAG_INTERNAL_LOOPBACK_PROVISIONED) alarm is raised when the user configures internal loopback.

Note Internal loopback can only be configured when the controller is in maintenance mode.

Clear the FAM_FAULT_TAG_INTERNAL_LOOPBACK_PROVISIONED Alarm

SUMMARY STEPS

1. This alarm is cleared when the user removes the internal loopback configuration.

DETAILED STEPS

Procedure

This alarm is cleared when the user removes the internal loopback configuration.

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).

Invalid sensor read error

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

Logical Object: SPI-ENVMON

Invalid sensor read error alarm raised when the system is unable to retreive data from its sensors.

Clear the Invalid sensor read error Alarm

Procedure

To clear this alarm, log in to the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html or call Cisco TAC (1 800 553-2447).

LC_BOOT_TIMEOUT

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

Logical Object: LC

The LC_BOOT_TIMEOUT Alarm is raised when the line card fails to boot in the expected amount of time or the line card modules do not boot correctly.

Clear the LC_BOOT_TIMEOUT Alarm

To clear this alarm:

Procedure

Step 1 Remove and re-insert the line card.

Step 2 If re-inserting the line card does not clear the alarm, reload the line card using the **reload location** *location* command.

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).

LC-DISCONNECTED

Default Severity: Major (MJ)

Logical Object: LC

The LC-DISCONNECTED alarm is raised when the Line Card Application (LCAPP) crashes or restarts.

Clear the LC-DISCONNECTED Alarm

Procedure

Step 1 Check if the LC_BOOT_TIMEOUT alarm is cleared.

Step 2 Log in to the line card and verify if the LCAPP is running fine.

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).

LC_SEATED

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

Logical Object: LC

The LC-SEATED alarm is raised when the line card is not fully seated.

Clear the LC_SEATED Alarm

Procedure

To clear this alarm, reinsert the line card properly into 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).

LC-SUDI-CERT-VERIFICATION-FAILURE

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

Logical Object: LC

The LC-SUDI-CERT-VERIFICATION-FAILURE alarm is raised when the SUDI certificates are not programmed.

Clear the LC-SUDI-CERT-VERIFICATION-FAILURE Alarm

Procedure

To clear the alarm, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html or call Cisco TAC (1 800 553-2447).

LICENSE-COMM-FAIL

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

Logical Object: plat_sl_client

The LICENSE-COMM-FAIL alarm is raised when the device is not able to communicate with the Cisco license cloud server.

Clear LICENSE-COMM-FAIL Alarm

Procedure

This alarm is cleared when the communication with the Cisco cloud license server is restored.

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

Line card missing

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

Logical Object: SPI-ENVMON

The *One or more LCs missing, running fans at max speed* alarm is raised when one or more line cards are missing, causing the fans to run at maximum speed.

Clear the Line card missing Alarm

To clear this alarm:

Procedure

Insert a line card or filler card in every slot where a line card is missing.

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).

FAM_FAULT_TAG_LINE_LOOPBACK_PROVISIONED

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

Logical Object: Controller

The *Line Loopback Configured* (FAM_FAULT_TAG_LINE_LOOPBACK_PROVISIONED) alarm is raised when the user configures line loopback.

Note Line loopback can only be configured when the controller is in maintenance mode.

Clear the FAM_FAULT_TAG_LINE_LOOPBACK_PROVISIONED Alarm

SUMMARY STEPS

1. This alarm is cleared when the user removes the line loopback configuration.

DETAILED STEPS

Procedure

This alarm is cleared when the user removes the line loopback configuration.

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).

LOCAL-FAULT Alarm

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

Logical Object: CLIENT

The LOCAL-FAULT alarm is raised when a local fault character sequence is received in the incoming MAC stream.

Clear the LOCAL-FAULT Alarm

Procedure

Verify that the port receives proper MAC streams from the far-end router or switch.

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).

LOCAL-DEG-SER Alarm

Default Severity: Major

Logical Object: CLIENT

The Local FEC DEG-SER (Degraded SER) alarm is received from remote end when it detects excessive FEC errors on the receiver side or when it sees AIS on the mapper ODU.

Note On the 2.4TX card in the muxponder mode, this alarm is not supported for the split ports 2 and 3 for 600G and 1000G trunk rates respectively.

Clear the LOCAL-DEG-SER Alarm

Procedure

This alarm is cleared when you clear the errors at the remote 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).

LO-RXPOWER Alarm

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

Logical Object: PPM

The LO-RXPOWER alarm is raised on the client or trunk optics controller when the measured individual lane optical signal power of the received signal falls below the default or user-defined threshold.

Clear the LO-RXPOWER Alarm

Procedure

Step 1 Configure low receive power threshold in range.

Step 2 Or verify that the trunk-rx port is cabled correctly, and clean the fiber connecting the faulty TXP/MXP card to the drop port of the DWDM 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).

LO-TXPOWER Alarm

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

Logical Object: PPM

The LO-TXPOWER alarm is raised on the client or trunk optics controller when the measured individual lane optical signal power of the transmitted signal falls below the default or user-defined threshold.

Clear the LO-TXPOWER Alarm

Procedure

Configure low transmit power threshold in range.

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).

RX-LOS-P Alarm

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

Logical Object: OTS, OSC, OTS-OCH

The Rx Loss of Signal Power (RX-LOS-P) at input signal port indicates that the PPM does not receive any incoming power signal. The purpose of the LOS-P alarm is to alert the user that optical power is not being received from the fiber.

Clear the RX-LOS-P Alarm

Procedure

Step 1 Verify whether there is a loss of received optical power. Compare the actual power levels with the expected power range.

Step 2 Verify the fiber continuity to the port of NCS 1014 and fix the fiber connection.

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).

MEA Alarm

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

Logical Object: LC/PPM

The Mismatch Equipment Attributes (MEA) alarm for the Pluggable Port Module (PPM) or Quad Small Form-Factor Pluggable (QSFP) is raised when:

- There is a mismatch in the configured client data rate and the supported QSFP physical data rate.
- The inserted line card is not compatible with the configuration that is currently available in the slot.

Clear the MEA Alarm

Procedure

Step 1 Verify the client data rate:

a) Verify the supported physical data rate of the QSFP on NCS 1014 using the **show inventory** command.
b) Verify the configured client data rate on NCS 1014 using the **show hw-module location** command.
c) If the above values do not match, insert the appropriate pluggable or configure the required client data rate.

For more details on configuring the client data rate, see *Configuring the Card Mode* chapter of the Configuration Guide for Cisco NCS 1014.

Step 2 Physically verify the type of card and configure the slot with the desired card type.

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).

OLC_APC_FM_CHANNEL_BELOW_MIN_PSD

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

Logical Object: OTS Controller

Supported from release: R25.4.1

The *Input channel PSD below minimum required*(OLC_APC_FM_CHANNEL_BELOW_MIN_PSD) alarm is raised on a COM port when the `channel_input_power` goes below the `channel_minimum_input_power`.

Clear the OLC_APC_FM_CHANNEL_BELOW_MIN_PSD alarm

The alarm is cleared when the input channel power exceeds the channel minimum input power.

To clear the alarm:

Before you begin

Procedure

Step 1 Verify the *Input power* using the `show olc channel-apc controller Ots0/0/0/0 regulation-info` command.

Step 2 Adjust the *channel-minimun-input-psd* to an appropriate value.

OLC_APC_FM_CHANNEL_HIGH_INPUT_POWER

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

Logical Object: OTS Controller

Supported from release: R25.4.1

The *Input channel power above the maximum expected*(OLC_APC_FM_CHANNEL_HIGH_INPUT_POWER) alarm is raised on a COM port when the `channel_input_power` is greater than the sum of the `expected_channel_input_power` and the `channel-rx-power-high-rel-thr`.

Clear the OLC_APC_FM_CHANNEL_HIGH_INPUT_POWER alarm

The alarm is cleared when the input channel power equals the sum of the expected channel input power and the channel RX power high relative threshold.

To clear the alarm:

Procedure

Step 1 Verify the *Expected input power* using the `show olc channel-apc controller Ots0/0/0/0 regulation-info` command.

Step 2 Adjust the *expected-total-input-power* to an appropriate value.

OLC_APC_FM_CHANNEL_LOW_INPUT_POWER

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

Logical Object: Controller

Supported from release: R25.4.1

The *Input channel power below the minimum expected*(OLC_APC_FM_CHANNEL_LOW_INPUT_POWER) alarm is raised on a COM port when the `channel_input_power` is less than the sum of the `expected_channel_input_power` and the `channel-rx-power-low-rel-thr`.

Clear the OLC_APC_FM_CHANNEL_LOW_INPUT_POWER alarm

The alarm is cleared when the input channel power equals the sum of the expected channel input power and the channel RX power low relative threshold.

To clear the alarm:

Before you begin

Procedure

Step 1 Verify the *Expected input power* using the `show olc channel-apc controller Ots0/0/0/0 regulation-info` command.

Step 2 Adjust the *expected-total-input-power* to an appropriate value.

OSNR Alarm

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

Logical Object: TRUNK

The Optical Signal Noise Ratio (OSNR) alarm occurs when the measured OSNR falls below the threshold.

Clear the OSNR Alarm

Procedure

Step 1 Verify the value of the minimum acceptable OSNR value of NCS 1014 using the **show controller optics R/S/I/P** command.

Step 2 If the value is not within the OSNR threshold range, configure the minimum acceptable OSNR value using the **controller optics R/S/I/P osnr-low-threshold** command in the configuration mode. The range is 0 to 4000 (in units of 0.1db).

Step 3 If the value is within the range of the minimum acceptable OSNR, contact TAC .

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).

OTNSEC-LOCALLY-SECURED

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

Logical Object: OTN

Supported from release: R25.2.1

The *OTN Sec Locally Secured* (OTNSEC-LOCALLY-SECURED) alarm is raised when the IKE session goes down and the OTNsec session is locally secured.

Clear the OTNSEC-LOCALLY-SECURED Alarm

Procedure

This alarm is cleared when the respective IKE session is up.

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).

OUT_OF_COMPLIANCE

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

Logical Object: plat_sl_client

The OUT_OF_COMPLIANCE alarm is raised when one or more license entitlements is not in compliance. This state is seen when the license does not have an available license in the corresponding Virtual Account that the Cisco device is registered to, in the Cisco Smart Account.

Clear Out of Compliance Alarm

SUMMARY STEPS

1. To clear this alarm, enter into a compliance by adding the correct number and type of licenses to the Smart Account.

DETAILED STEPS

Procedure

To clear this alarm, enter into a compliance by adding the correct number and type of licenses to the Smart Account.

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

PEM PID-MISMATCH

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

Logical Object: SPI-ENVMON

The PEM PID-MISMATCH alarm is raised when two different Power Entry Modules (PEM) or PSUs with different PIDs are connected to the 0/PM0 and 0/PM1 node positions.

Clear the PEM PID-MISMATCH Alarm

Procedure

To clear this alarm, make sure that both connected PSUs are of the same type and rating: either both AC 2KW or both AC 2.5KW. Similarly, for DC PSUs, both should be either DC 2KW or DC 2.5KW.

We recommend using PSUs with the same PIDs in both the 0/PM0 and 0/PM1 node positions.

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).

Power Module Error (PM_I2C_ACCESS_ERROR)

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

Logical Object: PEM

The Power Module Error (PM_I2C_ACCESS_ERROR) alarm is raised when there is an error on the power module. The detected error is a communication error on I2C bus.

Clear the Power Module Error (PM_I2C_ACCESS_ERROR) Alarm

Procedure

Step 1 Check if the PSU is unpowered or if its input power cable is disconnected, and confirm that redundant power supplies are installed and functioning.

Step 2 If the PSU is unpowered, perform an Online Insertion and Removal (OIR) procedure following Cisco guidelines.

Step 3 Move the PSU to a different compatible slot to see if the issue follows the PSU or remains with the original slot.

Note
Ensure that the chassis is adequately powered by other PSUs before attempting this, as insufficient power will cause the entire chassis to shut down, leading to traffic disruption.

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).

PORT_AUTO_TUNE_ERR_E

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

Logical Object: ESD

The PORT_AUTO_TUNE_ERR_E alarm is raised when the port auto-tuning fails.

Clear the PORT_AUTO_TUNE_ERR_E Alarm

Procedure

Cisco IOS XR automatically detects and clears this alarm by resetting the port.

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).

PORT_INIT_ERR_E

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

Logical Object: ESD

The PORT_INIT_ERR_E alarm is raised when the port initialization fails.

Clear the PORT_INIT_ERR_E Alarm

Procedure

Cisco IOS XR automatically detects and clears this alarm by resetting the port.

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).

POWER MODULE OUTPUT DISABLED

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

Logical Object: SPI-ENVMON

The POWER MODULE OUTPUT DISABLED alarm is raised power supply is not connected to the power module.

Clear the POWER MODULE OUTPUT DISABLED Alarm

Procedure

This alarm is automatically cleared when power supply is connected to the power module.

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).

POWER-MODULE-REDUNDANCY-LOST

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

Logical Object: SPI-ENVMON

The Power Group redundancy lost (POWER-MODULE-REDUNDANCY-LOST) alarm is raised if:

- the Power Supply Unit (PSU) is faulty or removed.
- the input PSU voltage goes beyond the working range of 180 to 264 volts for input high line (HL) and 90 to 140 volts for input low line (LL) nominal voltages.

Clear the POWER-MODULE-REDUNDANCY-LOST Alarm

Procedure

To clear this alarm:

- Re-insert the power module and then connect the power supply to the module.
- If the alarm does not clear after re-inserting, replace the power module.
- Check the input voltage value of the PSU using the **show environment power** command.
- If the input voltage is beyond the working range, check the power supplied to the PSU.

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).

Provisioning Failed Alarm

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

Logical Object: LC/Controller Name

The Provisioning Failed alarm is raised when invalid configuration is configured or invalid slice provisioning is made on the controller.

Clear the Provisioning Failed Alarm

Procedure

Step 1 Verify whether the provisioning configurations are supported for the line card.

Step 2 Change it to supported configurations for the line 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).

Provisioning in Progress Alarm

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

Logical Object: LC

The Provisioning in Progress alarm is raised when the provisioning request is in progress on the line card.

Clear the Provisioning in Progress Alarm

Procedure

Step 1 Verify the status of the alarm using the following debug command:

```
RP/0/RP0/CPU0:ios#show hw-module location '<0/n/NXR0>' mxponder
```

Step 2 Wait till the status changes to **Provisioned**.

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 Alarm

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

Logical Object: CLIENT

The REMOTE-FAULT alarm is raised on the NCS 1014 when a remote fault character sequence is received in the incoming MAC stream.

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 clear, log into the Technical 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-DEG-SER Alarm

Default Severity: Major

Logical Object: CLIENT

The remote FEC DEG-SER (Degraded SER) alarm is received from the remote Router when it sees Local Degraded SER on the receiver side.

Note On the 2.4TX card in the muxponder mode, this alarm is not supported for the split ports 2 and 3 for 600G and 1000G trunk rates respectively.

Clear the REMOTE-DEG-SER Alarm

Procedure

This alarm is cleared when you clear the errors at the remote 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).

RX-LOC

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

Logical Object: Line OTS Controller

Supported from release: R25.1.1

The RX-LOC alarm is raised when there is a loss in the fiber connection continuity.

When the RX-LOC alarm is raised at the line OTS, the following alarms at the controller and port are suppressed:

Table 1: Suppressed Alarms List

Alarms	Controller	Port
RX-LOS-P	• OSC • OTS • Line OTS-OCH	Line RX
TX-POWER-FAIL-LOW	• OTS • OTS-OCH	LINE TX
RX-LOS-P	OTS-OCH	Line RX

Clear the RX-LOC Alarm

Procedure

Check and repair any cut in fiber cable.

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).

SIA_GRACE_PERIOD_REMAINING

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

Logical Object: plat_sl_client

When the device enters an Out-of-Compliance (OOC) state, a grace period of 90 days begins. During this period, SIA license benefits can still be availed. The SIA_GRACE_PERIOD_REMAINING alarm is raised when a Software Innovation Access(SIA) upgrade is allowed during this grace period.

Clear SIA Grace Period Remaining

SUMMARY STEPS

1. This alarm is cleared when Software Innovation Access(SIA) licenses are purchased.

DETAILED STEPS

Procedure

This alarm is cleared when Software Innovation Access(SIA) licenses are purchased.

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

SIA_UPGRADE_BLOCKED

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

Logical Object: plat_sl_client

The SIA_UPGRADE_BLOCKED alarm is raised when Software Innovation Access(SIA) grace period has expired.

Clear SIA Grace Period Remaining

Procedure

This alarm is cleared when the SIA licences are purchased.

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

SIGLOSS Alarm

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

Logical Object: CLIENT

The Signal Loss on Data Interface (SIGLOSS) alarm is raised on the client-side QSFP when there is a loss of ethernet signal.

Clear the SIGLOSS Alarm

Procedure

Step 1 Ensure that the port connection at the near end of the client peer router is operational.

Step 2 Verify fiber continuity to the port.

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).

SPI_FLASH_CFG_INIT_ERR_E

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

Logical Object: ESD

The SPI_FLASH_CFG_INIT_ERR_E alarm is raised when there is an unsupported switch firmware version present.

Clear the SPI_FLASH_CFG_INIT_ERR_E Alarm

Procedure

Cisco IOS XR automatically detects and clears this alarm by resetting the Aldrin. If the alarm does not clear automatically:

- Restart the ESD process using the **process restart esd location 0/rp0/cpu0** command.
- Reload the rack using the **reload location 0/rack** command.

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).

SQUELCHED Alarm

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

Logical Object: CLIENT

Laser-squelching occurs on a QSFP pluggable when the upstream receive facility experiences loss of signal, loss of frame, flexo group indication mismatch, and OPU-CSF on client ports.

Clear the SQUELCHED Alarm

Procedure

This alarm will be cleared when optical alarms clear.

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).

SSD-ACCESS-ERROR

Default Severity: Critical (CR) ,Non-Service-Affecting(NSA)

Logical Object: Instorch

The SSD-ACCESS-ERROR is raised when the system cannot access the chassis SSD either because of chassis SSD corruption or because the chassis SSD has been removed.

Clear the SSD-ACCESS-ERROR Alarm

To clear this alarm:

Procedure

Step 1 Re-insert the chassis SSD if it is not properly inserted.

Step 2 If the alarm does not clear after reinserting, replace the corrupted SSD 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).

SWITCH_ALL_PORTS_DOWN_ERR_E

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

Logical Object: ESD

The SWITCH_ALL_PORTS_DOWN_ERR_E alarm is raised when all the switch ports are down.

Clear the SWITCH_ALL_PORTS_DOWN_ERR_E Alarm

Procedure

Cisco IOS XR automatically detects and clears this alarm by resetting the ports.

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).

SWITCH_CFG_INIT_ERR_E

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

Logical Object: ESD

The SWITCH_CFG_INIT_ERR_E alarm is raised when the initial switch configuration fails.

Clear the SWITCH_CFG_INIT_ERR_E Alarm

Procedure

Cisco IOS XR automatically detects and clears this alarm by resetting the switch.

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).

SWITCH_CRITICAL_PORT_FAILED_E

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

Logical Object: ESD

The SWITCH_CRITICAL_PORT_FAILED_E alarm is raised when there is a critical port failure.

Clear the SWITCH_CRITICAL_PORT_FAILED_E Alarm

Procedure

Cisco IOS XR automatically detects and clears this alarm by resetting the Aldrin. If the alarm does not clear automatically:

- Restart the ESD process using the **process restart esd location 0/rp0/cpu0** command.
- Reload the rack using the **reload location 0/rack** command.

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).

SWITCH_DMA_ERR_E

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

Logical Object: ESD

The SWITCH_DMA_ERR_E alarm is raised when the switch Direct Memory Access (DMA) engine fails.

Clear the SWITCH_DMA_ERR_E Alarm

Procedure

Cisco IOS XR automatically detects and clears this alarm by resetting the switch.

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).

SWITCH_EEPROM_INIT_ERR_E

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

Logical Object: ESD

The SWITCH_EEPROM_INIT_ERR_E alarm is raised when the Switch EEPROM initialization fails.

Clear the SWITCH_EEPROM_INIT_ERR_E Alarm

Procedure

Cisco IOS XR automatically detects and clears this alarm by resetting the switch.

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).

SWITCH_FDB_ERR_E

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

Logical Object: ESD

The SWITCH_FDB_ERR_E alarm is raised when the switch forwarding database (FDB) operation fails.

Clear the SWITCH_FDB_ERR_E Alarm

Procedure

Cisco IOS XR automatically detects and clears this alarm by resetting the switch.

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).

SWITCH_FDB_MAC_ADD_ERR_E

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

Logical Object: ESD

The SWITCH_FDB_MAC_ADD_ERR_E alarm is raised when the switch firmware is unable to add a MAC address to its database.

Clear the SWITCH_FDB_MAC_ADD_ERR_E Alarm

Procedure

To clear this alarm, contact technical support by logging into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html or call Cisco TAC (1 800 553-2447).

SWITCH_FIRMWARE_BOOT_FAIL_E

Default Severity: Critical (CR), Non-Service-Affecting (NSA)

Logical Object: ESD

The SWITCH_FIRMWARE_BOOT_FAIL_E alarm is raised when the switch firmware boot fails.

Clear the SWITCH_FIRMWARE_BOOT_FAIL_E Alarm

Procedure

This alarm can be cleared when the ESD auto clears the alarm by resetting the switch.

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).

SWITCH_NOT_DISCOVERED_E

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

Logical Object: ESD

The SWITCH_NOT_DISCOVERED_E alarm is raised when the switch is not discovered on the Peripheral Component Interconnect express (PCIe) bus.

Clear the SWITCH_NOT_DISCOVERED_E Alarm

Procedure

Cisco IOS XR automatically detects and clears this alarm by resetting the switch.

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).

SWITCH_RESET_RECOVERY_FAILED_E

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

Logical Object: ESD

The SWITCH_RESET_RECOVERY_FAILED_E alarm is raised when the Switch Reset operation does not recover the switch.

Clear the SWITCH_RESET_RECOVERY_FAILED_E Alarm

Procedure

Cisco IOS XR automatically detects and clears this alarm by reloading the card using the **reload cpu0/rp0** command.

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).

TD-FAILED

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

Logical Object: Controller OMS

The TD-FAILED alarm is raised when the Tone Detection fails.

Clear the TD-FAILED Alarm

Procedure

Stop Tone Detection on the corresponding controller using the **tone-pattern-detect controller ots** *R/S/I/P* **stop** command.

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).

TD-INPROGRESS

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

Logical Object: Controller OMS

The TD-INPROGRESS alarm is raised when the Tone Detection is in progress.

Clear the TD-INPROGRESS Alarm

Procedure

This alarm is cleared automatically when Tone Detection is completed successfully.

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).

TD-SUCCESS

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

Logical Object:Controller OMS

The TD-SUCCESS alarm is raised when Tone Detection is completed successfully.

Clear the TD-SUCCESS Alarm

Procedure

Stop Tone Detection on the corresponding controller using the **tone-pattern-detect controller ots** *R/S/I/P* **stop** command.

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).

TEMPERATURE

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

Note The severity of the alarm is determined by the temperature values detected by the sensor.

Logical Object: LC

The TEMPERATURE alarm is raised when the temperature of a sensor exceeds the normal operating range because of any of the following reasons:

- One or more fans stops working.
- Inadequate airflow.
- Environmental temperature of the room is abnormally high.

The alarm appears in the following format:

- [sensor name]: temperature alarm.

Clear the TEMPERATURE Alarm

Procedure

Step 1 Check the fan speed and temperature values using the **show environment** command.

Step 2 Check environmental temperature of the room is not abnormally high.

Step 3 Ensure that:

a) There are no airflow obstructions.

b) Fans are working fine.

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).

TIM Alarm

Default Severity: Critical, Service-Affecting (SA)

Logical Object: TRUNK

The Trail Trace Identifier Mismatch (TIM) alarm is raised when the expected TTI string does not match the received TTI string.

Clear the TIM Alarm

Procedure

Identify the cause for different expected and received TTI strings and resolve. The TIM mismatch can be caused due to mismatch in fiber connections.

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).

TX-POWER-FAIL-LOW

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

Logical Object: Controller DFB, Controller OSC, Controller OTS-OCH, Controller OMS, or Controller OCH

Supported from release: R25.1.1

The TX-POWER-FAIL-LOW alarm is raised when the output of the OTS power reading is below the Fail-Low threshold.

Clear the TX-POWER-FAIL-LOW Alarm

Procedure

Step 1 Check if the threshold values are correct using the **show controllers ots** *R/S/I/P* command.

Step 2 Check if the corresponding Rx power is correct using the **show controllers ots** *R/S/I/P* command. For example, an OTS Controller 2 TX receives power from the controller 0 RX.

Step 3 Check the configured EDFA gain values using the using the **show controllers ots** *R/S/I/P* command.

Step 4 Check for any hardware failure alarms using the **show alarms brief system active** command.

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).

UPGRADE_LICENSE_GRACE_PERIOD_REMAINING

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

Logical Object: plat_sl_client

The UPGRADE_LICENSE_GRACE_PERIOD_REMAINING alarm is raised when a software upgrade is allowed in the upgrade license grace period.

Clear Upgrade License Grace Period Remaining

SUMMARY STEPS

1. This alarm is cleared when SIA licenses are purchased.

DETAILED STEPS

Procedure

This alarm is cleared when SIA licenses are purchased.

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).

[Low | High] Voltage

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

Note The severity of the alarm is determined by the voltage values detected by the sensor.

Logical Object: LC

A [Low | High] Voltage is raised if any of the internal voltage measurements are not within the operating range. Following are the formats of the alarms along with their descriptions:

- *[sensor name]: high voltage alarm* is raised when the voltage is above the operating range.
- *[sensor name]: low voltage alarm* is raised when the voltage is below the operating range.

Clear the [Low | High] Voltage Alarm

Procedure

Verify the voltage of the power source. The voltage alarms clear automatically when the voltage is within the operating conditions. The voltage rating value varies depending on the standards of different countries for AC and DC power ranges.

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).

UNC-WORD Alarm

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

Logical Object: TRUNK

The Uncorrected FEC Word (UNC-WORD) condition is raised when the FEC is unable to correct the frame.

Clear the UNC-WORD Alarm

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 the optical receive levels are within the acceptable range.

Step 5 If the condition does not clear, verify that a single-mode fiber is used.

Step 6 Clean the fiber connectors at both ends for a signal degrade.

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).

UNSTABLE_LINK_E

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

Logical Object: ESD

The UNSTABLE_LINK_E alarm is raised when there is an unstable link with high number of UP and DOWN state changes.

Clear the UNSTABLE_LINK_E Alarm

Procedure

Cisco IOS XR automatically detects and clears this alarm by resetting the port.

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).

USB 0 Overcurrent Error

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

Logical Object: RP

The USB 0 Overcurrent Error alarm is raised when the over current is observed on USB0.

Clear the USB 0 Overcurrent Error Alarm

Procedure

This alarm is cleared automatically when the over current is removed for USB

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).

USB 1 Overcurrent Error

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

Logical Object: RP

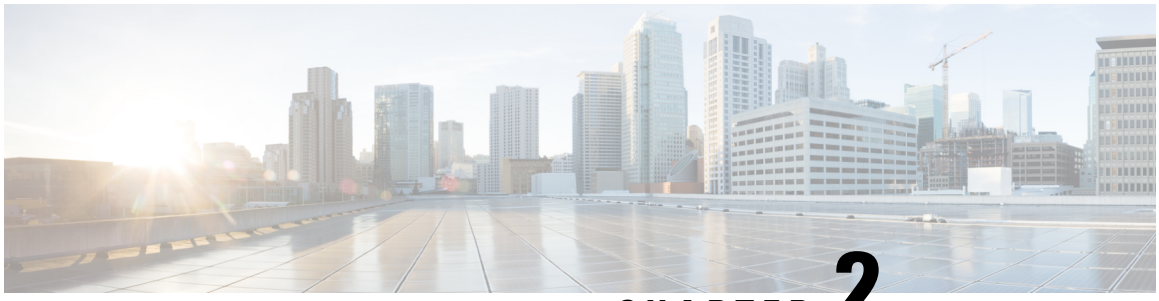
The USB 1 Overcurrent Error alarm is raised when the over current is observed on USB 1.

Clear the USB 1 Overcurrent Error Alarm

Procedure

This alarm is cleared automatically when the over current is removed for USB

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).



CHAPTER 2

General Troubleshooting

This chapter provides procedures for troubleshooting the most common problems encountered when operating the NCS 1014 chassis. To troubleshoot specific alarms, see the Alarm Troubleshooting chapter. If you cannot find what you are looking for, contact Cisco Technical Support (1 800 553-2447).

Capture Logs

When troubleshooting NCS 1014 issues, your technical support representative needs certain information about the situation and the symptoms that you are experiencing. To speed up the problem isolation and resolution process, collect the necessary data before you contact your representative.

To collect all debugging information, perform these steps:

.

Procedure

Step 1 **show logging**

Displays the contents of the logging buffers. You can also view details of FPD upgrade failures.

Example:

```
RP/0/RP0/CPU0:ios# show logging
Fri Nov 26 15:03:48.886 UTC
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
    Console logging: Disabled
    Monitor logging: level debugging, 0 messages logged
    Trap logging: level informational, 0 messages logged
    Buffer logging: level debugging, 1025 messages logged

Log Buffer (2097152 bytes):

RP/0/RP0/CPU0:Nov 25 16:40:28.533 UTC: syslogd[155]: %SECURITY-XR_SSL-6-INFO : XR SSL info: Setting
 fips register
RP/0/RP0/CPU0:Nov 25 16:40:36.323 UTC: cfgmgr-rp[120]: %MGBL-CONFIG-7-INTERNAL : Configuration Manager
 was unable to find subtree for 'sh_p_service_role_daemon' partition.  : cfgmgr-rp : (PID=2522) :
```

```
-Traceback= 7f1be3f92420 7f1be4bdd0c6 7f1be4bdd208 7f1be4bd74a4 7f1be4bd7e45 7f1be4bdb972 7f1be4bd7f0e
 55e025a46170 55e025a42429 55e025a3168f
RP/0/RP0/CPU0:Nov 25 16:40:36.457 UTC: aib[291]: Registering with IM
RP/0/RP0/CPU0:Nov 25 16:40:36.661 UTC: cma_partner[350]: Packet received on undiscovered module 160
RP/0/RP0/CPU0:Nov 25 16:40:37.113 UTC: ifmgr[142]: platform_pfi_ifh_get_if_alloc_info: Setting pic
.............
.............
```

Step 2 **show tech-support ncs1014**

Creates a .tgz file that contains the dump of the configuration and show command outputs. This file provides system information for the Cisco Technical Support.

Example:

```
RP/0/RP0/CPU0:ios# show tech-support ncs1014
Fri Nov 26 15:05:28.996 UTC
++ Show tech start time: 2021-Nov-26.150529.UTC ++
Fri Nov 26 15:05:30 UTC 2021 Waiting for gathering to complete
.....................................................................................................
Fri Nov 26 15:10:38 UTC 2021 Compressing show tech output
Show tech output available at 0/RP0/CPU0 :
/harddisk:/showtech/showtech-ncs1014-2021-Nov-26.150529.UTC.tgz
++ Show tech end time: 2021-Nov-26.151040.UTC ++
```

Step 3 **show tech-support install**

Collects the Cisco support file for the installation information. By default, the output of this command is saved on the NCS 1014 hard disk in a file with .tgz extension. Similarly, other show-tech-support commands can be used to gather data for a specific area.

Example:

```
RP/0/RP0/CPU0:N112#show tech-support install
++ Show tech start time: 2023-Dec-07.062636.UTC ++
Thu Dec  7 06:26:37 UTC 2023 Waiting for gathering to complete
.....................................................................................................
Thu Dec  7 06:32:48 UTC 2023 Compressing show tech output
Show tech output available at 0/RP0/CPU0 :
/harddisk:/showtech/showtech-N112-install-2023-Dec-07.062636.UTC.tgz
++ Show tech end time: 2023-Dec-07.063258.UTC ++
```

Using Onboard Failure Logging

Onboard Failure Logging (OBFL) collects and stores boot, environmental, and critical hardware data in the nonvolatile flash memory of the CPU controller card. This information is used for troubleshooting, testing, and diagnosis if a failure or other error occurs. This data provides improved accuracy in hardware troubleshooting and root cause isolation analysis. The data collected includes field-replaceable unit (FRU) serial number, OS version, total run time, boot status, temperature and voltage at boot, temperature and voltage history, and other board specific errors.

Procedure

show logging onboard {**fmea** | **inventory** | **temperature** | **uptime** | **voltage**}

Displays OBFL data.

Example:

The following example shows the *uptime* information.

```
sysadmin-vm:0_RP0# show logging onboard uptime

OBFL Uptime Information For : 0/RP0
       * indicates incomplete time-sync while record was written
       ! indicates time reset backwards while system was running
  ------------------------------------------------------------------------------------
       UPTIME CARD INFORMATION
  ------------------------------------------------------------------------------------
       Entity Name               :  Value
  ------------------------------------------------------------------------------------
      Previous Chassis SN        : CAT2311B0C5
      Current Chassis SN         : CAT2311B0CM
      Previous R/S/I             : 0/0/0
      Current R/S/I              : 0/0/0
      Write Interval             : 15 (min)
      First Power On TS          : 07/30/2019 07:33:56
      Last Erase TS              : --/--/---- --:--:--
      Rack Change Count          : 8
      Slot Change Count          : 8

  ------------------------------------------------------------------------------------
       UPTIME INFORMATION
  ------------------------------------------------------------------------------------
   Start Time (UTC)     | End Time (UTC)       | Card Uptime info
   mm/dd/yyyy hh:mm:ss | mm/dd/yyyy hh:mm:ss | Weeks.Days.Hrs.Min.Sec
  ------------------------------------------------------------------------------------
   10/28/2021 12:23:17 | 11/14/2021 21:09:18 | 2.3.8.46.1
   11/14/2021 21:09:18 | 11/18/2021 16:31:15 | 0.3.19.21.57
   11/18/2021 16:31:15 | 11/18/2021 21:10:35 | 0.0.4.39.20
   11/18/2021 21:10:35 | 11/19/2021 12:40:39 | 0.0.15.30.4
   11/19/2021 12:40:39 | 11/19/2021 14:16:10 | 0.0.1.35.31
   11/19/2021 14:16:10 | 11/22/2021 11:49:20 | 0.2.21.33.10
   11/22/2021 11:49:20 | 11/22/2021 22:51:48 | 0.0.11.2.28
   11/22/2021 22:51:48 | 11/23/2021 17:17:41 | 0.0.18.25.53
   11/24/2021 21:22:12 | 11/24/2021 23:11:16 | 0.0.1.49.4
   11/24/2021 23:11:16 | 11/24/2021 23:39:49 | 0.0.0.28.33
   11/24/2021 23:39:49 | 11/25/2021 15:25:32 | 0.0.15.45.43
   11/25/2021 15:25:32 | 11/25/2021 16:10:05 | 0.0.0.44.33
   11/25/2021 16:10:05 | 11/25/2021 16:25:08 | 0.0.0.15.3
   11/25/2021 16:25:08 | 11/25/2021 16:37:18 | 0.0.0.12.10
   11/25/2021 16:37:18 | 11/26/2021 15:08:27 | 0.0.22.31.9


OBFL Uptime Information For : 0/SC0
       * indicates incomplete time-sync while record was written
       ! indicates time reset backwards while system was running
  ------------------------------------------------------------------------------------
       UPTIME CARD INFORMATION
  ------------------------------------------------------------------------------------
       Entity Name               :  Value
  ------------------------------------------------------------------------------------
      Previous Chassis SN        : ------------
      Current Chassis SN         : CAT2311B0CM
      Previous R/S/I             : -/-/-
      Current R/S/I              : 0/1/0
      Write Interval             : 15 (min)
      First Power On TS          : 06/07/2019 08:52:42
      Last Erase TS              : --/--/---- --:--:--
      Rack Change Count          : 0
```

```
    Slot Change Count           : 0

-------------------------------------------------------------------------------
     UPTIME INFORMATION
-------------------------------------------------------------------------------
 Start Time (UTC)     | End Time (UTC)       | Card Uptime info
 mm/dd/yyyy hh:mm:ss | mm/dd/yyyy hh:mm:ss | Weeks.Days.Hrs.Min.Sec
-------------------------------------------------------------------------------
 10/24/2021 05:48:29 | 10/24/2021 06:27:51 | 0.0.0.39.22
 10/24/2021 06:27:51 | 10/24/2021 07:05:24 | 0.0.0.37.33
 10/24/2021 07:05:24 | 10/26/2021 23:43:32 | 0.2.16.38.8
 10/26/2021 23:43:32 | 10/26/2021 23:55:49 | 0.0.0.12.17
 10/26/2021 23:55:49 | 10/27/2021 00:09:49 | 0.0.0.14.0
 10/27/2021 00:09:49 | 10/27/2021 00:16:08 | 0.0.0.6.19
 10/27/2021 00:16:08 | 10/27/2021 23:37:51 | 0.0.23.21.43
 10/27/2021 23:37:51 | 10/27/2021 23:50:33 | 0.0.0.12.42
 11/24/2021 21:22:12 | 11/24/2021 23:11:16 | 0.0.1.49.4
 11/24/2021 23:11:16 | 11/24/2021 23:39:49 | 0.0.0.28.33
 11/24/2021 23:39:49 | 11/25/2021 15:25:32 | 0.0.15.45.43
 11/25/2021 15:25:32 | 11/25/2021 16:10:05 | 0.0.0.44.33
 11/25/2021 16:10:05 | 11/25/2021 16:25:08 | 0.0.0.15.3
 11/25/2021 16:25:08 | 11/25/2021 16:37:18 | 0.0.0.12.10
 11/25/2021 16:37:18 | 11/26/2021 15:09:27 | 0.0.22.32.9
```

Clear the CARD FAILED State

In Cisco NCS 1014, the "CARD FAILED" state indicates that a line card within the network system is no longer operational. This state typically suggests a hardware failure, software issue, or some other critical fault that prevents the card from doing its intended functions. Critical faults include *warm reload executed on a line card in shutdown state*.

Use this task to clear the CARD FAILED state of a line card located in rack 0 and slot 0.

Procedure

Step 1 Check the contents of the logging buffers.

The highlighted log suggests that a warm reload was executed on a line card in shutdown state. Only cold reload (reload location 0/*) can recover the LC from the shutdown state.

Example:

```
RP/0/RP0/CPU0:ios# show logging
Fri Nov 26 15:03:48.886 UTC
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
    Console logging: Disabled
    Monitor logging: level debugging, 0 messages logged
    Trap logging: level informational, 0 messages logged
    Buffer logging: level debugging, 1025 messages logged

Log Buffer (2097152 bytes):

RP/0/RP0/CPU0:Nov 25 16:40:28.533 UTC: syslogd[155]: %SECURITY-XR_SSL-6-INFO : XR SSL info: Setting
 fips register
RP/0/RP0/CPU0:Nov 25 16:40:36.323 UTC: cfgmgr-rp[120]: %MGBL-CONFIG-7-INTERNAL : Configuration Manager
```

```
 was unable to find subtree for 'sh_p_service_role_daemon' partition.  : cfgmgr-rp : (PID=2522) :
-Traceback= 7f1be3f92420 7f1be4bdd0c6 7f1be4bdd208 7f1be4bd74a4 7f1be4bd7e45 7f1be4bdb972 7f1be4bd7f0e
 55e025a46170 55e025a42429 55e025a3168f
RP/0/RP0/CPU0:Nov 25 16:40:36.457 UTC: aib[291]: Registering with IM
RP/0/RP0/CPU0:Nov 25 16:40:36.661 UTC: cma_partner[350]: Packet received on undiscovered module 160
RP/0/RP0/CPU0:Nov 25 16:40:37.113 UTC: ifmgr[142]: platform_pfi_ifh_get_if_alloc_info: Setting pic
RP/0/RP0/CPU0:Nov 25 16:30:38.122 UTC: shelfmgr[227]: %PLATFORM-SHELFMGR-3-OP_FAIL : Failed to reload
 0/0/NXR0: 'CPA_INTF' detected the 'fatal' condition 'Operation not supported'

.............
.............
```

Step 2 Carry out a cold restart of the affected device in rack 0 and slot 0.

Example:

```
RP/0/RP0/CPU0:ios# reload location 0/0
Fri Nov 26 15:03:48.886 UTC#
Proceed with reload? [confirm]
```

Step 3 Type `y` to continue.

Warning
The reload operation impacts the running traffic.

Wait for the device to restart and continue with the next step.

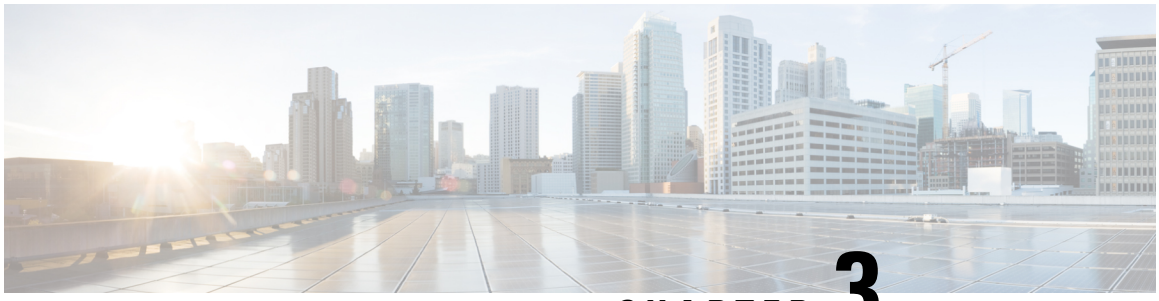
Step 4 Verify the state of the line card.

Now, you can see the line card in OPERATIONAL state.

Example:

```
RP/0/RP0/CPU0:ios#show platform
Node               Type                      State                     Config state
-------------------------------------------------------------------------------------
0/RP0/CPU0         NCS1K14-CNTLR-K9(Active)  IOS XR RUN                NSHUT,NMON
0/PM0              NCS1K4-AC-PSU             OPERATIONAL               NSHUT,NMON
0/PM1              NCS1K4-AC-PSU             OPERATIONAL               NSHUT,NMON
0/FT0              NCS1K14-FAN               OPERATIONAL               NSHUT,NMON
0/FT1              NCS1K14-FAN               OPERATIONAL               NSHUT,NMON
0/FT2              NCS1K14-FAN               OPERATIONAL               NSHUT,NMON
0/0/NXR0           NCS1K4-1.2T-K9            OPERATIONAL               NSHUT,NMON
0/1/NXR0           NCS1K14-2.4T-K9           OPERATIONAL               NSHUT,NMON
0/2/NXR0           NCS1K4-1.2T-K9            OPERATIONAL               NSHUT,NMON
0/3/NXR0           NCS1K4-1.2T-K9            OPERATIONAL               NSHUT,NMON
```

If the CARD FAILED state persists after a cold restart, contact your Cisco account representative or log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).



CHAPTER 3

Alarm Propagation Scenarios

In an optical network, alarm propagation defines how different alarms propagate in a larger link during any failure in the network. The alarm correlation algorithm suppresses the lower-priority alarms on each device in the network. Hence, the network administrator can assess the health of the optical network and detect the root cause of the problem by focusing only on the significant alarms on the node.

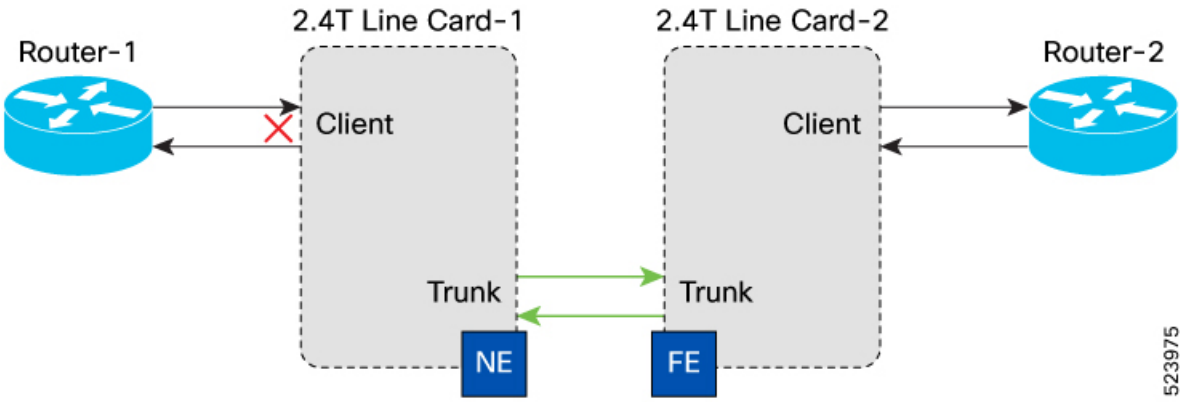
This chapter covers the alarms that are active and suppressed during the common alarm propagation scenarios when operating the NCS1K4-2.4T-K9 line card of the NCS 1014 chassis.

Client Unidirectional Receiver Fiber Cut

When there is a client unidirectional receiver fiber cut between Router-1 and 2.4T line card-1, alarms are raised and suppressed at the respective ports of each node.

This figure displays a client unidirectional receiver fiber cut.

Figure 1: Client Unidirectional Receiver Fiber Cut



These tables list the alarms raised at the respective ports of each node.

Table 2: Active and Suppressed Alarms for Near End (NE) Interface Faults

NE Interfaces	Active Alarms	Suppressed Alarms
Router 1	Remote Fault	No Alarms
NE_Client	SIGLOSS	No Alarms
NE_Trunk	No Alarms	No Alarms

Note From R24.4.x, when a fiber cut occurs on a Line RX port, if both the LOC and LOS-P alarms are present, the LOC alarm suppresses the LOS-P alarm. As a result, the LOS-P alarm is excluded from the output of the **show alarm brief system active** command but remains visible in the output of the **show controllers ots** command.

Table 3: Active and Suppressed Alarms for Far End (FE) Interface Faults

FE Interfaces	Active Alarms	Suppressed Alarms
Router 2	• Local Fault • LOCAL-DEG-SER	No Alarms
FE_Client	Remote Fault	No Alarms
FE_Trunk	OPUK-CSF	No Alarms

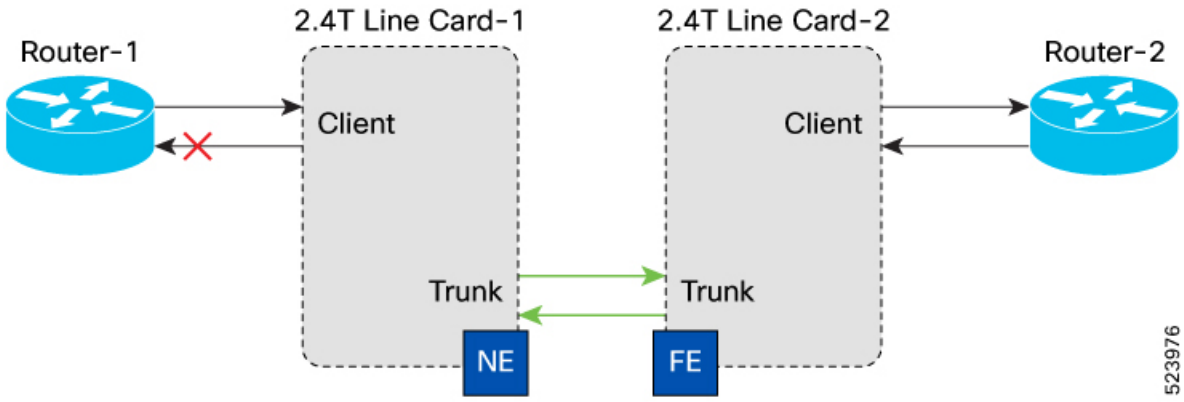
[1] The capability of the router is the determining factor for LD (LOCAL-DEG-SER) reporting. According to IEEE Standard 802.3, implementing Forward Error Correction (FEC) alarms is optional. However, if these alarms are supported, the router inserts an RD (Remote-Deg-Ser) in the upstream direction in response to the LD (Local-FEC -Deg-Ser) alarm.

Client Unidirectional Transmitter Fiber Cut

When there is a client unidirectional transmitter fiber cut between Router-1 and 2.4T Line Card-1, alarms are raised and suppressed at the respective ports of each node.

This figure displays the client unidirectional transmitter fiber cut.

Figure 2: Client Unidirectional Transmitter Fiber Cut



The following tables list the alarms that are raised at the respective ports of each node.

Table 4: Active and Suppressed Alarms for Near End (NE) Interface Faults

Node	Active Alarms	Suppressed Alarms
Router 1	LOSS	No Alarms
NE_Client	Remote Fault	No Alarms
NE_Trunk	No Alarms	No Alarms

Table 5: Active and Suppressed Alarms for Far End (FE) Interface Faults

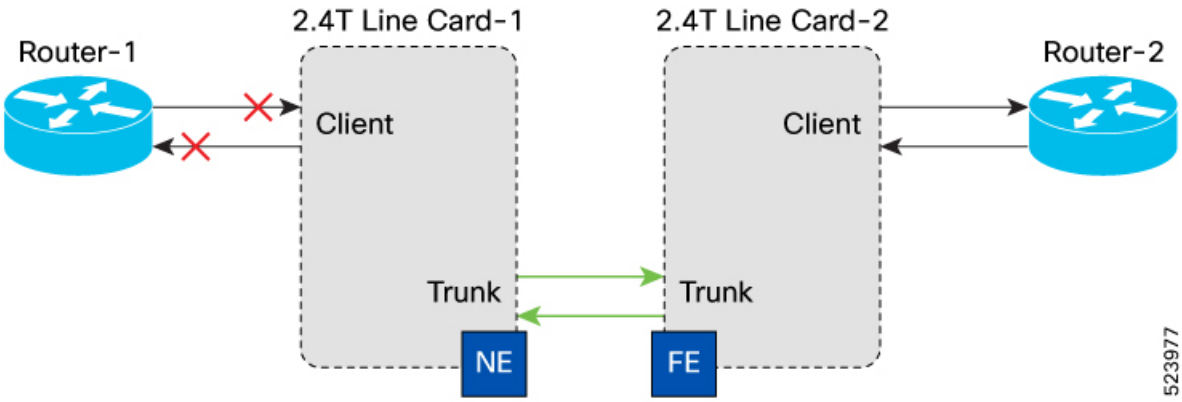
Node	Active Alarms	Suppressed Alarms
Router 2	Remote Fault	No Alarms
FE_Client	No Alarms	No Alarms
FE_Trunk	No Alarms	No Alarms

Client Bi-directional Fiber Cut

When there is a client bi-directional fiber cut between Router-1 and 2.4T Line Card-1, alarms are raised and suppressed at the respective ports of each node.

This figure displays a client bi-directional receiver fiber cut.

Figure 3: Client Bi-directional Fiber Cut



These tables list the alarms that are raised at the respective ports of each node.

Table 6: Active and Suppressed Alarms for Near End (NE) Interface Faults

Node	Active Alarms	Suppressed Alarms
Router 1	LOSS	No Alarms
NE_Client	SIGLOSS	No Alarms
NE_Trunk	No Alarms	No Alarms

Table 7: Active and Suppressed Alarms for Far End (FE) Interface Faults

Node	Active Alarms	Suppressed Alarms
Router 2	• Local Fault • LD[2]	No Alarms
FE_Client	Remote Fault	No Alarms
FE_Trunk	OPUK-CSF	No Alarms

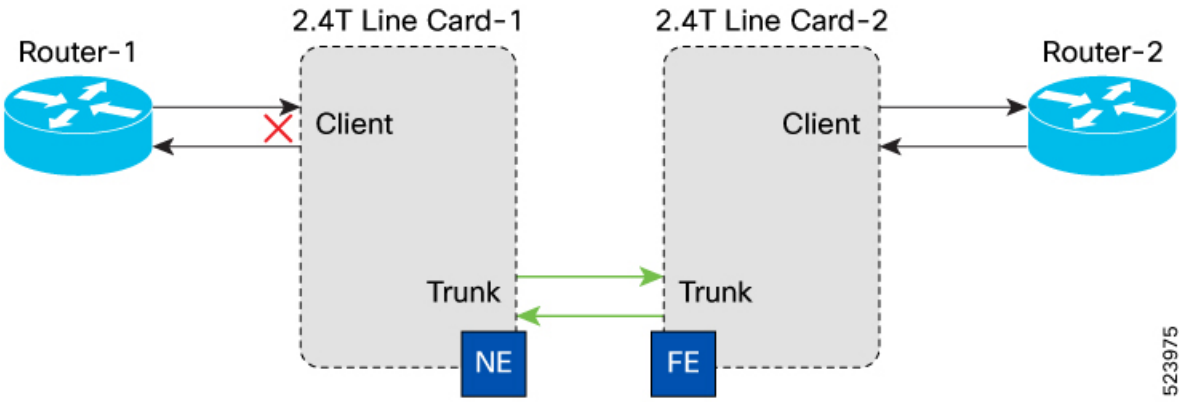
[2] The capability of the router is the determining factor for LD (LOCAL-DEG-SER) reporting. According to IEEE Standard 802.3, implementing Forward Error Correction (FEC) alarms is optional. However, if these alarms are supported, the router inserts an RD (Remote-Deg-Ser) in the upstream direction in response to the LD (Local-FEC -Deg-Ser) alarm.

Client Unidirectional Loss of Synchronization on Data Interface

When there is a client unidirectional Loss of Synchronization on Data Interface (SYNCLOSS) between Router-1 and 2.4T line card-1, alarms are raised and suppressed at the respective ports of each node.

This figure displays the unidirectional SYNCLOSS.

Figure 4: Client Unidirectional SYNCLOSS



These tables list the alarms that are raised and suppressed at the respective ports of each node.

Table 8: Active and Suppressed Alarms for Near End (NE) Interface Faults

Node	Active Alarms	Suppressed Alarms
Router 1	Remote Fault	No Alarms
NE_Client	SYNCLOSS	No Alarms
NE_Trunk	No Alarms	No Alarms

Table 9: Active and Suppressed Alarms for Far End (FE) Interface Faults

Node	Active Alarms	Suppressed Alarms
Router 2	• Local Fault • LOCAL-DEG-SER[3]	No Alarms
FE_Client	Remote Fault	No Alarms
FE_Trunk	OPUK-CSF	No Alarms

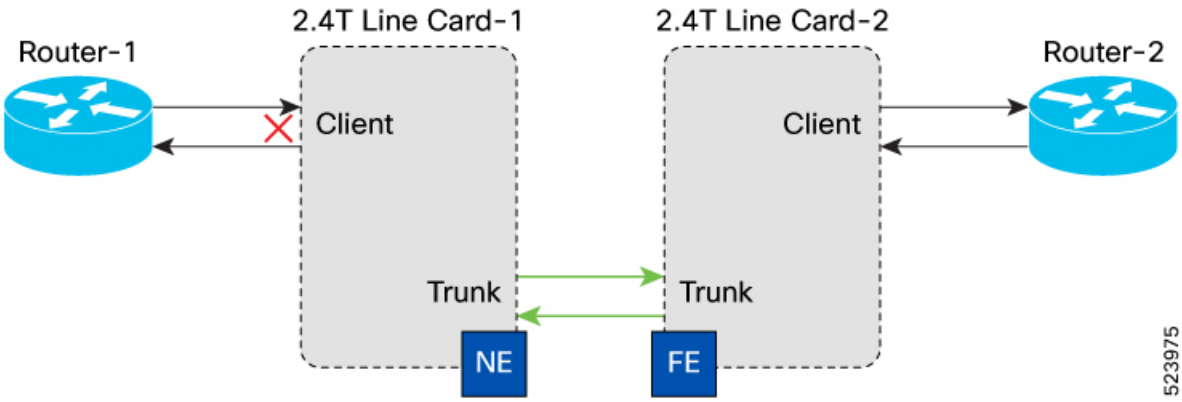
[3] The capability of the router is the determining factor for LD (LOCAL-DEG-SER) reporting. According to IEEE Standard 802.3, implementing Forward Error Correction (FEC) alarms is optional. However, if these alarms are supported, the router inserts an RD (Remote-Deg-Ser) in the upstream direction in response to the LD (Local-FEC -Deg-Ser) alarm.

Client Unidirectional LOCAL FAULT

When there is a client unidirectional LOCAL FAULT (LF) between Router-1 and 2.4T Line Card-1, alarms are raised and suppressed at the respective ports of each node.

This figure displays unidirectional LF.

Figure 5: Client Unidirectional LF



These tables list the alarms that are raised and suppressed at the respective ports of each node.

Table 10: Active and Suppressed Alarms for Near End (NE) Interface Faults

Node	Active Alarms	Suppressed Alarms
Router 1	Remote Fault	No Alarms
NE_Client	Local Fault	No Alarms
NE_Trunk	No Alarms	No Alarms

Table 11: Active and Suppressed Alarms for Far End (FE) Interface Faults

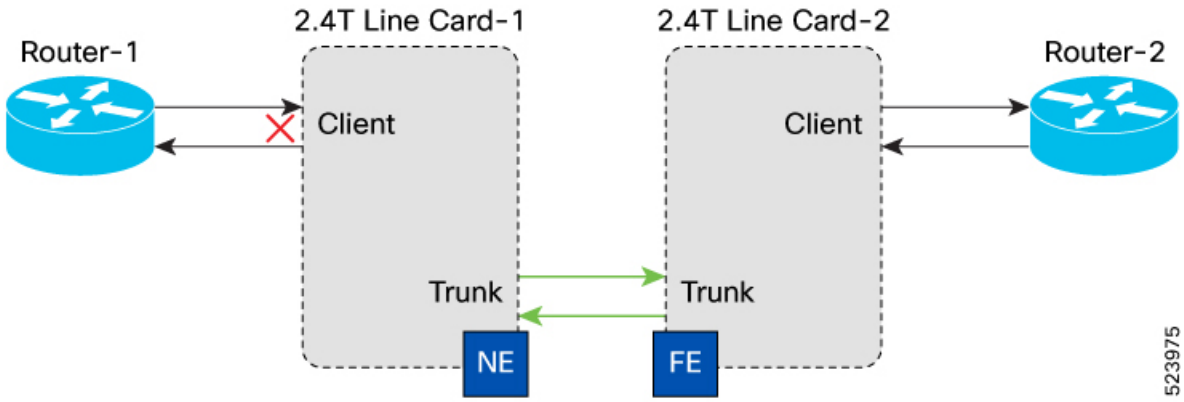
Node	Active Alarms	Suppressed Alarms
Router 2	Local Fault	No Alarms
FE_Client	Remote Fault	No Alarms
FE_Trunk	No Alarms	No Alarms

Client Unidirectional REMOTE-FAULT

When there is a client unidirectional REMOTE-FAULT (RF) between Router-1 and 2.4T Line Card-1, alarms are raised and suppressed at the respective ports of each node.

This figure displays unidirectional RF.

Figure 6: Client Unidirectional RF



These tables list the alarms that are raised and suppressed at the respective ports of each node:

Table 12: Active and Suppressed Alarms for Near End (NE) Interface Faults

Node	Active Alarms	Suppressed Alarms
Router 1	Any fault can be triggered (In case of LOSS/LF, Remote fault is triggered).	No Alarms
NE_Client	Remote Fault	No Alarms
NE_Trunk	No Alarms	No Alarms

Table 13: Active and Suppressed Alarms for Far End (FE) Interface Faults

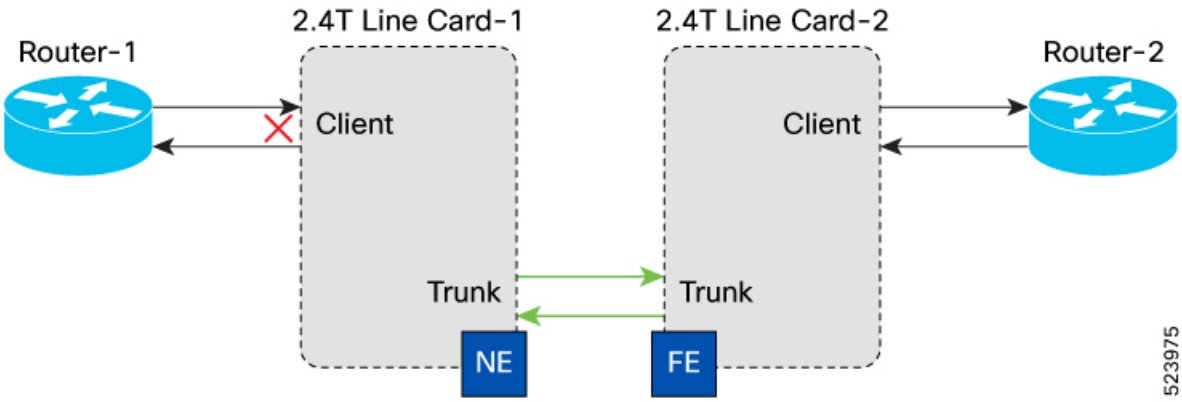
Node	Active Alarms	Suppressed Alarms
Router 2	Remote Fault	No Alarms
FE_Client	No Alarms	No Alarms
FE_Trunk	No Alarms	No Alarms

Client Unidirectional High Symbol Error Rate

When there is a client unidirectional High Symbol Error Rate (Hi-SER) between Router-1 and 2.4T Line Card-1, alarms are raised and suppressed at the respective ports of each node.

This figure displays client unidirectional Hi-SER fault.

Figure 7: Client Unidirectional HI-SER



These tables list the alarms that are raised at the respective ports of each node:

Table 14: Active and Suppressed Alarms for Near End (NE) Interface Faults

Node	Active Alarms	Suppressed Alarms
Router-1	No Alarms	No Alarms
NE_Client	• HI-SER • DEG-SER	No Alarms
NE_Trunk	No Alarms	No Alarms

Table 15: Active and Suppressed Alarms for Far End (FE) Interface Faults

Node	Active Alarms	Suppressed Alarms
Router -2	LOCAL-DEG-SER[4]	No Alarms
FE_Client	No Alarms	No Alarms
FE_Trunk	No Alarms	No Alarms

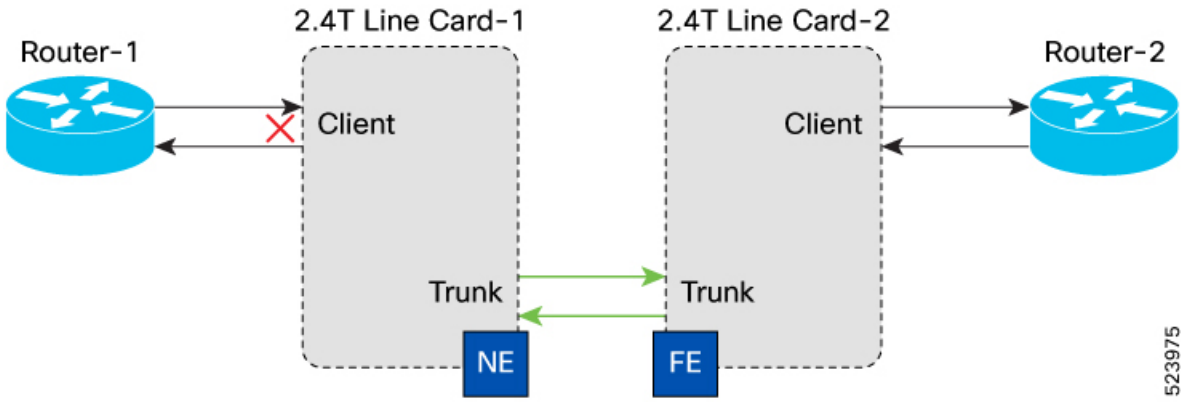
[4] The capability of the router is the determining factor for LD (LOCAL-DEG-SER) reporting. According to IEEE Standard 802.3, implementing Forward Error Correction (FEC) alarms is optional. However, if these alarms are supported, the router inserts an RD (Remote-Deg-Ser) in the upstream direction in response to the LD (Local-FEC -Deg-Ser) alarm.

Client Unidirectional Degraded Symbol Error Rate

When there is a client unidirectional Degraded Symbol Error Rate (DEG-SER) between Router-1 and 2.4T Line Card-1, alarms are raised and suppressed at the respective ports of each node.

This figure displays client unidirectional DEG-SER:

Figure 8: Client Unidirectional DEG-SER



These tables list the alarms that are raised at the respective ports of each node:

Table 16: Active and Suppressed Alarms for Near End (NE) Interface Faults

Node	Active Alarms	Suppressed Alarms
Router-1	No Alarms	No Alarms
NE_Client	DEG-SER Example: DEG-SER :DECLARE: FourHundredGigECtrlr0/1/0/1:	No Alarms
NE_Trunk	No Alarms	No Alarms

Table 17: Active and Suppressed Alarms for Far End (FE) Interface Faults

Node	Active Alarms	Suppressed Alarms
Router-2	LOCAL-DEG-SER[5]	No Alarms
FE_Client	No Alarms	No Alarms
FE_Trunk	No Alarms	No Alarms

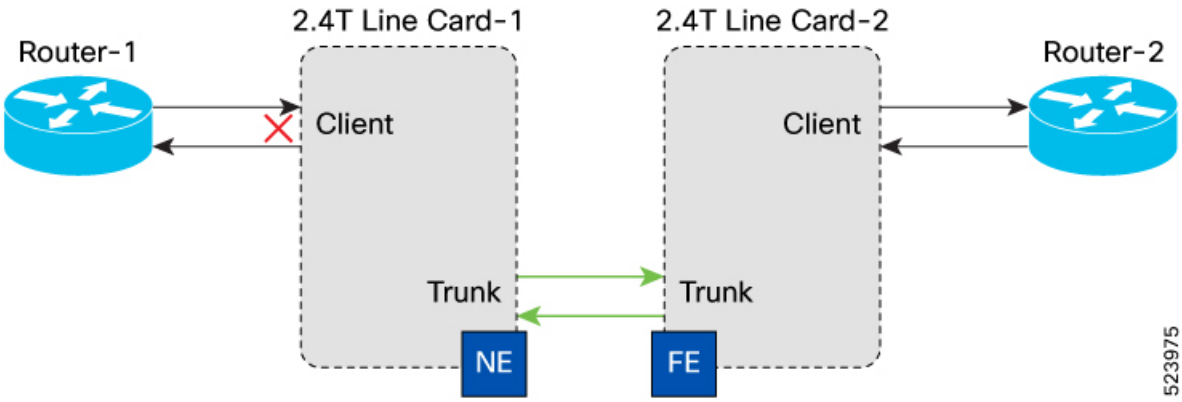
[5] The capability of the router is the determining factor for LD (LOCAL-DEG-SER) reporting. According to IEEE Standard 802.3, implementing Forward Error Correction (FEC) alarms is optional. However, if these alarms are supported, the router inserts an RD (Remote-Deg-Ser) in the upstream direction in response to the LD (Local-FEC -Deg-Ser) alarm.

Client Unidirectional LOCAL-DEG-SER

When there is a client unidirectional LOCAL-DEG-SER (LD) between Router-1 and 2.4T Line Card-1, alarms are raised and suppressed at the respective ports of each node.

This figure displays client unidirectional LD.

Figure 9: Client Unidirectional LD



These tables list the alarms that are raised at the respective ports of each node.

Table 18: Active and Suppressed Alarms for Near End (NE) Interface Faults

Node	Active Alarms	Suppressed Alarms
Router-1	No Alarms	No Alarms
NE_Client	LOCAL-DEG-SER	No Alarms
NE_Trunk	No Alarms	No Alarms

Table 19: Active and Suppressed Alarms for Far End (FE) Interface Faults

Node	Active Alarms	Suppressed Alarms
Router 2	LOCAL-DEG-SER[6]	No Alarms
FE_Client	No Alarms	No Alarms
FE_Trunk	No Alarms	No Alarms

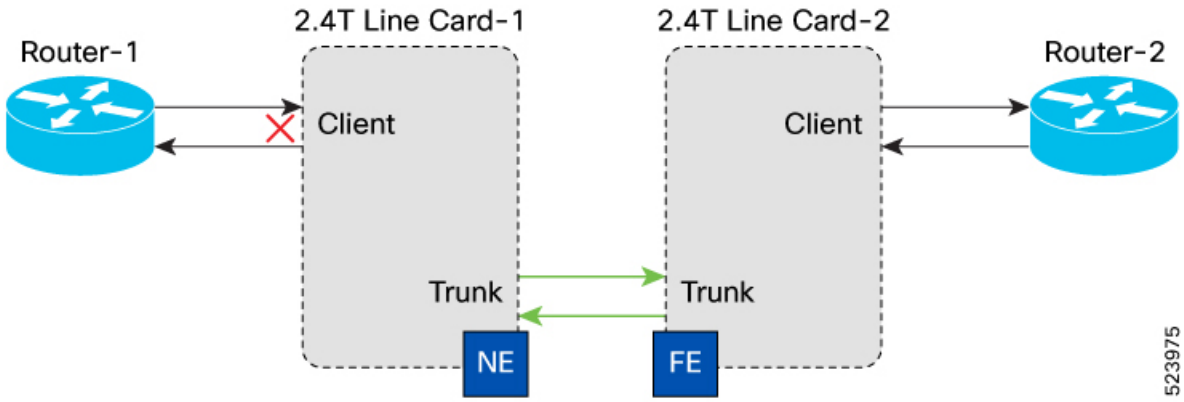
[6] The capability of the router is the determining factor for LD (LOCAL-DEG-SER) reporting. According to IEEE Standard 802.3, implementing Forward Error Correction (FEC) alarms is optional. However, if these alarms are supported, the router inserts an RD (Remote-Deg-Ser) in the upstream direction in response to the LD (Local-FEC -Deg-Ser) alarm.

Client Unidirectional REMOTE-DEG-SER

When there is a client unidirectional REMOTE-DEG-SER (RD) between Router-1 and 2.4T Line Card-1, alarms are raised and suppressed at the respective ports of each node.

This figure displays client unidirectional RD.

Figure 10: Client Unidirectional RD



These tables list the alarms that are raised at the respective ports of each node.

Table 20: Active and Suppressed Alarms for Near End (NE) Interface Faults

Node	Active Alarms	Suppressed Alarms
Router 1	LOCAL-DEG-SER[7]	No Alarms
NE_Client	REMOTE-DEG-SER	No Alarms
NE_Trunk	No Alarms	No Alarms

[7] The capability of the router is the determining factor for LD (LOCAL-DEG-SER) reporting. According to IEEE Standard 802.3, implementing Forward Error Correction (FEC) alarms is optional. However, if these alarms are supported, the router inserts an RD (Remote-Deg-Ser) in the upstream direction in response to the LD (Local-FEC -Deg-Ser) alarm.

Table 21: Active and Suppressed Alarms for Far End (FE) Interface Faults

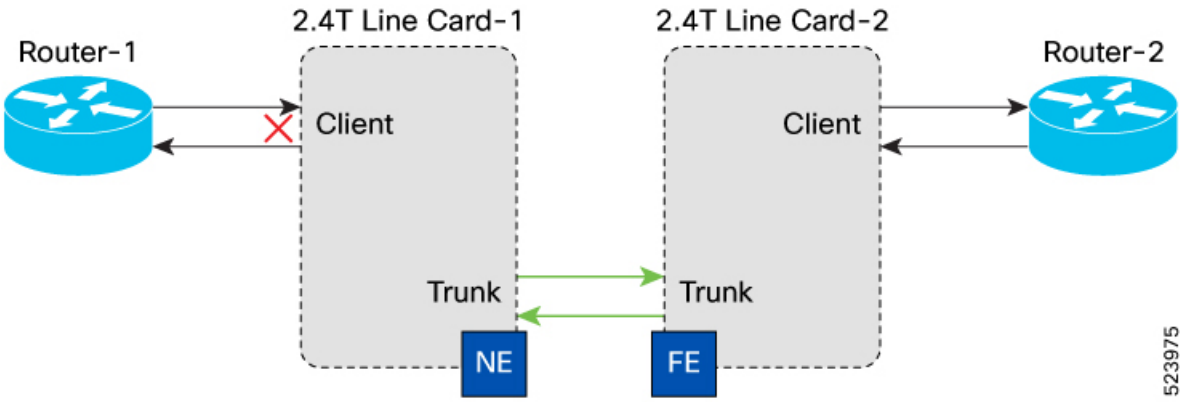
Node	Active Alarms	Suppressed Alarms
Router 2	RD	No Alarms
FE_Client	No Alarms	No Alarms
FE_Trunk	No Alarms	No Alarms

Client Unidirectional Improper Removal

When there is a client unidirectional Improper Removal (IMPROPRMVL) between Router-1 and 2.4T Line Card-1, alarms are raised and suppressed at the respective ports of each node.

This figure displays client unidirectional IMPROPRMVL.

Figure 11: Client Unidirectional IMPROPRMVL



These tables lists the alarms that are raised at the respective ports of each node.

Table 22: Active and Suppressed Alarms for Near End (NE) Interface Faults

Node	Active Alarms	Suppressed Alarms
Router-1	LOS	No Alarms
NE_Client	IMPROPRMVL	SYNCLOSS
NE_Trunk	No Alarms	No Alarms

Table 23: Active and Suppressed Alarms for Far End (FE) Interface Faults

Node	Active Alarms	Suppressed Alarms
Router-2	• Local Fault • LOCAL-DEG-SER[8]	No Alarms
FE_Client	Remote Fault	No Alarms
FE_Trunk	OPUK-CSF	No Alarms

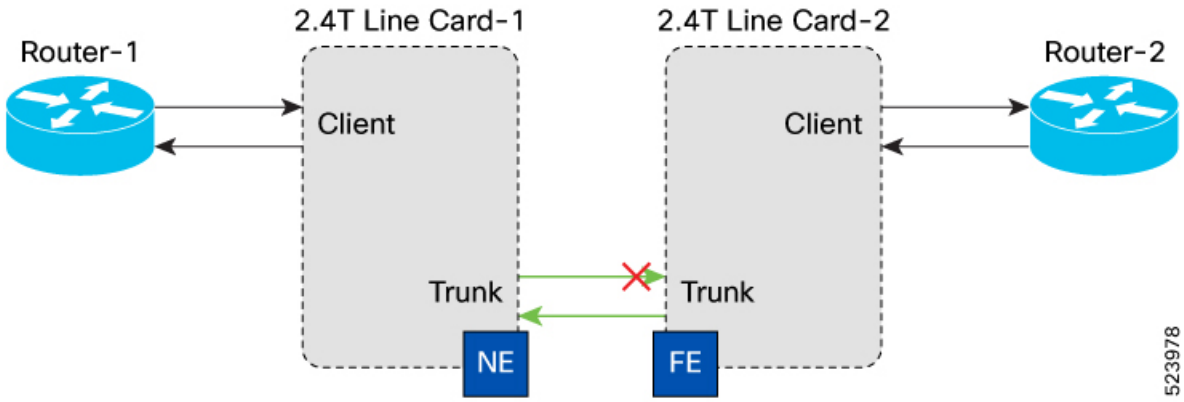
[8] The capability of the router is the determining factor for LD (LOCAL-DEG-SER) reporting. According to IEEE Standard 802.3, implementing Forward Error Correction (FEC) alarms is optional. However, if these alarms are supported, the router inserts an RD (Remote-Deg-Ser) in the upstream direction in response to the LD (Local-FEC -Deg-Ser) alarm.

Trunk Unidirectional Fiber Cut

When there is a trunk unidirectional fiber cut between 2.4T line card-1 and 2.4T line card-2, alarms are raised and suppressed at the respective ports of each node.

This figure displays trunk unidirectional fiber cut.

Figure 12: Trunk Unidirectional Fiber Cut



These tables list the alarms that are raised at the respective ports of each node.

Table 24: Active and Suppressed Alarms for Near End (NE) Interface Faults

Node	Active Alarms	Suppressed Alarms
Router-1	Remote Fault	No Alarms
NE_Client	No Alarms	No Alarms
NE_Trunk	• FLEXO-RDI • ODUK-BDI-PM	No Alarms

Table 25: Active and Suppressed Alarms for Far End (FE) Interface Faults

Node	Active Alarms	Suppressed Alarms
Router-2	• Local Fault • LOCAL-DEG-SER[9]	No Alarms
FE_Client	Remote Fault	No Alarms
FE_Trunk	LOS-P	No Alarms

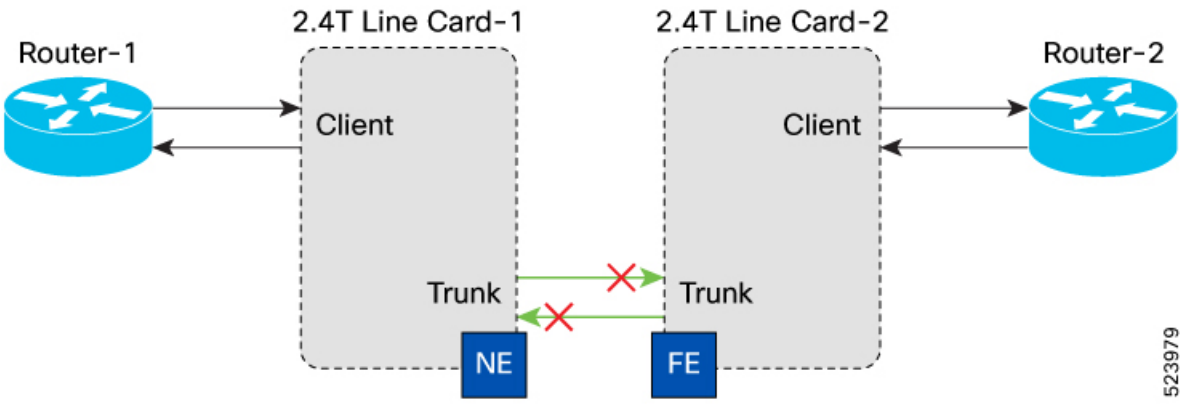
[9] The capability of the router is the determining factor for LD (LOCAL-DEG-SER) reporting. According to IEEE Standard 802.3, implementing Forward Error Correction (FEC) alarms is optional. However, if these alarms are supported, the router inserts an RD (Remote-Deg-Ser) in the upstream direction in response to the LD (Local-FEC -Deg-Ser) alarm.

Trunk Bidirectional Fiber Cut

When there is a trunk bi-directional fiber cut between 2.4T line card-1 and 2.4T line card-2 alarms are raised and suppressed at the respective ports of each node.

This figure displays trunk bidirectional fiber cut.

Figure 13: Trunk Bi-directional Fiber Cut



These tables list the alarms that are raised at the respective ports of each node.

Table 26: Near End (NE) Interface Faults: Active and Suppressed Alarms

Node	Active Alarms	Suppressed Alarms
Router 1	• LOCAL-DEG-SER[10] • Local Fault	No Alarms
NE_Client	Remote Fault	No Alarms
NE_Trunk	LOS-P	No Alarms

[10] The capability of the router is the determining factor for LD (LOCAL-DEG-SER) reporting. According to IEEE Standard 802.3, implementing Forward Error Correction (FEC) alarms is optional. However, if these alarms are supported, the router inserts an RD (Remote-Deg-Ser) in the upstream direction in response to the LD (Local-FEC -Deg-Ser) alarm.

Table 27: Active and Suppressed Alarms for Far End (FE) Interface Faults

Node	Active Alarms	Suppressed Alarms
Router 2	• Local Fault • LOCAL-DEG-SER[11]	No Alarms
FE_Client	Remote Fault	No Alarms
FE_Trunk	LOS-P	No Alarms

[11] The capability of the router is the determining factor for LD (LOCAL-DEG-SER) reporting. According to IEEE Standard 802.3, implementing Forward Error Correction (FEC) alarms is optional. However, if these alarms are supported, the router inserts an RD (Remote-Deg-Ser) in the upstream direction in response to the LD (Local-FEC -Deg-Ser) alarm.

Trunk Frequency Mismatch - Complete Offset with 150GHz Spacing

When there is a trunk frequency mismatch between 2.4T line card-1 and 2.4T line card-2 alarms, are raised and suppressed at the respective ports of each node.

This figure displays trunk frequency mismatch for complete offset with 150GHz spacing.

Figure 14: Trunk Frequency Mismatch

These tables list the alarms that are raised at the respective ports of each node.

Table 28: Active and Suppressed Alarms for Near End (NE) Interface Faults

Node	Active Alarms	Suppressed Alarms
Router-1	• Local Fault • LOCAL-DEG-SER[12]	No Alarms
NE_Client	Remote Fault	No Alarms
NE_Trunk	LOS-P	No Alarms

[12] The capability of the router is the determining factor for LD (LOCAL-DEG-SER) reporting. According to IEEE Standard 802.3, implementing Forward Error Correction (FEC) alarms is optional. However, if these alarms are supported, the router inserts an RD (Remote-Deg-Ser) in the upstream direction in response to the LD (Local-FEC -Deg-Ser) alarm.

Table 29: Active and Suppressed Alarms for Far End (FE) Interface Faults

Node	Active Alarms	Suppressed Alarms
Router -2	• Local Fault • LOCAL-DEG-SER[13]	No Alarms
FE_Client	Remote Fault	No Alarms
FE_Trunk	LOS-P	No Alarms

[13] The capability of the router is the determining factor for LD (LOCAL-DEG-SER) reporting. According to IEEE Standard 802.3, implementing Forward Error Correction (FEC) alarms is optional. However, if these alarms are supported, the router inserts an RD (Remote-Deg-Ser) in the upstream direction in response to the LD (Local-FEC -Deg-Ser) alarm.

Trunk Frequency Mismatch - Partial Offset with 75GHz Spacing

When there is a trunk frequency mismatch between 2.4T line card-1 and 2.4T line card-2 alarms, are raised and suppressed at the respective ports of each node.

The following figure displays trunk frequency mismatch for partial offset with 75GHz spacing::

Figure 15: Trunk Frequency Mismatch

These tables list the alarms that are raised at the respective ports of each node.

Table 30: Active and Suppressed Alarms for Near End (NE) Interface Faults

NE Interface Faults		
Node	**Active Alarms**	**Suppressed Alarms**
Router-1	• LF • LD[14]	No Alarms
NE_Client	RF Example, RF: DECLARE :FourHundredGigECtrlr0/1/0/1	No Alarms
NE_Trunk	FLEXO-LOF & OSNR Example: FLEXO-LOF :DECLARE :CoherentDSP0/1/0/0: OSNR :DECLARE :Optics0/1/0/0	No Alarms

[14] The capability of the router is the determining factor for LD (LOCAL-DEG-SER) reporting. According to IEEE Standard 802.3, implementing Forward Error Correction (FEC) alarms is optional. However, if these alarms are supported, the router inserts an RD (Remote-Deg-Ser) in the upstream direction in response to the LD (Local-FEC -Deg-Ser) alarm.

Table 31: Active and Suppressed Alarms for Far End (FE) Interface Faults

FE Interface Faults		
Node	**Active Alarms**	**Suppressed Alarms**
Router -2	• LF • LD[15]	No Alarms
FE_Client	RF Example, RF: DECLARE : FourHundredGigECtrlr0/1/0/1	No Alarms
FE_Trunk	FLEXO-LOF & OSNR Example: FLEXO-LOF :DECLARE : CoherentDSP0/1/0/0: OSNR :DECLARE :Optics0/1/0/0	No Alarms

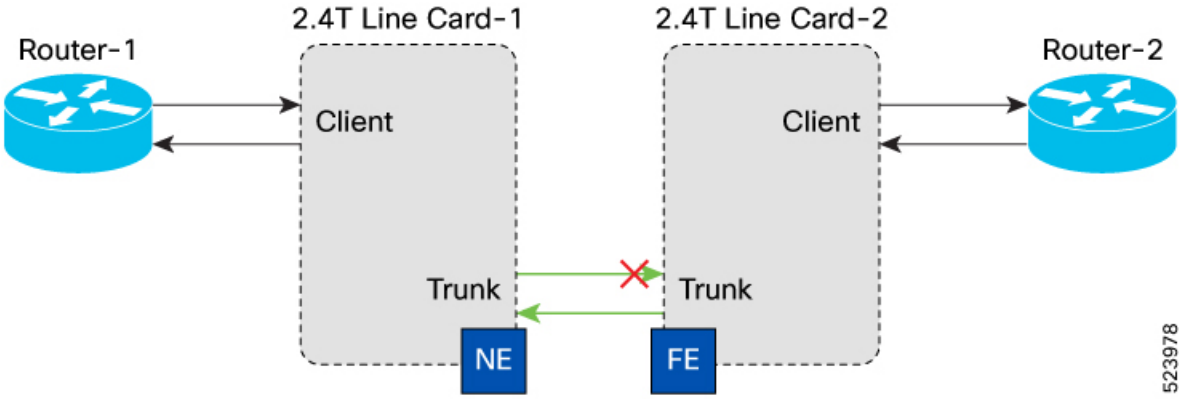
[15] The capability of the router is the determining factor for LD (LOCAL-DEG-SER) reporting. According to IEEE Standard 802.3, implementing Forward Error Correction (FEC) alarms is optional. However, if these alarms are supported, the router inserts an RD (Remote-Deg-Ser) in the upstream direction in response to the LD (Local-FEC -Deg-Ser) alarm.

Trunk Unidirectional Loss of Frame

When there is a trunk unidirectional Loss of Frame (LOF) between 2.4T line card-1 and 2.4T line card-2, alarms are raised and suppressed at the respective ports of each node.

This figure displays trunk LOF.

Figure 16: Trunk Unidirectional LOF



These tables list the alarms that are raised at the respective ports of each node.

Table 32: Active and Suppressed Alarms for Near End (NE) Interface Faults

Node	Active Alarms	Suppressed Alarms
Router-1	RF	No Alarms
NE_Client	No Alarms	No Alarms
NE_Trunk	• FLEXO-RDI Example: FLEXO-RDI :DECLARE :CoherentDSP0/1/0/0: • ODUK-BDI-PM Example: ODUK-BDI-PM :DECLARE :ODU-FLEX0/1/0/0/1:	No Alarms

Table 33: Active and Suppressed Alarms for Far End (FE) Interface Faults

Node	Active Alarms	Suppressed Alarms

Router -2	• LF • LD[16]	No Alarms
FE_Client	RF Example, RF: DECLARE :FourHundredGigECtrlr0/1/0/1	No Alarms
FE_Trunk	• FLEXO-LOF Example: FLEXO-LOF :DECLARE :CoherentDSP0/1/0/0: • OSNR Example: OSNR:DECLARE :Optics0/1/0/0:	No Alarms

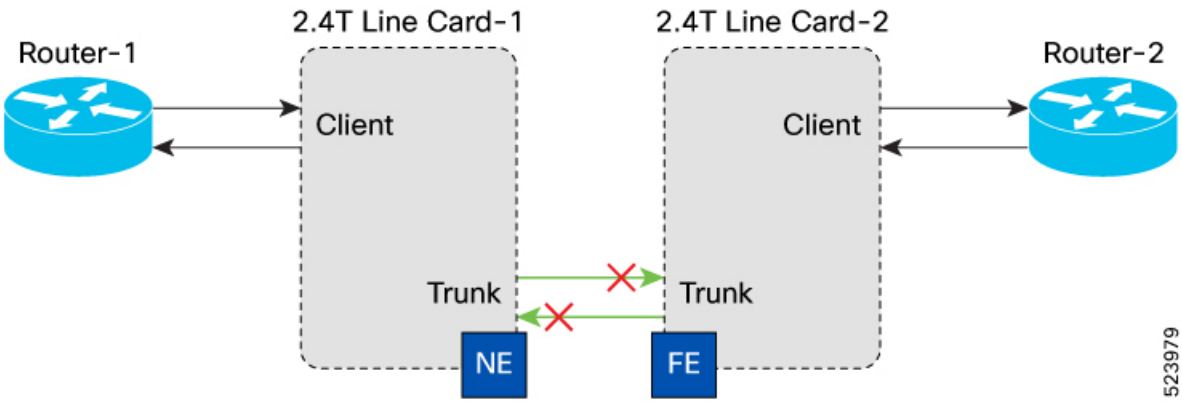
[16] The capability of the router is the determining factor for LD (LOCAL-DEG-SER) reporting. According to IEEE Standard 802.3, implementing Forward Error Correction (FEC) alarms is optional. However, if these alarms are supported, the router inserts an RD (Remote-Deg-Ser) in the upstream direction in response to the LD (Local-FEC -Deg-Ser) alarm.

Trunk Group ID Mismatch

When there is a trunk Group ID Mismatch (GIDM) between 2.4T line card-1 and 2.4T line card-2, alarms are raised and suppressed at the respective ports of each node.

The following figure displays trunk GIDM:

Figure 17: Trunk GIDM



The following tables list the alarms that are raised at the respective ports of each node:

Table 34: Active and Suppressed Alarms for Near End (NE) Interface Faults

Node	Active Alarms	Suppressed Alarms

Router-1	• LD • LF	No Alarms
NE_Client	RF Example: RF :DECLARE :FourHundredGigECtrlr0/1/0/1	No Alarms
NE_Trunk	Flexo-GIDM Example: Flexo-GIDM :DECLARE :CoherentDSP0/1/0/0:	No Alarms

Table 35: Active and Suppressed Alarms for Far End (FE) Interface Faults

Node	Active Alarms	Suppressed Alarms
Router-2	• LF • LD[17]	No Alarms
FE_Client	RF Example, RF: DECLARE :FourHundredGigECtrlr0/1/0/1	No Alarms
FE_Trunk	FLEXO-GIDM Example: FLEXO-GIDM :DECLARE :CoherentDSP0/1/0/0:	No Alarms

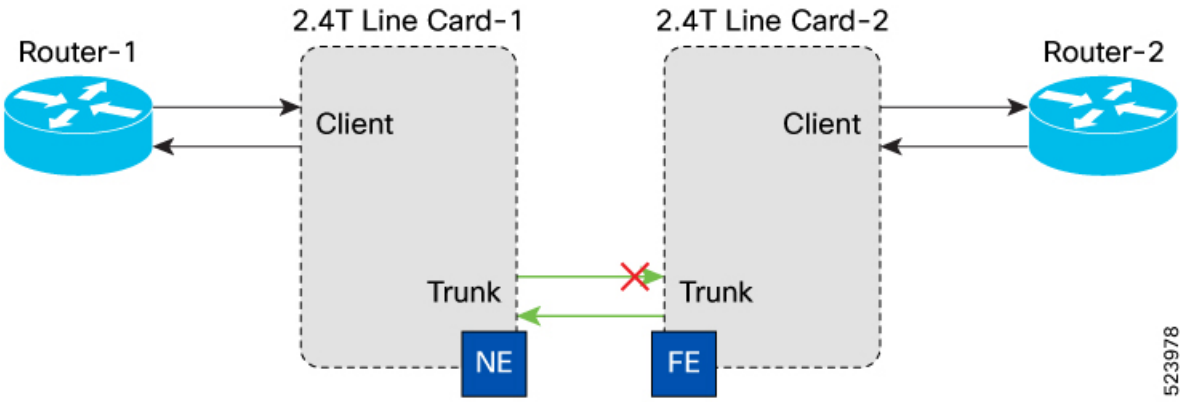
[17] The capability of the router is the determining factor for LD (LOCAL-DEG-SER) reporting. According to IEEE Standard 802.3, implementing Forward Error Correction (FEC) alarms is optional. However, if these alarms are supported, the router inserts an RD (Remote-Deg-Ser) in the upstream direction in response to the LD (Local-FEC -Deg-Ser) alarm.

Trunk Unidirectional OTUK-TIM

When there is a trunk unidirectional OTUK-TIM between 2.4T line card-1 and 2.4T line card-2, alarms are raised and suppressed at the respective ports of each node.

This figure displays trunk unidirectional OTUK-TIM.

Figure 18: Trunk Unidirectional OTUK-TIM



These tables list the alarms that are raised at the respective ports of each node.

Table 36: Active and Suppressed Alarms for Near End (NE) Interface Faults

Node	Active Alarms	Suppressed Alarms
Router -1	No Alarms	No Alarms
NE_Client	No Alarms	No Alarms
NE_Trunk	No Alarms	No Alarms

Table 37: Active and Suppressed Alarms for Far End (FE) Interface Faults

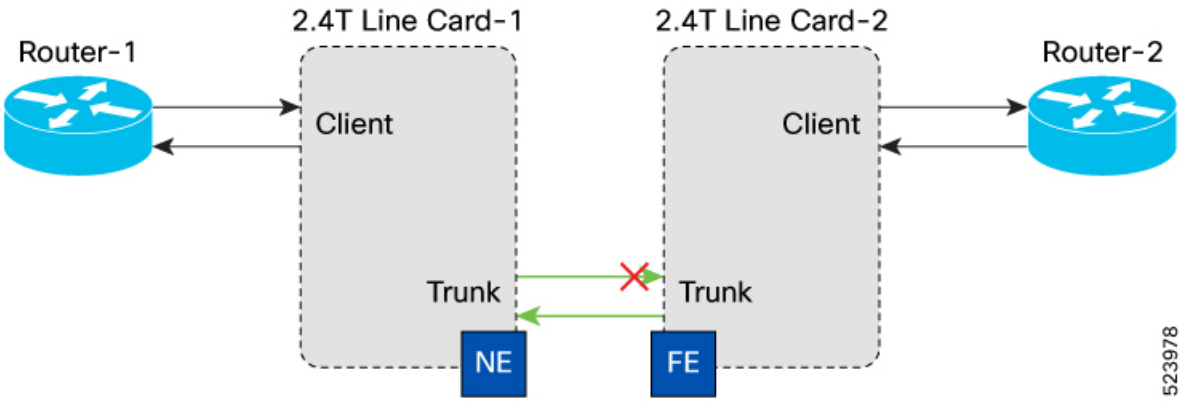
Node	Active Alarms	Suppressed Alarms
Router-2	No Alarms	No Alarms
FE_Client	No Alarms	No Alarms
FE_Trunk	OTUK-TIM Example: OTUK-TIM :DECLARE :CoherentDSP0/1/0/0:	No Alarms

Trunk Unidirectional Improper Removal

When there is a trunk optics Improper Removal (IMPROPRMVL) between 2.4T line card-1 and 2.4T line card-2, alarms are raised and suppressed at the respective ports of each node.

This figure displays trunk optics IMPROPRMVL.

Figure 19: Trunk Unidirectional IMPROPRMVL



These tables list the alarms that are raised at the respective ports of each node.

Table 38: Active and Suppressed Alarms for Near End (NE) Interface Faults

Node	Active Alarms	Suppressed Alarms
Router-1	• LF • LD[18]	No Alarms
NE_Client	RF Example: RF :DECLARE :FourHundredGigECtrlr0/1/0/1	No Alarms
NE_Trunk	LOS-P	No Alarms

[18] The capability of the router is the determining factor for LD (LOCAL-DEG-SER) reporting. According to IEEE Standard 802.3, implementing Forward Error Correction (FEC) alarms is optional. However, if these alarms are supported, the router inserts an RD (Remote-Deg-Ser) in the upstream direction in response to the LD (Local-FEC -Deg-Ser) alarm.

Table 39: Far End (FE) Interface Faults: Active and Suppressed Alarms

Node	Active Alarms	Suppressed Alarms
Router-2	• LF • LD[19]	No Alarms
FE_Client	RF Example: RF :DECLARE :FourHundredGigECtrlr0/1/0/1	No Alarms

FE_Trunk	IMPROPRMVL Example: IMPROPRMVL :DECLARE :Optics0/1/0/1:	No Alarms

[19] The capability of the router is the determining factor for LD (LOCAL-DEG-SER) reporting. According to IEEE Standard 802.3, implementing Forward Error Correction (FEC) alarms is optional. However, if these alarms are supported, the router inserts an RD (Remote-Deg-Ser) in the upstream direction in response to the LD (Local-FEC -Deg-Ser) alarm.