Troubleshooting Guide for Cisco NCS 1002, IOS XR Releases 6.3.x, 7.1.x, 7.2.x, and 7.3.x

First Published: 2017-10-12

Last Modified: 2024-07-24

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.

- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.

- To submit a service request, visit Cisco Support.

- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.

- To obtain general networking, training, and certification titles, visit Cisco Press.

- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

C O N T E N T S

General Troubleshooting

Certain software releases have reached end-of-life status. For more information, see the End-of-Life and End-of-Sale Notices*.*

This chapter provides procedures for troubleshooting the most common problems encountered when operating an NCS 1002. To troubleshoot specific alarms, see Alarm Troubleshooting, on page 45. If you cannot find what you are looking for, contact Cisco Technical Support (1 800 553-2447).

This chapter includes the following sections:

Validating and Troubleshooting Installation of the Software Packages

Step 1   **show version**

Displays the software version and details such as system uptime.

Example:

```
RP/0/RP0/CPU0:ios# show version
Wed Nov 11 06:08:46.785 UTC

Cisco IOS XR Software, Version 6.0.0.22I
Copyright (c) 2013-2015 by Cisco Systems, Inc.

Build Information:
 Built By     : xxxxx
 Built On     : Fri Nov 13 17:08:39 IST 2015
 Build Host   : agl-ads-111
 Workspace    : /nobackup/xxxxx/idprom
 Version      : 6.0.0.22I
 Location     : /opt/cisco/XR/packages/

cisco NCS1K () processor
System uptime is 3 hours, 3 minutes
```

Step 2   **show install repository**

Displays a list of all the installed software packages on the NCS 1002.

Example:

```
RP/0/RP0/CPU0:ios# show install repository
Wed Nov 11 06:05:33.699 UTC
1 package(s) in XR repository:
    ncs1k-xr-6.0.0.22I
```

Step 3   **show install active**

Displays a list of all the installed and active software packages on the NCS 1002.

The following sample output displays active software packages in the EXEC mode.

Example:

```
RP/0/RP0/CPU0:ios# show install active
Wed Nov 11 06:06:40.221 UTC
Node 0/RP0/CPU0 [RP]
  Boot Partition: xr_lv0
  Active Packages: 1
  ncs1k-xr-6.0.0.22I version=6.0.0.22I [Boot image]
```

The following sample output displays active software packages in the system admin EXEC mode.

```
sysadmin-vm:0_RP0# show install active
Wed Nov  11 06:06:47.804 UTC
 Node 0/RP0 [RP]
 Active Packages: 1
 ncs1k-sysadmin-6.0.0.22I version=6.0.0.22I [Boot image]
```

Step 4   **show install committed**

Displays a list of all committed software packages on the NCS 1002.

The committed software packages are the software packages that are booted on an NCS 1002 reload. Committed packages are the packages that are persistent across reloads. If you install and activate a package, it remains active until the next reload. If you commit a package set, all packages in that set remain active across reloads until the package set is replaced with another committed package set.

The following sample output displays the committed software packages in the EXEC mode.

Example:

```
RP/0/RP0/CPU0:ios# show install committed
Wed Nov 11 06:07:53.181 UTC
Node 0/RP0/CPU0 [RP]
  Boot Partition: xr_lv0
  Committed Packages: 1
        ncs1k-xr-6.0.0.22I version=6.0.0.22I [Boot image]
```

The following sample output displays the committed software packages in the system admin EXEC mode.

```
sysadmin-vm:0_RP0# show install committed
Wed Nov  11 06:08:02.409 UTC
 Node 0/RP0 [RP]
    Committed Packages: 1
        ncs1k-sysadmin-6.0.0.22I version=6.0.0.22I [Boot image]
```

Step 5   **show install log**

Displays information on the history of the installation operations. This command provides information about both successful and failed installation operations on the NCS 1002. You can also verify a Service Maintenance Update (SMU) installation using this command.

Example:

```
RP/0/RP0/CPU0:ios# show install log 49 detail
Wed Dec  9 01:19:18.680 UTC
Dec 09 01:19:07 Install operation 49 started by root:
 install add source tftp://10.105.236.167 ncs1k-k9sec.rpm
Dec 09 01:19:08 Action 1: install add action started
Dec 09 01:19:08 ERROR! Either file is not proper or error in getting rpm metadata from rpm file

Dec 09 01:19:08 ERROR!! failed to complete install add precheck

Dec 09 01:19:09 Install operation 49 aborted
Dec 09 01:19:10 Ending operation 49
```

In the above example, either a wrong rpm package is used or the rpm package is corrupted.

For failure on install add source, check that the package is correctly named and is available at the location.

What to do next

If the expected active software packages are not displayed, install the packages (if required) and activate the packages using the **install activate** *package_name* command.

Troubleshooting Problems with Node

Node is Unreachable

Step 1   Verify cable connectivity.

Step 2   Verify that the power supply is on.

Step 3   Reboot the NCS 1002.

Step 4   Verify the hardware module and inventory data. For more information, see Verifying the Status of Hardware Modules, on page 4.

Console and Node are Not Responsive

Console problems occur when the NCS 1002 becomes unresponsive to an input at the console port. If the console is not responsive, it means that a high priority process prevents the console driver from responding to input.

Step 1   Verify cable connectivity.

Step 2   Verify that the power supply is on.

Step 3   Verify the NCS 1002 LED status. If all LEDs are down, it might be an issue with the power supply.

Step 4   Verify that the CPU is inserted properly.

Step 5   Reboot the NCS 1002.

Verifying the Status of Hardware Modules

You can verify the state of the hardware modules in the following scenarios:

- Node is not reachable.

- Node recovers from a problem.

- Node had a power cycle.

- Node reboot.

- Node upgrade.

- Node settles down after the Cisco IOS XR has continuously reloaded.

Step 1   **show platform**

When you execute this command from the Cisco IOS XR EXEC mode, the status of the Cisco IOS XR is displayed.

Verify that the node state is Operational and the admin state is UP.

Example:

```
RP/0/RP0/CPU0:ios# show platform
Wed Nov 11 01:22:28.953 UTC
Node name         Node type           Node state      Admin state   Config state
--------------------------------------------------------------------------------
0/RP0             NCS1K-CNTLR-K9      OPERATIONAL     UP            NSHUT
```

a) If the Cisco IOS XR is not operational, no output is shown in the result. In this case, verify the state of service domain router (SDR) on the node using the **show sdr** command.

The following example shows sample output from the **show sdr** command in Cisco IOS XR EXEC mode.

```
RP/0/RP0/CPU0:ios# show sdr
RP/0/RP0/CPU0:ios#sh sdr
Tue Nov 10 22:57:20.921 UTC
Type                    NodeName        NodeState      RedState      PartnerName
--------------------------------------------------------------------------
RP                      0/RP0/CPU0      IOS XR RUN     ACTIVE        NONE
NCS1K-CNTLR-K9          0/RP0           OPERATIONAL                  N/A
```

The following example shows sample output from the **show sdr** command in system admin EXEC mode.

```
sysadmin-vm:0_RP0# show sdr
Tue Nov  10 22:56:41.225 UTC
sdr default-sdr
 location 0/RP0/VM1
  sdr-id            2
  IP Address of VM   198.51.100.1
  MAC address of VM  E2:3A:DD:0A:8D:03
  VM State          RUNNING
  start-time        2020-11-06T10:41:52.340092+00:00
  Last Reload Reason FIRST_BOOT
  Reboot Count      1
```

Step 2   **admin**

Enters system admin EXEC mode.

Example:

```
 RP/0/RP0/CPU0:ios# admin
```

Step 3   **show platform**

Displays information and status for each node in the system.

Example:

```
sysadmin-vm:0_RP0# show platform
Tue Feb 27 10:26:58.763 UTC
Location Card Type      HW State   SW State     Config State
--------------------------------------------------------------------------
0/0     NCS1002        OPERATIONAL N/A          NSHUT
0/RP0   NCS1002--RP    OPERATIONAL OPERATIONAL NSHUT
0/FT0   NCS1K-FTA      OPERATIONAL N/A          NSHUT
0/FT1   NCS1K-FTA      OPERATIONAL N/A          NSHUT
```

Verify that all the modules of the NCS 1002 are displayed in the result. The software state and the hardware state must be OPERATIONAL.

The various hardware and software states are:

Hardware states:

- OPERATIONAL—Node is operating normally and is fully functional

- POWERED_ON—Power is on and the node is booting up

- FAILED—Node is powered on but has experienced some internal failure

- PRESENT—Node is in the shutdown state

- OFFLINE—User has changed the node state to OFFLINE. The node is accessible for diagnostics

Software states:

- OPERATIONAL—Software is operating normally and is fully functional

- SW_INACTIVE—Software is not completely operational

- FAILED—Software is operational but the card has experienced some internal failure

Step 4 **show platform detail**

Displays the hardware and software states, and other details of the node.

Example:

```
sysadmin-vm:0_RP0# show platform detail
Wed Aug 5 09:49:06.521 UTC
Platform Information for 0/0
PID : NCS1002
Description : "Network Convergence System 1000 Controller"
VID/SN : V01
HW Oper State : OPERATIONAL
SW Oper State : N/A
Configuration : "NSHUT RST"
HW Version : 0.1
Last Event : HW_EVENT_OK
Last Event Reason : "HW Event OK"
Platform Information for 0/RP0
PID : NCS1002--RP
Description : "Network Convergence System 1000 Controller"
VID/SN : V01
HW Oper State : OPERATIONAL
SW Oper State : OPERATIONAL
Configuration : "NSHUT RST"
HW Version : 0.1
Last Event : UNKNOWN
Last Event Reason : UNKNOWN
```

Step 5 **show inventory**

Displays the details of the physical entities of the NCS 1002 along with the details of QSFPs and CFPs when you execute this command in the Cisco IOS XR EXEC mode.

You can verify if any QSFP or CFP has been removed from the NCS 1002.

Example:

```
RP/0/RP0/CPU0:ios# show inventory
RP/0/RP0/CPU0:ios#show inventory
Fri May 18 10:46:51.323 UTC
NAME: "0/0", DESCR: "Network Convergence System 1002 20 QSFP28/QSFP+ slots"
PID: NCS1002-K9         , VID: V03, SN: CAT2116B170


NAME: "0/0-Optics0/0/0/1", DESCR: "Non-Cisco QSFP28 100G LR4 Pluggable Optics Module"
PID: SPQCELRCDFB        , VID: 01 , SN: G9I2011804


NAME: "0/0-Optics0/0/0/4", DESCR: "Non-Cisco QSFP28 100G LR4 Pluggable Optics Module"
PID: TR-FC13L-N00       , VID: 01 , SN: INGAJ0930306


NAME: "0/0-Optics0/0/0/6", DESCR: "Cisco CFP2 DWDM Pluggable Optics"
PID: ONS-CFP2-WDM       , VID: V01 , SN: OUK1936006S


NAME: "0/0-Optics0/0/0/7", DESCR: "Cisco 4x10GE QSFP+ LR-S Pluggable Optics Module"
PID: QSFP-4X10G-LR-S    , VID: V02 , SN: INL20410069


NAME: "0/0-Optics0/0/0/8-LANE1", DESCR: "Cisco 10G SFP LR Pluggable Optics Module"
PID: SFP-10G-LR         , VID: V01 , SN: SPC1907074R


NAME: "0/0-Optics0/0/0/9", DESCR: "Cisco 40GE QSFP+ SR4 Pluggable Optics Module"
PID: QSFP-40G-SR4       , VID: V03 , SN: JFQ20332088


NAME: "0/0-Optics0/0/0/10", DESCR: "Non-Cisco QSFP28 100G LR4 Pluggable Optics Module"
PID: SPQCELRCDFB        , VID: 01 , SN: GAV2008935


NAME: "0/0-Optics0/0/0/11-LANE1", DESCR: "Cisco 10G SFP LR Pluggable Optics Module"
PID: SFP-10G-LR         , VID: V01 , SN: SPC190707YP


NAME: "0/0-Optics0/0/0/17-LANE1", DESCR: "Cisco 10G SFP SR Pluggable Optics Module"
PID: SFP-10G-SR         , VID: V03 , SN: JUR1904073P


NAME: "0/0-Optics0/0/0/18", DESCR: "Non-Cisco QSFP28 100G LR4 Pluggable Optics Module"
PID: FTLC1151RDPL       , VID: A0 , SN: UVE1C6C


NAME: "0/0-Optics0/0/0/19", DESCR: "Cisco CFP2 DWDM Pluggable Optics"
PID: ONS-CFP2-WDM       , VID: V05 , SN: OVE204404PA


NAME: "0/0-Optics0/0/0/21", DESCR: "Cisco 4x10GE QSFP+ LR-S Pluggable Optics Module"
PID: QSFP-4x10G-LR-S    , VID: V01 , SN: INL20200012


NAME: "0/0-Optics0/0/0/22-LANE1", DESCR: "Cisco 10G SFP LR Pluggable Optics Module"
PID: SFP-10G-LR         , VID: V01 , SN: SPC190707YS


NAME: "0/0-Optics0/0/0/23", DESCR: "Cisco 40GE QSFP+ SR4 Pluggable Optics Module"
PID: QSFP-40G-SR4       , VID: V03 , SN: JFQ2033201H


NAME: "0/0-Optics0/0/0/24", DESCR: "Non-Cisco QSFP28 100G LR4 Pluggable Optics Module"
PID: FTLC1151RDPL       , VID: A0 , SN: UWD2QMM


NAME: "0/0-Optics0/0/0/25-LANE1", DESCR: "Cisco 10G SFP ER Pluggable Optics Module"
PID: SFP-10G-ER         , VID: V02 , SN: ONT213100BW


NAME: "0/RP0", DESCR: "Network Convergence System 1000 Controller"
PID: NCS1K-CNTLR        , VID: V04, SN: CAT2052B0FZ


NAME: "Rack 0", DESCR: "Network Convergence System 1002 20 QSFP28/QSFP+ slots"
PID: NCS1002-K9         , VID: V03, SN: CAT2116B170


NAME: "0/FT0", DESCR: "Network Convergence System 1000 Fan"
PID: NCS1K-FTA          , VID: V01, SN: N/A


NAME: "0/FT1", DESCR: "Network Convergence System 1000 Fan"
```

```
PID: NCS1K-FTA         , VID: V01, SN: N/A

NAME: "0/FT2", DESCR: "Network Convergence System 1000 Fan"
PID: NCS1K-FTA         , VID: V01, SN: N/A

NAME: "0/PM0", DESCR: "Network Convergence System 1000 2KW AC PSU"
PID: NCS1K-2KW-AC      , VID: V01, SN: POG2041J0BW

NAME: "0/PM1", DESCR: "Network Convergence System 1000 2KW AC PSU"
PID: NCS1K-2KW-AC      , VID: V01, SN: POG2041J01C
```

What to do next

Verify the software version of the NCS 1002. For more information, see

Verifying the Software Version

The NCS 1002 is shipped with a pre-installed Cisco IOS XR software. Verify that the latest version of the software is installed. If a newer version is available, perform a system upgrade. This will install the newer version of the software and provide the latest feature set on the NCS 1002.

show version

Displays the software version and details such as system uptime in the Cisco IOS XR EXEC mode.

Example:

```
RP/0/RP0/CPU0:ios# show version
Tue Nov 10 23:02:37.683 UTC

Cisco IOS XR Software, Version 6.0.0.26I
Copyright (c) 2013-2015 by Cisco Systems, Inc.

Build Information:
 Built By     : xxxx
 Built On     : Tue Dec  1 17:02:18 PST 2015
 Build Host   : build-lnx-100
 Workspace    : /auto/build-lnx-106-san1/r60x-ws6/nightly_r60x/151201B_ncs1k/workspace
 Version      : 6.0.0.26I
 Location     : /opt/cisco/XR/packages/

cisco NCS1K () processor
System uptime is 4 days, 12 hours, 20 minutes
```

What to do next

Verify the result to ascertain whether a system upgrade is required. If the upgrade is required, see the *System Setup and Software Installation Guide for Cisco NCS 1000 Series*.

Troubleshooting the Management Interface

Before you begin

Management interface should be configured.

Step 1   **show interfaces mgmtEth** *instance*

Displays the management interface configuration.

Example:

```
RP/0/RP0/CPU0:ios# show interfaces MgmtEth 0/RP0/CPU0/0
Fri Nov 13 19:42:29.716 UTC
MgmtEth0/RP0/CPU0/0 is administratively down, line protocol is administratively down
  Interface state transitions: 0
  Hardware is Management Ethernet, address is badb.adba.d098 (bia badb.adba.d098)
  Internet address is 10.58.227.183/24
  MTU 1514 bytes, BW 100000 Kbit (Max: 100000 Kbit)
     reliability 255/255, txload 0/255, rxload 0/255
  Encapsulation ARPA,
  Full-duplex, 100Mb/s, CX, link type is autonegotiation
  loopback not set,
  ARP type ARPA, ARP timeout 04:00:00
  Last input never, output never
  Last clearing of "show interface" counters never
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 total input drops
     0 drops for unrecognized upper-level protocol
     Received 0 broadcast packets, 0 multicast packets
            0 runts, 0 giants, 0 throttles, 0 parity
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 total output drops
     Output 0 broadcast packets, 0 multicast packets
     0 output errors, 0 underruns, 0 applique, 0 resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
```

a) In the above result, the management interface is administratively down. Use the **no shut** command to enable the management interface.

The following example shows sample output from the **show running-config interface mgmtEth** command when the management interface is in the no shut state.

```
RP/0/RP0/CPU0:ios#show running-config interface mgmtEth 0/RP0/CPU0/0
Fri Nov 13 19:42:54.368 UTC
interface MgmtEth0/RP0/CPU0/0
 ipv4 address 10.58.227.183 255.255.255.0
 !
```

You can also use the **show interfaces summary** and **show interfaces brief** commands in the Cisco IOS XR EXEC mode to verify the management interface status.

• The following example shows sample output from the **show interfaces summary** command.

```
RP/0/RP0/CPU0:ios# show interfaces summary
Sun Nov 15 19:31:46.469 UTC
```

```
Interface Type          Total    UP      Down    Admin Down
--------------          -----    --      ----    ----------
ALL TYPES               2        2       0       0
--------------
IFT_ETHERNET            1        1       0       0
IFT_NULL                1        1       0       0
```

• The following example shows sample output from the **show interfaces brief** command.

```
RP/0/RP0/CPU0:ios# show interfaces brief
Sun Nov 15 19:31:41.806 UTC

              Intf      Intf      LineP               Encap  MTU       BW
              Name      State     State               Type   (byte)    (Kbps)
--------------------------------------------------------------------------------
               Nu0        up        up                Null   1500          0
      Mg0/RP0/CPU0/0      up        up                ARPA   1514     100000
```

Step 2 When the line protocol is down, you must verify the Layer 3 connectivity. You can perform the following steps.

a) Check the Ethernet cable connection and physical connectivity of the NCS 1002 to get the line protocol up.

b) Ensure ARP connectivity.

c) Use the **ping** command to check reachability and network connectivity on the IP network.

d) Verify the static IP and default gateway configuration.

Troubleshooting Slice Provisioning

Step 1 **show hw-module slice** *slicenumber*

Displays details of the slice provisioning.

Example:

```
RP/0/RP0/CPU0:ios# show hw-module slice 3
Fri Nov  6 10:12:16.684 UTC
Slice ID:               3
Status:                 Provisioning Failed [ETNA Config Failure]
Client Bitrate:         100
Trunk Bitrate:          100
```

In the above example, the slice provisioning has failed because of an ETNA configuration failure.

Some of the failure reasons that can appear in the command output are:

• CFG INIT Config Failure—Indicates DP FPGA download issue.

• PPM Config Failure—Indicates PPM Driver failure.

• CDR Config Failure—Indicates CDR failure.

• ETNA Config Failure—Indicates ETNA device or programming failure.

• DP FPGA Config Failure—Indicates DP FPGA programming failure.

Step 2   **upgrade hw-module slice** *slice_number* **re-provision**

Reprovisions the slice.

Step 3   Reload the Cisco IOS-XR if reprovisioning the slice does not work.

Troubleshooting Environmental Parameters

Some of the common environmental problems are listed below.

- Fan failure

- Fan not detected

- Fan speed problem

- Power module fails

- Power module not detected

- Temperature of the device exceeds a threshold value

- Voltage of the device exceeds a threshold value

Step 1   **admin**

Enters system admin EXEC mode.

Example:

```
RP/0/RP0/CPU0:ios# admin
```

Step 2   **show environment** [**all** | **fan** | **power** | **voltages** | **current** | **temperatures**] [**location** | *location*]

Displays the environmental parameters of the NCS 1002.

Example:

The following example shows sample output from the **show environment** command with the **fan** keyword.

```
sysadmin-vm:0_RP0# show environment fan
Wed Nov  11 02:04:58.161 UTC
=====================================
                        Fan speed (rpm)
Location      FRU Type          FAN_0
-------------------------------------
0/FT0         NCS1K-FTA          4800
0/FT1         NCS1K-FTA          4800
0/FT2         NCS1K-FTA          4680
0/PM1         NCS1K-2KW-AC       8064
```

The table below lists the temperature threshold values for the different fan speeds.

Fan speed (rpm)	Rising Min Temperature (°C)	Rising Max Temperature (°C)	Falling Max Temperature (°C)	Falling Min Temperature (°C)
4800	-127	28	27	-127
5500	29	30	29	28
8500	31	36	35	30
10500	37	41	40	36
12500	42	44	43	41
14500	45	127	127	44

The following example shows sample output from the **show environment** command with the **temperatures** keyword.

```
sysadmin-vm:0_RP0# show environment temperatures location 0/RP0
Tue Feb  27 10:32:38.967 UTC
===============================================================================
Location   TEMPERATURE                   Value   Crit Major Minor Minor Major  Crit
                       Sensor            (deg C)  (Lo) (Lo)  (Lo)  (Hi)  (Hi)  (Hi)
-------------------------------------------------------------------------------
0/RP0
             Thermistor 1                27    -10    0     0    55    55    85
             Thermistor 2                28    -10    0     0    55    55    85
          Hot Spot Temperature           26    -10    0     0    55    55    85
```

The following example shows sample output from the **show environment** command with the **power** keyword.

```
sysadmin-vm:0_RP0# show environment power
Tue Feb  13 15:29:54.827 UTC
===============================================================================
CHASSIS LEVEL POWER INFO: 0
===============================================================================
   Total output power capacity (Group 0 + Group 1) :      0W +    2000W
   Total output power required             :     225W
   Total power input                       :     895W
   Total power output                      :     833W

Power Group 1:
===============================================================================
   Power      Supply    ------Input----   ------Output---     Status
   Module     Type       Volts   Amps      Volts   Amps
===============================================================================
   0/PM1      2kW-AC     229.5   3.9       12.0    69.4    OK

Total of Power Group 1:      895W/  3.9A      833W/ 69.4A


===============================================================================
   Location    Card Type          Power      Power     Status
                                  Allocated  Used
                                  Watts      Watts
===============================================================================
   0/0         S-L-NCS1K-P0        70         -        RESERVED
   0/RP0       NCS1002--RP         35         -        ON
   0/FT0       NCS1K-FTA           40         -        ON
   0/FT1       NCS1K-FTA           40         -        ON
   0/FT2       NCS1K-FTA           40         -        ON
```

The following example shows sample output from the **show environment** command with the **voltages** keyword.

```
sysadmin-vm:0_RP0# show environment voltages location 0/RP0
Thu Aug  6  09:35:09.211 UTC
================================================================================
Location  VOLTAGE                        Value   Crit Minor Minor  Crit
          Sensor                         (mV)    (Lo) (Lo)  (Hi)   (Hi)
--------------------------------------------------------------------------------
0/RP0
          ! VP1P0_CPU                    1200     900   950  1050  1100
          ! CPU_CORE_VCC                 1200     900   950  1050  1100
          ! CPU_CORE_VNN                 1200     900   950  1050  1100
          ! VP1P1                        1200     990  1050  1160  1210
            VP1P2                        1200    1080  1140  1260  1320
          ! VP1P35_DDR                   1200    1220  1280  1420  1490
          ! VP1P35                       1200    1220  1280  1420  1490
          ! VP1P5                        1200    1350  1430  1580  1650
          ! VP1P8_CPU                    1200    1620  1710  1890  1980
          ! VP3P3_STBY                   1200    2970  3140  3470  3630
          ! VP3P3                        1200    2970  3140  3470  3630
          ! VP5P0                        1200    4500  4750  5250  5500
          ! VP12P0                       1200   10800 11400 12600 13200
          ! VREF                         1200    2430  2570  2840  2970
          ! 12V Input Voltage            1200    8000 10000 14000 16000
```

Step 3   **show inventory**

Displays inventory information for all the physical entities of the NCS 1002.

```
RP/0/RP0/CPU0:ios# show inventory
RP/0/RP0/CPU0:ios#show inventory
Fri May 18 10:46:51.323 UTC
NAME: "0/0", DESCR: "Network Convergence System 1002 20 QSFP28/QSFP+ slots"
PID: NCS1002-K9        , VID: V03, SN: CAT2116B170

NAME: "0/0-Optics0/0/0/1", DESCR: "Non-Cisco QSFP28 100G LR4 Pluggable Optics Module"
PID: SPQCELRCDFB        , VID: 01 , SN: G9I2011804

NAME: "0/0-Optics0/0/0/4", DESCR: "Non-Cisco QSFP28 100G LR4 Pluggable Optics Module"
PID: TR-FC13L-N00       , VID: 01 , SN: INGAJ0930306

NAME: "0/0-Optics0/0/0/6", DESCR: "Cisco CFP2 DWDM Pluggable Optics"
PID: ONS-CFP2-WDM       , VID: V01 , SN: OUK1936006S

NAME: "0/0-Optics0/0/0/7", DESCR: "Cisco 4x10GE QSFP+ LR-S Pluggable Optics Module"
PID: QSFP-4X10G-LR-S    , VID: V02 , SN: INL20410069

NAME: "0/0-Optics0/0/0/8-LANE1", DESCR: "Cisco 10G SFP LR Pluggable Optics Module"
PID: SFP-10G-LR         , VID: V01 , SN: SPC1907074R

NAME: "0/0-Optics0/0/0/9", DESCR: "Cisco 40GE QSFP+ SR4 Pluggable Optics Module"
PID: QSFP-40G-SR4       , VID: V03 , SN: JFQ20332088

NAME: "0/0-Optics0/0/0/10", DESCR: "Non-Cisco QSFP28 100G LR4 Pluggable Optics Module"
PID: SPQCELRCDFB        , VID: 01 , SN: GAV2008935

NAME: "0/0-Optics0/0/0/11-LANE1", DESCR: "Cisco 10G SFP LR Pluggable Optics Module"
PID: SFP-10G-LR         , VID: V01 , SN: SPC190707YP

NAME: "0/0-Optics0/0/0/17-LANE1", DESCR: "Cisco 10G SFP SR Pluggable Optics Module"
PID: SFP-10G-SR         , VID: V03 , SN: JUR1904073P

NAME: "0/0-Optics0/0/0/18", DESCR: "Non-Cisco QSFP28 100G LR4 Pluggable Optics Module"
PID: FTLC1151RDPL       , VID: A0 , SN: UVE1C6C

NAME: "0/0-Optics0/0/0/19", DESCR: "Cisco CFP2 DWDM Pluggable Optics"
PID: ONS-CFP2-WDM       , VID: V05 , SN: OVE204404PA
```

```
NAME: "0/0-Optics0/0/0/21", DESCR: "Cisco 4x10GE QSFP+ LR-S Pluggable Optics Module"
PID: QSFP-4x10G-LR-S    , VID: V01 , SN: INL20200012

NAME: "0/0-Optics0/0/0/22-LANE1", DESCR: "Cisco 10G SFP LR Pluggable Optics Module"
PID: SFP-10G-LR         , VID: V01 , SN: SPC190707YS

NAME: "0/0-Optics0/0/0/23", DESCR: "Cisco 40GE QSFP+ SR4 Pluggable Optics Module"
PID: QSFP-40G-SR4        , VID: V03 , SN: JFQ2033201H

NAME: "0/0-Optics0/0/0/24", DESCR: "Non-Cisco QSFP28 100G LR4 Pluggable Optics Module"
PID: FTLC1151RDPL        , VID: A0 , SN: UWD2QMM

NAME: "0/0-Optics0/0/0/25-LANE1", DESCR: "Cisco 10G SFP ER Pluggable Optics Module"
PID: SFP-10G-ER          , VID: V02 , SN: ONT213100BW

NAME: "0/RP0", DESCR: "Network Convergence System 1000 Controller"
PID: NCS1K-CNTLR         , VID: V04, SN: CAT2052B0FZ

NAME: "Rack 0", DESCR: "Network Convergence System 1002 20 QSFP28/QSFP+ slots"
PID: NCS1002-K9          , VID: V03, SN: CAT2116B170

NAME: "0/FT0", DESCR: "Network Convergence System 1000 Fan"
PID: NCS1K-FTA           , VID: V01, SN: N/A

NAME: "0/FT1", DESCR: "Network Convergence System 1000 Fan"
PID: NCS1K-FTA           , VID: V01, SN: N/A

NAME: "0/FT2", DESCR: "Network Convergence System 1000 Fan"
PID: NCS1K-FTA           , VID: V01, SN: N/A

NAME: "0/PM0", DESCR: "Network Convergence System 1000 2KW AC PSU"
PID: NCS1K-2KW-AC        , VID: V01, SN: POG2041J0BW

NAME: "0/PM1", DESCR: "Network Convergence System 1000 2KW AC PSU"
PID: NCS1K-2KW-AC        , VID: V01, SN: POG2041J01C
```

What to do next

Environment parameter anomalies are logged in the syslog. Hence, if an environment parameter displayed in the **show environment** command output is not as expected, check the syslog using the **show logging** command. The syslog provides details on any logged problems.

Troubleshooting Firmware Upgrade Failure

Step 1   **show hw-module fpd**

Verify the firmware version. Displays the firmware information of various hardware components of the NCS 1002.

The following example is for Release 6.0.1:

Example:

```
  RP/0/RP0/CPU0:ios# show hw-module fpd
Tue Apr 12 09:04:14.935 UTC
FPD Versions
=================
```

```
Location Card type HWver FPD device ATR Status Running Programd
--------------------------------------------------------------------------------
0/0      NCS1002 2.4 CDSP_PORT_05         CURRENT 3.56 3.56
0/0      NCS1002 2.4 CDSP_PORT_06         CURRENT 3.56 3.56
0/0      NCS1002 2.4 CDSP_PORT_12         CURRENT 3.56 3.56
0/0      NCS1002 2.4 CDSP_PORT_13         CURRENT 3.56 3.56
0/0      NCS1002     CDSP_PORT_19         UPGD FAIL
0/0      NCS1002 2.4 CDSP_PORT_20         CURRENT 3.56 3.56
0/0      NCS1002 2.4 CDSP_PORT_26         CURRENT 3.56 3.56
0/0      NCS1002 2.4 CDSP_PORT_27         CURRENT 3.56 3.56
0/0      NCS1002     CFP2_PORT_05         NOT READY
0/0      NCS1002 2.0 CFP2_PORT_06         CURRENT 4.38 4.38
0/0      NCS1002     CFP2_PORT_12         NOT READY
0/0      NCS1002     CFP2_PORT_13         NOT READY
0/0      NCS1002     CFP2_PORT_19         NOT READY
0/0      NCS1002 2.1 CFP2_PORT_20         CURRENT 5.19 5.19
0/0      NCS1002     CFP2_PORT_26         NOT READY
0/0      NCS1002     CFP2_PORT_27         NOT READY
0/0      NCS1002 0.1 CTRL_BKP_LOW  B      CURRENT 1.22
0/0      NCS1002 0.1 CTRL_BKP_UP   B      CURRENT 1.22
0/0      NCS1002 0.1 CTRL_FPGA_LOW        CURRENT 1.22 1.22
0/0      NCS1002 0.1 CTRL_FPGA_UP         CURRENT 1.22 1.22
0/RP0 NCS1K-CNTLR-K9 0.1 BIOS_Backup BS CURRENT 13.10
0/RP0 NCS1K-CNTLR-K9 0.1 BIOS_Primary S CURRENT 13.10 13.10
0/RP0 NCS1K-CNTLR-K9 0.1 Daisy_Duke_BKP BS CURRENT 0.15
0/RP0 NCS1K-CNTLR-K9 0.1 Daisy_Duke_FPGA S CURRENT 0.15 0.15
```

In the above output, the Status of the CDSP_PORT_19 is UPGD FAIL. For more information on the different states of the firmware, see .

Step 2   **show hw-module slice** *slice_number*

Displays the slice and Datapath FPGA (DP FPGA) information of the NCS 1002.

The following example is for Release 6.0.1:

Example:

```
  RP/0/RP0/CPU0:ios# show hw-module slice 2
Tue Apr 12 09:09:24.527 UTC
Slice ID: 2
Status: Provisioned
Client Bitrate: 40
Trunk Bitrate: 200
DP FPGA Version: F-203
HW Status: CURRENT

Client Port - Trunk Port CoherentDSP0/0/0/20
Traffic Split Percentage

FortyGigECtrlr0/0/0/14 100
FortyGigECtrlr0/0/0/15 100
FortyGigECtrlr0/0/0/16 100
FortyGigECtrlr0/0/0/17 100
FortyGigECtrlr0/0/0/18 100
```

In the above output, DP FPGA Version indicates the image of the datapath FPGA. Here, F-203 is the image version of the 40 G image. The CURRENT value of the HW Status parameter indicates that the firmware version is the latest.

T indicates 10 G and H indicates 100 G image versions. If Need UPG appears in the output, you must upgrade the slice to get the updated DP FPGA using the **upgrade hw-module slice** *slice_number* **re-provision** command.

What to do next

Upgrade the required firmware by using the **upgrade hw-module location 0/0 fpd** *fpd_device_name* command or update all the FPDs using the **upgrade hw-module location all fpd** *fpd_device_name* command in the Cisco IOS XR EXEC mode. After an upgrade is completed, the Status column shows RLOAD REQ if the ISO image requires reload.

If Reload is Required

If the FPGA location is 0/RP0, use the **admin hw-module location 0/RP0 reload** command. This command reboots only the CPU. Hence, the traffic is not impacted. If the FPGA location is 0/0, use the **admin hw-module location all reload** command. This command reboots the chassis. Hence, the traffic is impacted. After the reload is completed, the new FPGA runs the current version.

Verifying the Firmware Version

The firmware on various hardware components of the NCS 1002 must be compatible with the installed Cisco IOS XR image. Incompatibility might cause the NCS 1002 to malfunction.

Step 1   **show hw-module fpd**

Verify the firmware version. Displays the firmware information of various hardware components of the NCS 1002.

In Release 6.0.1, the following example displays the firmware information of various hardware components of the NCS 1002.

Example:

```
  RP/0/RP0/CPU0:ios# show hw-module fpd
Tue Apr 12 09:04:14.935 UTC
FPD Versions
=================
Location Card type HWver FPD device ATR Status Running Programd
-----------------------------------------------------------------------------
0/0     NCS1002 2.4 CDSP_PORT_05       CURRENT 3.56 3.56
0/0     NCS1002 2.4 CDSP_PORT_06       CURRENT 3.56 3.56
0/0     NCS1002 2.4 CDSP_PORT_12       CURRENT 3.56 3.56
0/0     NCS1002 2.4 CDSP_PORT_13       CURRENT 3.56 3.56
0/0     NCS1002 2.4 CDSP_PORT_19       CURRENT 3.56 3.56
0/0     NCS1002 2.4 CDSP_PORT_20       CURRENT 3.56 3.56
0/0     NCS1002 2.4 CDSP_PORT_26       CURRENT 3.56 3.56
0/0     NCS1002 2.4 CDSP_PORT_27       CURRENT 3.56 3.56
0/0     NCS1002     CFP2_PORT_05       NOT READY
0/0     NCS1002 2.0 CFP2_PORT_06       CURRENT 4.38 4.38
0/0     NCS1002     CFP2_PORT_12       NOT READY
0/0     NCS1002     CFP2_PORT_13       NOT READY
0/0     NCS1002     CFP2_PORT_19       NOT READY
0/0     NCS1002 2.1 CFP2_PORT_20       CURRENT 5.19 5.19
0/0     NCS1002     CFP2_PORT_26       NOT READY
0/0     NCS1002     CFP2_PORT_27       NOT READY
0/0     NCS1002 0.1 CTRL_BKP_LOW  B    CURRENT 1.22
0/0     NCS1002 0.1 CTRL_BKP_UP   B    CURRENT 1.22
0/0     NCS1002 0.1 CTRL_FPGA_LOW      CURRENT 1.22 1.22
```

```
0/0     NCS1002 0.1 CTRL_FPGA_UP        CURRENT 1.22 1.22
0/RP0 NCS1K-CNTLR-K9 0.1 BIOS_Backup BS CURRENT 13.10
0/RP0 NCS1K-CNTLR-K9 0.1 BIOS_Primary S CURRENT 13.10 13.10
0/RP0 NCS1K-CNTLR-K9 0.1 Daisy_Duke_BKP BS CURRENT 0.15
0/RP0 NCS1K-CNTLR-K9 0.1 Daisy_Duke_FPGA S CURRENT 0.15 0.15
```

In the above output, some of the significant fields are:

- FPD Device—Name of the hardware component such as FPD, CFP, and so on.

- ATR—Attribute of the hardware component. Some of the attributes are:

    - B—Backup Image

    - S—Secure Image

    - P—Protected Image

- Status—Upgrade status of the firmware. The different states are:

    - CURRENT—The firmware version is the latest version.

    - READY—The firmware of the FPD is ready for an upgrade.

    - NOT READY—The firmware of the FPD is not ready for an upgrade.

    - NEED UPGD—A newer firmware version is available in the installed image. It is recommended that an upgrade be performed.

    - RLOAD REQ—The upgrade has been completed, and the ISO image requires a reload.

    - UPGD DONE—The firmware upgrade is successful.

    - UPGD FAIL—The firmware upgrade has failed.

    - BACK IMG—The firmware is corrupted. Reinstall the firmware.

    - UPGD SKIP—The upgrade has been skipped because the installed firmware version is higher than the one available in the image.

- Running—Current version of the firmware running on the FPD.

Note   CFP2 upgrade is not supported in 6.0.

Step 2   **show hw-module slice** *slice_number*

Displays the slice and Datapath FPGA (DP-FPGA) information of the NCS 1002.

In Release 6.0.1, the following example displays the slice and DP-FPGA of the NCS 1002.

Example:

```
  RP/0/RP0/CPU0:ios# show hw-module slice 2
Tue Apr 12 09:09:24.527 UTC
Slice ID: 2
Status: Provisioned
Client Bitrate: 40
Trunk Bitrate: 200
DP FPGA Version: F-203
HW Status: CURRENT
```

```
Client Port - Trunk Port CoherentDSP0/0/0/20
Traffic Split Percentage

FortyGigECtrlr0/0/0/14 100
FortyGigECtrlr0/0/0/15 100
FortyGigECtrlr0/0/0/16 100
FortyGigECtrlr0/0/0/17 100
FortyGigECtrlr0/0/0/18 100
```

In the above output, DP FPGA Version indicates the image of the datapath FPGA. Here, F-203 is the image version of the 40 G image. The CURRENT value of the HW Status parameter indicates that the firmware version is the latest.

T indicates 10 G and H indicates 100 G image versions. If Need UPG appears in the output, you must upgrade the slice to get the updated DP FPGA using the **upgrade hw-module slice** *slice_number* **re-provision** command.

The different Status are:

- Provisioned—Indicates slice is provisioned

- Provisioning in progress—Indicates slice provisioning is in progress

- Not provisioned—Indicates slice is not provisioned

- Provisioning Failed—Indicates slice provisioning has failed. For more information, see Troubleshooting Slice Provisioning, on page 10.

Troubleshooting Optical Connectivity

The following topics are discussed:

Using Loopbacks

Use loopbacks to test newly created circuits before running live traffic or to logically locate the source of a network failure.

Note   Internal and line loopback modes are supported only on 10 G client Ethernet and trunk Coherent DSP ports.

Line loopback

A line loopback tests the line interface unit (LIU) of the device, the electrical interface assembly (EIA), and related cabling. After applying a line loopback on a port, use a test set to run traffic over the loopback. A successful line loopback isolates the LIU, the EIA, or the cabling plant as the potential cause of a network problem. You can verify issues related to the fiber and pluggables using this loopback.

Internal loopback

An internal loopback tests the data path as it passes through various components of the device and loops back. After applying an internal loopback on a port, use a test set to run traffic over the loopback. You can verify issues related to the programming of the device using this loopback.

You can use loopback to troubleshoot some of the following problems in the client or trunk ports.

- No incoming traffic

- Link is down

- Incoming cyclic redundancy check (CRC) errors

- No outgoing traffic

- LOS at the trunk port

For 10 G mode, individual ports can be put in loopback (internal or line) on a per lane basis by applying the corresponding configuration on the 10G controller.

Before you begin

To create a loopback on a port, the port must be in the maintenance administrative state.

Step 1   **configure**

Enters the configuration mode.

Example:

RP/0/RP0/CPU0:ios# **configure**

Step 2   **controller** *controllertype R/S/I/P*

Enters the Ethernet controller configuration mode.

Example:

RP/0/RP0/CPU0:ios(config)# **controller TenGigECtrlr 0/0/0/11/1**

Step 3   **sec-admin-state maintenance**

Configures the Ethernet controller in the maintenance administrative state.

Example:

RP/0/RP0/CPU0:ios(config-eth-ctrlr)# **sec-admin-state maintenance**

Step 4   **commit**

Saves the configuration changes and remains within the configuration session.

Example:

RP/0/RP0/CPU0:ios(config-eth-ctrlr)# **commit**

Step 5   You can configure either terminal (internal) loopback or facility (line) loopback.

a)   **loopback internal**

Configures internal loopback.

Example:

RP/0/RP0/CPU0:ios(config-eth-ctrlr)# **loopback internal**

b)   **loopback line**

Configures line loopback.

Example:

```
RP/0/RP0/CPU0:ios(config-eth-ctrlr)# loopback line
```

Step 6   **commit**

Saves the configuration changes and remains within the configuration session.

Example:

```
RP/0/RP0/CPU0:ios(config-eth-ctrlr)# commit
```

Step 7   You can verify the internal or line loopback configuration using the following show commands.

a) **show controllers** *controllertype R/S/I/P*

Displays status and configuration information about the controller.

Note   In the maintenance mode, all alarms are suppressed and the **show alarms** command will not show the alarms details. Use the **show controllers** *controllertype R/S/I/P* to view the client and trunk alarms.

Example:

The following example shows the line loopback configured on the Ethernet controller.

```
RP/0/RP0/CPU0:ios# show controllers TenGigECtrlr 0/0/0/1/1
Tue Dec  1 19:19:47.620 UTC
Operational data for interface TenGigECtrlr0/0/0/1/1:

State:
    Administrative state: enabled
    Operational state: Down (Reason: State undefined)
    LED state: Red On
    Maintenance: Enabled
    AINS Soak: None
    Laser Squelch: Disabled
Phy:
    Media type: Not known
    Alarms:
        Current:
            Loss of Frequency Sync Data
Autonegotiation disabled.
Operational values:
    Speed: 10Gbps
    Duplex: Full Duplex
    Flowcontrol: None
    Loopback: Line
    Inter-packet gap: standard (12)
```

b) **show running-config**

Displays the NCS 1002 configuration.

Example:

```
RP/0/RP0/CPU0:ios# show running-config
...
<snip>
controller TenGigECtrlr0/0/0/1/1
 loopback line
 sec-admin-state maintenance
```

```
       ...
       <snip>
```

Using Link Layer Discovery Protocol Snooping

LLDP snooping is enabled on the Ethernet controllers when you provision the controllers. You can use LLDP snooping to troubleshoot problems in the client ports. For example, to verify the far end device connected to the client interface. You can troubleshoot connectivity issues using LLDP snooping using the following procedure.

show controllers *controller* **lldp-snoop**

Displays the MAC address. Verify that the MAC address displayed is same as the MAC address of the traffic generating port. In Release 6.0.1, you can view more details about the LLDP neighbor.

Example:

```
RP/0/RP0/CPU0:ios# show controllers fortyGigECtrlr 0/0/0/7 lldp-snoop
Thu Aug  30 02:47:18.208 UTC

        LLDP Neighbor Snoop Data
-----------------------------------------------
Capability codes:
        (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
        (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Local Controller:     fortyGigECtrlr0/0/0/7

Source MAC Address:   0010.9400.0001

Chassis ID:           198.51.100.2

Port ID:              0010.9400.0001

Port Description:     Spirent Port

System Name:          not advertised

System Description:   Spirent Test Center

Hold Time(TTL):       99 seconds

System Capabilities:  N/A

Enabled Capabilities: N/A

Management Address:   not advertised

LLDP Packet Drop      FALSE
enabled:

RX LLDP Packet        88
Count:

RP/0/RP0/CP0:         ios#
```

Using Trail Trace Identifier

A Trail Trace Identifier (TTI) is used for verifying the optical connection on the trunk side.

Use the following procedure to configure and verify the TTI.

Step 1 **controller coherentDSP** *R/S/I/P* **tti** {**sent** | **expected**} **ascii** *string*

Configures the transmit and expected TTI strings. The ASCII text string can be a maximum of 64 characters. The TTI string has to be configured on both the trunk ports that are inter-connected to each other. If a pattern mismatch occurs, a TIM alarm is raised.

Note Source Access Point Identifier (SAPI), Destination Access Point Identifier (DAPI), and operator inputs are not supported.

Example:

```
RP/0/RP0/CPU0:ios(config)# controller coherentDSP 0/0/0/12 tti sent ascii abc
RP/0/RP0/CPU0:ios(config)# controller coherentDSP 0/0/0/12 tti expected ascii abc
```

Step 2 **show controller coherentDSP** *R/S/I/P*

Displays details of the coherent DSP controller. Verify the transmit and expected TTI strings.

Example:

```
RP/0/RP0/CPU0:ios# show controll coherentDSP 0/0/0/6
Tue Nov 17 22:57:20.724 UTC

Port                                      : CoherentDSP 0/0/0/6
Controller State                          : Down
Secondary State                           : Normal
Derived State                             : In Service
Loopback mode                             : None
BER Thresholds                            : SF = 1.0E-5  SD = 1.0E-7
Performance Monitoring                    : Enable

Alarm Information:
LOS = 2 LOF = 1 LOM = 2
OOF = 0 OOM = 0 AIS = 0
IAE = 0 BIAE = 0        SF_BER = 0
SD_BER = 0      BDI = 0 TIM = 0
FECMISMATCH = 0 FEC-UNC = 0
Detected Alarms                           : LOS

OTU TTI Sent
    OPERATOR SPECIFIC  ASCII              : abc
                                          :
    OPERATOR SPECIFIC HEX                 : 6162630000000000000000000000000
                                          : 0000000000000000000000000000000
OTU TTI Received
    OPERATOR SPECIFIC  ASCII              : abc
                                          :
```

```
        OPERATOR SPECIFIC HEX                      : 616263000000000000000000000000
                                                   : 000000000000000000000000000000
OTU TTI Expected
        OPERATOR SPECIFIC  ASCII                   : abc
                                                   :
        OPERATOR SPECIFIC HEX                      : 616263000000000000000000000000
                                                   : 000000000000000000000000000000
FEC mode                                           : Soft-Decision 7
Network SRLG values                                : Not Configured
```

Step 3 **show alarms brief card location** *R/S/I/P* **active**

Displays details of the alarms in brief. Verify the transmit and expected TTI strings.

Example:

```
RP/0/RP0/CPU0:ios# show alarms brief card location 0/RP0/CPU0 active
Sat Feb 17 11:45:24.590 UTC

-------------------------------------------------------------------------------
Active Alarms
-------------------------------------------------------------------------------
Location Severity Group   Set Time          Description


-------------------------------------------------------------------------------


  0/0      Minor   OTN    02/17/2015 11:44:22  CoherentDSP0/0/0/13 - Section Monitoring Trail Trace
 Indentifier Mismatch
```

What to do next

1. If the transmit or expected string was changed, restore the original string.

2. Use a loopback. For more information, see Using Loopbacks, on page 18.

Troubleshooting the Trunk Port

Step 1 **show controller coherentDSP** *R/S/I/P*

Displays details of the coherent DSP controller.

Example:

```
RP/0/RP0/CPU0:ios# show controller coherentDSP 0/0/0/6
Tue Nov 17 22:57:20.724 UTC

Port                                  : CoherentDSP 0/0/0/6
Controller State                      : Down
Secondary State                       : Normal
Derived State                         : In Service
Loopback mode                         : None
BER Thresholds                        : SF = 1.0E-5  SD = 1.0E-7
```

```
Performance Monitoring                             : Enable

Alarm Information:
LOS = 2 LOF = 1 LOM = 2
OOF = 0 OOM = 0 AIS = 0
IAE = 0 BIAE = 0        SF_BER = 0
SD_BER = 0      BDI = 0 TIM = 0
FECMISMATCH = 0 FEC-UNC = 0
```
Detected Alarms   : LOS
```
OTU TTI Sent
     OPERATOR SPECIFIC  ASCII                 :
                                              :
     OPERATOR SPECIFIC HEX                    : 00000000000000000000000000000000
                                              : 00000000000000000000000000000000
OTU TTI Expected
     OPERATOR SPECIFIC  ASCII                 :
                                              :
     OPERATOR SPECIFIC HEX                    : 00000000000000000000000000000000
                                              : 00000000000000000000000000000000
FEC mode                                      : Soft-Decision 7
Network SRLG values                           : Not Configured
```

In the above output, you can verify the state of the controller and also verify the alarms related to the trunk port.

Step 2   **show controller optics** *R/S/I/P*

Displays details of the optics controller.

Example:

```
RP/0/RP0/CPU0:ios# show controller optics  0/0/0/6
Tue Nov 17 22:54:38.244 UTC
 Controller State: Down
 Transport Admin State: In Service
 Laser State: On
 LED State: Red
 Optics Status
        Optics Type:  DWDM optics
        DWDM Carrier Info: C-Band, MSA ITU Channel=69, Frequency=192.70THz,
        Wavelength=1555.747nm
        Alarm Status:
        -------------
        Detected Alarms: None
        LOS/LOL/Fault Status:
        --------------------
        Detected LOS/LOL/FAULT: None

        Alarm Statistics:
        HIGH-RX-PWR = 1            LOW-RX-PWR = 0
        HIGH-TX-PWR = 0            LOW-TX-PWR = 2
        HIGH-LBC = 5              HIGH-DGD = 0
        OOR-CD = 0                OSNR = 0
        WVL-OOL = 0
        Laser Bias Current = 3.0 %
        Actual TX Power = -0.76 dBm
        RX Power = -40.00 dBm

<truncated>
        Chromatic Dispersion 65 ps/nm
        Configured CD-MIN -70000 ps/nm  CD-MAX 70000 ps/nm
        Second Order Polarization Mode Dispersion = 259.00 ps^2
        Optical Signal to Noise Ratio = 29.50 dB
        Polarization Dependent Loss = 0.00 dB
```

```
            Polarization Change Rate = 3.00 rad/s
            Differential Group Delay = 7.30 ps
```

In the above output, you can verify the state of the controller, LED state, wavelength, TX power, RX power, OSNR, and the alarms.

Step 3   If there is an LOS alarm on the trunk port:

a) Verify the fiber continuity to the port of the NCS 1002 and fix the fiber connection.

b) Verify the wavelength and the channel mapping of the optics controllers. For more information, see Verifying Wavelength and Channel Mapping for Optics Controllers, on page 28.

What to do next

1. Verify the performance monitoring parameters of the Optics, and coherent DSP controllers. For more information, see Verifying the Performance Monitoring Parameters of Controllers, on page 29.

2. Use loopbacks. For more information, see Using Loopbacks, on page 18.

3. Use TTI. For more information, see Using Trail Trace Identifier, on page 22.

Troubleshooting Breakout Ports

The client port can be enabled in normal mode or breakout mode. When the client bit rate is 10G, the mode is breakout mode. You must map a lane to a 10G port.

Before you begin

All the five client ports of the slice need to be configured with the same bit rate.

Step 1   **show controllers optics** *R/S/I/P* **pm current 15-min optics** *lanenumber*

Displays the PM data for the optics controller.

In the following example, Lane 1 is monitored within the Optics 0/1/0/0 corresponding to the 10G Ethernet controller 0/1/0/0/1.

Example:

```
RP/0/RP0:ios# show controllers optics 0/1/0/0 pm current 15-min optics 1
Tue Feb 10 14:59:06.945 UTC
Optics in the current interval {14:45:00 - 14:59:05 Tue Feb 15 2015]

Optics current bucket type : Valid
          MIN      AVG      MAX      Threshold(Min) TCA(enable)  Threshold(Max) TCA(enable)

LBC[mA] : 735     735     735     0               NO              0              NO
OPT[dBm]:-1.23   -1.23   -1.23   2.5             NO              3.5            NO
OPR[dBm]:-1.07   -1.07   -1.07   -23.98          NO              -7.5           NO
```

In the following example, Lane 2 is monitored within the Optics 0/1/0/0 corresponding to the 10G Ethernet controller 0/1/0/0/2.

```
RP/0/RP0:ios# show controllers optics 0/1/0/0 pm current 15-min optics 2
Tue Feb 10 14:59:10.936 UTC
Optics in the current interval {14:45:00 - 14:59:11 Tue Feb 15 2015]

Optics current bucket type : Valid
          MIN      AVG     MAX    Threshold(Min) TCA(enable) Threshold(Max) TCA(enable)

LBC[mA] : 770      770     770    0                NO            0            NO
OPT[dBm]:-1.25    -1.25   -1.25   2.5              NO            3.5          NO
OPR[dBm]:-1.41    -1.41   -1.41   -23.98           NO            -7.5         NO
```

Step 2 **show controllers optics** *R/S/I/P*

Displays details about the optics controller.

In the following example, you can view the parameters for each lane of the Optics 0/2/0/0 controller.

Example:

```
RP/0/RP0/CPU0:ios# show controllers optics 0/2/0/0
Tue Feb 13 15:35:34.051 UTC
optics: Driver is not sending wave channel number and grey wavelength.
Controller State: Administratively Down
Transport Admin State: Out Of Service
Laser State: Off
LED State: Off
Optics Status
Optics Type: Grey optics
Alarm Status:
Detected Alarms: None
LOS/LOL/Fault Status:
Detected LOS/LOL/FAULT: None
Alarm Statistics:
HIGH-RX-PWR = 0 LOW-RX-PWR = 0
HIGH-TX-PWR = 0 LOW-TX-PWR = 0
HIGH-LBC = 0
Performance Monitoring: Enable
Rx Low Threshold = -12.0 dBm
Rx High Threshold = 4.9 dBm
Tx Low Threshold = -10.1 dBm
Tx High Threshold = 3.5 dBm
Configured Tx Power = 0.00 dBm
LBC High Threshold = 98 percentage
Polarization parameters not supported by optics
Network SRLG values:
Not Configured
Lane Laser Bias TX Power RX Power
---- ---------- ---------- ----------
1 18.9 % -1.04 dBm -7.44 dBm
2 19.2 % -1.05 dBm -10.84 dBm
3 24.3 % -1.16 dBm -8.45 dBm
4 19.3 % -1.09 dBm -10.50 dBm
```

Step 3 **show tech-support ncs1k**

Collects the output logs.

What to do next

Verify the PM parameters of the Ethernet Controller. For more information on these parameters, see Verifying the Performance Monitoring Parameters of Controllers, on page 29.

Troubleshooting Breakout Patch Panel

Step 1   **show tech-support ncs1k**

Collects the output logs to troubleshoot breakout patch panel.

Step 2   Collect the logs of the following files to troubleshoot breakout patch panel. These files are present under XR bash prompt.

/var/log/pp_srv.log and **/var/log/pp_client.log**

Troubleshooting a Failed Commit Configuration

Use the following command to troubleshoot a configuration failure.

1. **Solution** Use the **show configuration failed** command to get information on why the configuration failed.

```
RP/0/RP0/CPU0:ios(config)# show configuration failed
Wed Dec  9 06:05:39.694 UTC
!! SEMANTIC ERRORS: This configuration was rejected by
!! the system due to semantic errors. The individual
!! errors with each failed configuration command can be
!! found below.


controller Optics0/0/0/13
 dwdm-carrier 100MHz-grid frequency 1911500
!!% Invalid argument: Wavelength change is allowed only in shutdown or maintenance state
!
end
```

Removing and Re-inserting DIMMs on the Controller Card

There are two DIMMs on the controller card (NCS1K-CNTLR=). If one DIMM is displaced, BIOS will boot; however, Cisco IOS XR does not boot due to insufficient memory. If both DIMMs are displaced, BIOS will not boot. In both the scenarios, it is recommended to remove and re-insert DIMMs on the controller card.

Before you begin

Follow the standard electrostatic discharge (ESD) rules according to local site practice before replacing DIMMs.

Step 1   Remove DIMMs - Push the connector latches down.

Step 2   Re-insert DIMMs - Push DIMM down into the connector by pressing on two points close to the far ends of DIMM.

Step 3   Verify correct insertion - The two connector latches must be closed if DIMM has been correctly inserted. Pull DIMM up to verify.

Figure 1: Remove and Re-insert DIMMs
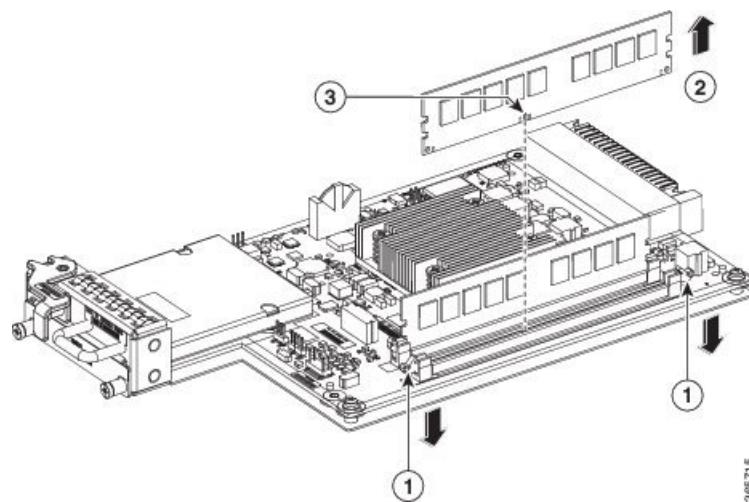
1	Push connector latches down
2	Pull DIMM up
3	Align when installing DIMM

Verifying Wavelength and Channel Mapping for Optics Controllers

Some of the troubleshooting scenarios where you need to verify the wavelength and channel mapping of the optics controllers are:

- Verify the connection between the NCS 1002 and a line system.

- Troubleshoot problems with the traffic.

- Clear an LOS.

show controllers optics R/S/I/P dwdm-carrrier-map

Displays the wavelength and channel mapping for optics controllers.

```
RP/0/RP0/CPU0:ios# show controllers optics 0/0/0/11 dwdm-carrrier-map
Thu Aug 27 15:59:00.385 UTC
DWDM Carrier Band:: C-Band
MSA ITU channel range supported: 1~97
DWDM Carrier Map table
-------------------------------------------------------
ITU Ch G.694.1 Frequency Wavelength
Num Ch Num (THz) (nm)
-------------------------------------------------------
1 60 196.10 1528.773
-------------------------------------------------------
2 59 196.05 1529.163
-------------------------------------------------------
3 58 196.00 1529.553
-------------------------------------------------------
4 57 195.95 1529.944
-------------------------------------------------------
5 56 195.90 1530.334
-------------------------------------------------------
6 55 195.85 1530.725
-------------------------------------------------------
7 54 195.80 1531.116
-------------------------------------------------------
8 53 195.75 1531.507
-------------------------------------------------------
9 52 195.70 1531.898
-------------------------------------------------------
10 51 195.65 1532.290
-------------------------------------------------------
11 50 195.60 1532.681
-------------------------------------------------------
12 49 195.55 1533.073
-------------------------------------------------------
13 48 195.50 1533.465
-------------------------------------------------------
14 47 195.45 1533.858
-------------------------------------------------------
15 46 195.40 1534.250
-------------------------------------------------------
16 45 195.35 1534.643
-------------------------------------------------------
17 44 195.30 1535.036
-------------------------------------------------------
18 43 195.25 1535.429
-------------------------------------------------------
19 42 195.20 1535.822
-------------------------------------------------------
20 41 195.15 1536.216
-------------------------------------------------------
<snip>
```

Verifying the Performance Monitoring Parameters of Controllers

Performance monitoring (PM) parameters are used by service providers to gather, store, set thresholds for, and report performance data for early detection of problems. The user can retrieve both current and historical PM counters for the various controllers in 10 seconds, 15 minutes and 1 day intervals.

show controllers *controllertype R/S/I/P* {**pm** {**current** | **history**} {**15-min** | **24-hour**} {**optics** | **ether** | **fec** | **otn**} *linenumber* }

Note For Ethernet controllers, only ingress statistics are supported.

The following sample output displays the current performance monitoring parameters of the Optics controller in 15 minute intervals.

Example:

```
RP/0/RP0:ios# show controllers optics 0/1/0/0 pm current 15-min optics 1
Tue Feb 10 14:59:06.945 UTC
Optics in the current interval {14:45:00 - 14:59:05 Tue Feb 15 2015]

Optics current bucket type : Valid
          MIN     AVG     MAX     Threshold(Min) TCA(enable) Threshold(Max) TCA(enable)

LBC[mA] : 735     735     735     0                NO             0             NO
OPT[dBm]:-1.23   -1.23   -1.23   2.5              NO             3.5           NO
OPR[dBm]:-1.07   -1.07   -1.07   -23.98           NO             -7.5          NO
```

The following sample output displays the historical performance monitoring parameters of the Ethernet controller in 24 hour intervals.

Example:

```
RP/0/RP0/CPU0:ios# show controllers HundredGigECtrlr 0/0/0/11 pm current 24-hour ether
Thu Nov 12 04:16:40.598 UTC

ETHER in the current interval [00:00:00 - 04:16:40 Thu Nov 12 2020]

ETHER current bucket type : Invalid

 RX-UTIL[%]:      98.49 Threshold : 0.00       TCA(enable) : NO

 RX-PKT :  46296223036  Threshold :   0 TCA(enable) : NO

 STAT-PKT :         0  Threshold :   0 TCA(enable) : NO

 OCTET-STAT : 60897581359118    Threshold :   0 TCA(enable) : NO

 OVERSIZE-PKT :     0  Threshold :   0 TCA(enable) : NO

 FCS-ERR :          0  Threshold :   0 TCA(enable) : NO

 LONG-FRAME :       0   Threshold :   0 TCA(enable) : NO

 JABBER-STATS :     0  Threshold :   0 TCA(enable) : NO

 64-OCTET :         0  Threshold :   0 TCA(enable) : NO

 65-127-OCTET :     0  Threshold :   0 TCA(enable) : NO

 128-255-OCTET :    0  Threshold :   0 TCA(enable) : NO

 256-511-OCTET :    0  Threshold :   0 TCA(enable) : NO
<snip>
```

The following sample output displays the current performance monitoring parameters of the coherent DSP controller in 15 minute intervals.

Example:

```
RP/0/RP0/CPU0:ios# show controllers coherentDSP 0/0/0/13 pm current 15-min otn
Thu Nov 12 04:14:50.475 UTC

g709 OTN in the current interval [ 4:00:00 - 04:14:50 Thu Nov 12 2020]

OTN current bucket type : Valid
    ES-NE   : 0          Threshold : 500      TCA(enable)  : YES
    ESR-NE  : 0.00000    Threshold : 0.00000  TCA(enable)  : NO
    SES-NE  : 0          Threshold : 500      TCA(enable)  : YES
    SESR-NE : 0.00000    Threshold : 0.00000  TCA(enable)  : NO
    UAS-NE  : 0          Threshold : 500      TCA(enable)  : YES
    BBE-NE  : 0          Threshold : 10000    TCA(enable)  : YES
    BBER-NE : 0.00000    Threshold : 0.00000  TCA(enable)  : NO
    FC-NE   : 0          Threshold : 10       TCA(enable)  : YES

    ES-FE   : 0          Threshold : 500      TCA(enable)  : YES
    ESR-FE  : 0.00000    Threshold : 0.00000  TCA(enable)  : NO
    SES-FE  : 0          Threshold : 500      TCA(enable)  : YES
    SESR-FE : 0.00000    Threshold : 0.00000  TCA(enable)  : NO
    UAS-FE  : 0          Threshold : 500      TCA(enable)  : YES
    BBE-FE  : 0          Threshold : 10000    TCA(enable)  : YES
    BBER-FE : 0.00000    Threshold : 0.00000  TCA(enable)  : NO
    FC-FE   : 0          Threshold : 10       TCA(enable)  : YES
```

The following sample output displays the current performance monitoring parameters of the coherent DSP controller for FEC in 15 minute intervals.

Example:

```
RP/0/RP0/CPU0:ios# show controllers coherentDSP 0/0/0/26 pm current 15-min fec
Thu Nov 12 01:22:48.953 UTC

g709 FEC in the current interval [ 1:15:00 - 01:22:49 Thu Nov 12 2020]

FEC current bucket type : Valid
    EC-BITS   : 619592625      Threshold : 903330       TCA(enable)  : YES
    UC-WORDS  : 0              Threshold : 5            TCA(enable)  : YES

                  MIN        AVG        MAX     Threshold  TCA       Threshold  TCA
                                                (min)      (enable)  (max)      (enable)
PreFEC BER  :  4.7E-06    6.2E-06    8.5E-06      0         NO         0         NO
PostFEC BER : <1.0E-15   <1.0E-15   <1.0E-15      0         NO         0         NO
```

Verifying and Troubleshooting Headless State Settings

NCS 1002 has a CPU that can be removed. It can carry traffic for at least 72 hours without the CPU. The functioning of the data path without CPU is termed as a headless operation.

Use the following commands to verify or troubleshoot headless state settings or hitless restart problems.

Step 1   **show hw-module slice** *slice_number* **internal**

Displays internal details of the slice and verifies if hitless restart is enabled on the slice. If hitless restart is enabled, the slice is initialized in the stateful (hitless restart) mode during the next CPU Online Insertion and Removal (OIR), or reload

operation and traffic is not impacted. If hitless restart is not enabled, the slice is initialized in the stateless mode and traffic is impacted.

Example:

```
RP/0/RP0/CPU0:ios# show hw-module slice 1 internal
Thu Nov 19 03:46:35.968 UTC
Slice ID:               1
Status:                 Provisioned
Client Bitrate:         10
Trunk Bitrate:          100

Headless Internal Information:
        State data: 0xA1B2C3D4
```

In the above example, the State data is 0xA1B2C3D4. If the value of the State data is 0xA1B2C3D4, the slice starts in the stateful mode and there is no impact on the traffic during the device CPU OIR or reload operation.

Example:

```
RP/0/RP0/CPU0:ios#show hw-module slice 1 internal
Fri Dec  4 09:52:08.823 UTC
Slice ID:               1
Status:                 Not Provisioned
Client Bitrate:         32767
Trunk Bitrate:          0
Headless Internal Information:
        State data: 0x0
```

In the above example, the State data is 0x0. Hence, the slice restarts in stateless mode.

After you provision the slice and the ports, use the above command to check if stateful mode is enabled on the slice.

The system can restart due to one of the following conditions:

- CPU OIR

- Device reload

- IOS-XR reload

- System admin reload

- mxp_driver process restart

Hitless restart or the headless functionality is enabled only if the slice is successfully provisioned. This mode is disabled if any one of the following configurations are in progress or have failed on the slice:

- **shutdown** or **no shutdown** of optics, Ethernet, or coherent DSP controllers.

- Transmit power configurations

- DWDM carrier frequency configuration

- Client and trunk loopback configurations

- FEC mode configuration

- Transmit TTI configuration

- Expected TTI configuration

During CPU OIR, or a reload operation, if a slice is initialized in the stateful mode and any datapath hardware component is not accessible, the headless feature cancels the reprovisioning of the slice to prevent any traffic impact.

Example:

```
RP/0/RP0/CPU0:ios#  show hw-module slice 0 internal
Tue Feb  9 05:24:48.075 UTC
Slice ID:              0
Status:                Reprovisioning Aborted [DP Access Failure - hitless reload]
Client Bitrate:        10
Trunk Bitrate:         100

Headless Internal Information:
        State data: 0xA1B2C3D4
```

Step 2   **show alarm brief card location** *location* **active**

Displays active alarms. You can verify if the equipment fail alarm is raised on the slice. This alarm is raised on the slice if the slice is not in a proper state or any hardware component is not accessible.

Example:

```
RP/0/RP0/CPU0:ios#show alarms brief card location 0/RP0/CPU0 active
Fri Jan 29 06:25:06.919 UTC

-------------------------------------------------------------------------------
Active Alarms
-------------------------------------------------------------------------------
Location       Severity     Group         Set Time            Description


-------------------------------------------------------------------------------
0/0            Critical     Slice         01/29/2016 06:23:46   Equipment Failure Slice 2


0/0            Critical     Controller    01/29/2016 05:58:28   Optics0/0/0/0 - Improper Removal
```

What to do next

Collect the output of the **show tech ncs1k detail** command if any the following conditions occur:

- Equipment fail alarm is raised.

- Stateful mode is disabled for an unknown reason.

Monitoring Headless Statistics

In the headless mode, the data path and statistics are maintained for at least 72 hours. These statistics are automatically cleared during the next reload or CPU-OIR operation.

Use this procedure to display the statistics collected during the last headless operation.

show controllers *controllertype R/S/I/P* **headless-stats**

Displays the statistics collected during the last headless operation. The collected statistics are preserved for a slice until the hardware module configuration is removed or changed on that slice.

Example:

The following example displays the statistics collected for the Ethernet controller during the last headless operation.

```
RP/0/RP0/CPU0:ios# show controllers fortyGigECtrlr 0/0/0/7 headless-stats
Thu Aug 30 06:32:58.936 UTC

Started in Stateful mode: Yes
Headless Start Time: Thu Aug 30 06:31:09 2018
Headless End   Time: Thu Aug 30 06:32:34 2018
Ethernet Headless Statistics
    RxPktsOverSized        : 0
    RxPktsBadFcs           : 0
    RxErrorJabbers         : 0
    RxPktsMulticast        : 3
    RxPktsBroadcast        : 0
    RxPktsUnicast          : 2020282144
    RxPktsUnderSized       : 0
    RxPkts                 : 2020282147
    RxBytesGood            : 387949441048
    RxPktsGood             : 2020282147
    RxRecvFragments        : 0
    RxPkts64Bytes          : 0
    RxPkts65To127Bytes     : 3
    RxPkts128to255Bytes    : 2004490979
    RxPkts256To511Bytes    : 15791165
    RxPkts512To1023Bytes   : 0
    RxPkts1024To1518Bytes  : 0
    RxTotalBytes           : 387949441096
    RxPktsDrop             : 0
    RxPause                : 0
    TxPkts                 : 2020283895
    TxTotalBytes           : 387949776554
    TxPktsUndersized       : 0
    TxPktsOversized        : 0
    TxPktsFragments        : 0
    TxPktsJabber           : 0
    TxPktsBadFcs           : 0
    TxPause                : 0
    RxLldpkts              : 3
```

The following example displays the statistics collected for the coherent DSP controller during the last headless operation.

```
RP/0/RP0/CPU0:ios# show controllers coherentDSP 0/0/0/12 headless-stats

Fri Dec 11 12:06:23.831 UTC

Started in Stateful mode: Yes
Headless Start Time: Fri Dec 11 11:21:23 2015
Headless End   Time: Fri Dec 11 11:23:59 2015
OTN Headless Statistics
    SmBip  :    0
    SmBei  :    0
    Fec EC :    4294967295
    Fec UC :    0
```

In the above example, the important fields are:

- Started in Stateful Mode—Indicates whether the slice corresponding to the controller port is in a stateful or stateless mode during the last CPU OIR, or reload operation.

- Headless Start Time—Time at which the NCS 1002 entered the headless mode of operation.

- Headless End Time—Time at which the NCS 1002 came out of the headless mode.

- SmBip—Section Monitoring Backward Error Indicator

- SmBei—Section Monitoring Bit Interleaved Parity

- Fec EC—Forward error correction Errors Corrected

- Fec UC—Forward Error Correction Uncorrected Words

Slices that start in the stateful mode are not reset during the last CPU OIR, or reload operation. Hence, the traffic is not interrupted on these slices. Slices that start in the stateless mode are reset. Hence, the traffic is interrupted on these slices. Slices that are successfully provisioned are in stateful mode. Headless start time and end time values are valid only if the slice corresponding to the controller is in a stateful mode.

Using SNMP for Troubleshooting

The supported MIBs in NCS 1002 are:

- CISCO-CONFIG-MAN-MIB

- CISCO-ENHANCED-MEMPOOL-MIB

- CISCO-PROCESS-MIB

- CISCO-SYSLOG-MIB

- ENTITY-MIB

- CISCO-ENTITY-FRU-CONTROL-MIB

- CISCO-IF-EXTENSION-MIB

- RMON-MIB

- CISCO-ENTITY-SENSOR-MIB

- CISCO-OPTICAL-MIB

- CISCO-OTN-IF-MIB

- LLDP-MIB

The CISCO-OTN-IF-MIB defines the managed objects for physical layer characteristics and the performance statistics of the OTN interfaces.

The CISCO-OPTICAL-MIB defines the managed objects for physical layer characteristics and the performance statistics of the optical interfaces.

For information on Cisco IOS XR SNMP Best Practices, see http://www.cisco.com/c/en/us/td/docs/ios_xr_sw/iosxr_r3-9-1/mib/guide/crs-gsr_appe.html.

Use the following commands in EXEC mode to verify and monitor the SNMP for network monitoring and management.

- **show snmp**—Displays the status of SNMP communications.

- **show snmp mib access**—Displays the counters per OID that indicate the number of times an operation was done on an OID.

- **show snmp mib access time**—Displays the timestamp of the last operation on an OID.

- **show snmp trace requests**—Displays a log of the high level PDU processing trace points.

- **debug snmp packet**—Displays information about every SNMP packet sent or received by the NCS 1002.

- **debug snmp requests**—Displays information about every SNMP request made by the SNMP manager.

Using Netconf for Troubleshooting

Netconf provides mechanisms to install, manipulate, and delete the configuration of network devices. The Netconf protocol provides a set of operations to manage device configurations and retrieve device state information.

Use the following commands in EXEC mode to retrieve device state information.

Before you begin

- Verify the installation of k9sec package.

- Generate the crypto key for SSH using the **crypto key generate dsa** command.

Note If you access NCS 1002 after regenerating the crypto key, you must remove the **~/.ssh/known_hosts** file as there will be a key mismatch between the host and the NCS 1002.

- Configure SSH.

```
RP/0/RP0/CPU0:ios# configure
RP/0/RP0/CPU0(config)# ssh server v2
RP/0/RP0/CPU0(config)# ssh server netconf port 830
RP/0/RP0/CPU0(config)# ssh server netconf  vrf default
```

Note Port 830 is the default Netconf port.

- Configure Netconf.

```
RP/0/RP0/CPU0:ios# configure
RP/0/RP0/CPU0(config)# netconf-yang agent ssh
```

Step 1 **show netconf-yang clients**

Displays the client details for netconf-yang.

Example:

```
RP/0/RP0/CPU0:ios# show netconf-yang clients
Tue Dec  8 07:49:14.846 UTC
Netconf clients
client session ID|     NC version|   client connect time|     last OP time|     last OP type|
    <lock>|
       1188487019|           1.1|      0d 16h 56m 50s|         01:17:13|              get|
         No|
       3445210079|           1.1|      0d 16h 56m 38s|         01:16:54|              get|
         No|
       3027026318|           1.1|      0d 16h 56m  1s|         01:16:50|              get|
         No|
       2653293062|           1.1|      0d 16h 56m 33s|         01:16:53|              get|
         No|
        96573454|           1.1|      0d 16h 56m 15s|         01:17:13|              get|
         No|
       2771481091|           1.1|      0d 16h 56m 45s|         01:17:14|              get|
         No|
```

Step 2   **show netconf-yang statistics**

Displays the statistical details for netconf-yang.

Example:

```
RP/0/RP0/CPU0:ios# show netconf-yang statistics
Tue Dec  8 07:49:45.506 UTC
Summary statistics
                        # requests|          total time|  min time per request|    max time per
 request|    avg time per request|
other                           0|    0h  0m  0s   0ms|    0h  0m  0s   0ms|       0h  0m
0s   0ms|      0h  0m  0s   0ms|
close-session                   0|    0h  0m  0s   0ms|    0h  0m  0s   0ms|       0h  0m
0s   0ms|      0h  0m  0s   0ms|
kill-session                    0|    0h  0m  0s   0ms|    0h  0m  0s   0ms|       0h  0m
0s   0ms|      0h  0m  0s   0ms|
get-schema                      0|    0h  0m  0s   0ms|    0h  0m  0s   0ms|       0h  0m
0s   0ms|      0h  0m  0s   0ms|
get                         11161|    0h  0m 48s 332ms|    0h  0m  0s   0ms|       0h  0m
0s  27ms|      0h  0m  0s   0ms|
get-config                      0|    0h  0m  0s   0ms|    0h  0m  0s   0ms|       0h  0m
0s   0ms|      0h  0m  0s   0ms|
edit-config                     0|    0h  0m  0s   0ms|    0h  0m  0s   0ms|       0h  0m
0s   0ms|      0h  0m  0s   0ms|
commit                          0|    0h  0m  0s   0ms|    0h  0m  0s   0ms|       0h  0m
0s   0ms|      0h  0m  0s   0ms|
cancel-commit                   0|    0h  0m  0s   0ms|    0h  0m  0s   0ms|       0h  0m
0s   0ms|      0h  0m  0s   0ms|
lock                            0|    0h  0m  0s   0ms|    0h  0m  0s   0ms|       0h  0m
0s   0ms|      0h  0m  0s   0ms|
unlock                          0|    0h  0m  0s   0ms|    0h  0m  0s   0ms|       0h  0m
0s   0ms|      0h  0m  0s   0ms|
discard-changes                 0|    0h  0m  0s   0ms|    0h  0m  0s   0ms|       0h  0m
0s   0ms|      0h  0m  0s   0ms|
validate                        0|    0h  0m  0s   0ms|    0h  0m  0s   0ms|       0h  0m
0s   0ms|      0h  0m  0s   0ms|
xml parse                   11161|    0h  0m  5s 717ms|    0h  0m  0s   0ms|       0h  0m
0s   2ms|      0h  0m  0s   0ms|
netconf processor           11161|    0h  0m 48s 332ms|    0h  0m  0s   0ms|       0h  0m
0s  27ms|      0h  0m  0s   0ms|
YFW                         11161|    0h  7m 32s 350ms|    0h  0m  0s  10ms|       0h  0m
0s  97ms|      0h  0m  0s   0ms|
pending requests                0|    0h  0m  0s   0ms|    0h  0m  0s   0ms|       0h  0m
```

```
0s   0ms|      0h  0m  0s   0ms|
Statistics for session with ID: 1188487019
<snip>
```

Step 3 **show netconf-yang trace**

Debugs and verifies Netconf.

Example:

```
RP/0/RP0/CPU0:ios# show netconf-yang trace
Tue Dec  8 07:50:54.590 UTC
[12/08/15 07:30:37.851 UTC 1046d3 4942] TRC: nc_sm_session_find_session_id:1386 Found session 3027026318
 0x1852f68
[12/08/15 07:30:37.851 UTC 1046d4 4942] DBG: nc_sm_yfw_response_cb:2816 Received OK response for
session-id '3027026318', for message-id '856615', which has 'NO ERROR' and 'DATA'
[12/08/15 07:30:37.851 UTC 1046d5 4942] TRC: nc_sm_yfw_response_complete:2700 DATA element in chunk
 state: CONTINUE
[12/08/15 07:30:37.851 UTC 1046d6 4942] TRC: nc_pxs_send:223 SERVER->CLIENT 688 (iov: 0x1ae7bd8)
[12/08/15 07:30:37.851 UTC 1046d7 4942] TRC: nc_sm_yfw_response_handle:2638 malloc_trim called (rc
= 1)
[12/08/15 07:30:37.851 UTC 1046d8 4942] TRC: nc_sm_yfw_response_cb:2906 More responses to come for
msg id '856615'
[12/08/15 07:30:37.852 UTC 1046d9 13229] TRC: nc_px_fdout_handler:563 SSH PIPE OUTPUT cond: 0x2, fd
 129, ctx 0x60d800
[12/08/15 07:30:37.859 UTC 1046da 4942] TRC: nc_sm_session_find_session_id:1386 Found session 3027026318
 0x1852f68
[12/08/15 07:30:37.859 UTC 1046db 4942] DBG: nc_sm_yfw_response_cb:2816 Received OK response for
session-id '3027026318', for message-id '856615', which has 'NO ERROR' and 'DATA'
[12/08/15 07:30:37.859 UTC 1046dc 4942] TRC: nc_sm_yfw_response_complete:2700 DATA element in chunk
 state:
<snip>
```

Verifying Alarms

show alarms brief [**card** [**location** *location*] | **rack**|**system**]   [**active**|**clients**|**history**|**stats**]]

show alarms detail [**card** [**location** *location*] | **rack**|**system**]   [**active**|**clients**|**history**|**stats**]]

Displays alarms in brief or detail.

Example:

```
RP/0/RP0/CPU0:ios# show alarms brief card location 0/RP0/CPU0 active
Mon Dec 14 00:01:29.499 UTC

-------------------------------------------------------------------------------
Active Alarms
-------------------------------------------------------------------------------
Location      Severity    Group       Set Time           Description


-------------------------------------------------------------------------------
0/0           Minor       Controller   12/10/2015 07:49:41   Optics0/0/0/0 - Optics Low
Receive Power
0/0           Critical    Controller   02/13/2001 13:34:32 Optics0/0/0/7 - Improper Removal
0/0           Critical    Controller   02/13/2001 13:34:32 Optics0/0/0/8 - Improper Removal
0/0           Critical    Controller   02/13/2001 13:34:32 Optics0/0/0/9 - Improper Removal
0/0           Critical    Controller   02/13/2001 13:34:32 Optics0/0/0/10 - Improper Removal
```

```
0/0            Critical    Controller    02/13/2001 13:34:32 Optics0/0/0/20 - Improper Removal
0/0            Major       Ethernet      02/13/2001 13:34:34 HundredGigECtrlr0/0/0/14 - Carrier
 Loss On The LAN
```

Note   In the maintenance mode, all alarms are suppressed and the **show alarms** command will not show the alarms details. Use the **show controllers** *controllertype R/S/I/P* command to view the client and trunk alarms.

What to do next

For more information about alarms and steps to clear them, see the .

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.

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
Sat Nov  28 17:53:24.796 UTC

OBFL Uptime Information For : 0/RP0
  NOTE: Read Operation in progress; Incomplete Data Displayed
       * 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      : ABC_CHA_SN
       Current Chassis SN       : CHANGE-ME-
       Previous R/S/I           : 0/0/0
       Current R/S/I            : 0/0/0
       Write Interval           : 15 (min)
       First Power On TS        : 10/08/2015 06:47:10
       Last Erase TS            : --/--/---- --:--:--
       Rack Change Count        : 1
       Slot Change Count        : 4


  --------------------------------------------------------------------------------
       UPTIME INFORMATION
  --------------------------------------------------------------------------------
   Start Time Stamp   | End Time Stamp      | Card Uptime info
   mm/dd/yyyy hh:mm:ss | mm/dd/yyyy hh:mm:ss | Weeks.Days.Hrs.Min.Sec
```

```
--------------------------------------------------------------------------------
11/27/2015 20:44:32 | 11/27/2015 22:11:18 | 0.0.1.26.46
11/27/2015 22:11:18 | 11/28/2015 17:21:59 | 0.0.19.10.41
11/28/2015 17:21:59 | 11/28/2015 17:51:59 | 0.0.0.30.0
```

Capturing Logs

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
Sat Nov 28 22:12:45.450 UTC
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
    Console logging: level debugging, 2720 messages logged
    Monitor logging: level debugging, 281 messages logged
    Trap logging: level informational, 0 messages logged
    Buffer logging: level debugging, 3332 messages logged

Log Buffer (2097152 bytes):
<snip>
```

a)   **logging buffered** *size*

Configures the size of the logging buffer. The range is from 2097152 to 125000000 bytes.

Example:

```
RP/0/RP0/CPU0:ios(config)#logging buffered 3000000
```

Step 2   **show tech-support** and **show tech-support ncs1k**

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 ncs1k
Fri Nov 13 17:31:23.360 UTC
++ Show tech start time: 2015-Nov-13.173123.UTC ++
Fri Nov 13 17:31:25 UTC 2015 Waiting for gathering to complete
.
Fri Nov 13 17:33:32 UTC 2015 Compressing show tech output
Show tech output available at 0/RP0/CPU0 : /harddisk:/showtech/showtech-ncs1k-2015-Nov-13.173123.UTC.tgz
```

Step 3   **show tech-support alarm-mgr**

Collects the Cisco support file for the alarm manager component.

Example:

```
RP/0/RP0/CPU0:ios#show tech-support alarm-mgr
Sat Jan 30 21:41:53.894 UTC
```

```
++ Show tech start time: 2016-Jan-30.214154.UTC ++
Sat Jan 30 21:41:56 UTC 2016 Waiting for gathering to complete
Sat Jan 30 21:44:02 UTC 2016 Compressing show tech output
Show tech output available at 0/RP0/CPU0 :
/harddisk:/showtech/showtech-alarm_mgr-2016-Jan-30.214154.UTC.tgz
++ Show tech end time: 2016-Jan-30.214402.UTC ++
```

Step 4 **show tech-support ptah**

Collects the Cisco support file for the Physical Transport Alarm Hardware (PTAH) component.

Example:

```
RP/0/RP0/CPU0:ios#show tech-support ptah file disk0:
Sat Jan 30 21:50:33.016 UTC
++ Show tech start time: 2016-Jan-30.215033.UTC ++
Sat Jan 30 21:50:35 UTC 2016 Waiting for gathering to complete
Sat Jan 30 21:52:41 UTC 2016 Compressing show tech output
Show tech output available at 0/RP0/CPU0 : /harddisk:/showtech-ptah-2016-Jan-30.215033.UTC.tgz
++ Show tech end time: 2016-Jan-30.215242.UTC ++
```

Step 5 **show proc mxp_driver | inc Job**

Captures the job ID of the mxp_driver process, which is the NCS 1002 muxponder driver process.

Example:

```
RP/0/RP0/CPU0:ios#show proc mxp_driver | inc Job
Sat Jan 30 21:46:26.584 UTC
                Job Id: 189
```

Step 6 **show ptah trace all jid** *job_id*

Captures the interaction traces between the mxp_driver process and PTAH.

Example:

```
RP/0/RP0/CPU0:ios#show ptah trace all jid 189 location 0/RP0/CPU0 | file
disk0:show_ptah_trace_189_job.log
Sat Jan 30 21:47:29.633 UTC
[OK]
RP/0/RP0/CPU0:ios#dir disk0:
Sat Jan 30 21:47:47.661 UTC

Directory of disk0:
 8114 drwxr-xr-x 2   4096 Jan 30 00:12 ztp
   12 lrwxrwxrwx 1     12 Jan 30 00:09 config -> /misc/config
16225 drwxr-xr-x 2   4096 Jan 30 21:44 showtech
   11 drwxr-xr-x 2   4096 Jan 30 00:09 core
   23 -rwx------ 1 295238 Jan 30 21:47 show_ptah_trace_189_job.log
 8115 drwxr-xr-x 2   4096 Jan 30 01:05 nvgen_traces
 8113 drwx------ 2   4096 Jan 30 00:10 clihistory

1005620 kbytes total (935528 kbytes free)
```

What to do next

You should gather the above information before calling the Cisco Technical Assistance Center (TAC).

Verifying Process Details and Crash Dump

Step 1   **show processes**

Displays information about active processes.

Example:

The following example shows the output of the **show processes** command in the EXEC mode.

```
RP/0/RP0/CPU0:ios# show processes
!! File saved at 17:22:13 UTC Fri Nov 13 2015 by root
JID    TID  Stack  pri  state       NAME            rt_pri
1      1     0K    20   Sleeping    init            0
66449  913   0K    20   Sleeping    oom.sh          0
66470  934   0K    20   Sleeping    cgroup_oom.sh   0
66471  935   0K    20   Sleeping    oom.sh          0
66495  959   0K    0    Sleeping    cgroup_oom      0
66495  997   0K    0    Sleeping    lwm_debug_threa 0
66495  998   0K    0    Sleeping    cgroup_oom      0
<snip>
```

The following example shows the output of the **show processes** command in the system admin EXEC mode.

```
sysadmin-vm:0_RP0# show processes all location 0/rp0
Sat Nov  28 22:52:27.441 UTC
-----------------------------------------------------------------
node:      0/RP0
-----------------------------------------------------------------
LAST STARTED             STATE   RE-     MANDA-  MAINT-  NAME(IID) ARGS
                                 START   TORY    MODE
-----------------------------------------------------------------
11/28/2015 17:21:29.000 Run     1                       aaad(0)
11/28/2015 17:21:32.000 Run     1                       ael_mgbl(0)
11/28/2015 17:21:29.000 Run     1       M               calv_alarm_mgr(0)
11/28/2015 17:21:29.000 Run     1       M               cm(0)
11/28/2015 17:21:29.000 Run     1       M               confd_helper(0) -t token -v -d -w 400 -b 30
 -p 600 -r 10 -f 10
11/28/2015 17:21:29.000 Run     1                       ctrl_driver(0) -i atom -u |1f10:1.0 -l
|1f11:2.0
11/28/2015 17:21:29.000 Run     1                       dd_driver(0)
<snip>
```

Step 2   **show processes** *process-name*

Displays detailed information about a process.

Example:

```
RP/0/RP0/CPU0:ios#show processes mxp_driver
Sat Feb 11 03:05:49.468 UTC
            Job Id: 148
               PID: 3795
    Executable path: /opt/cisco/XR/packages/ncs1k-os-support-2.0.0.0-r61101I/rp/bin/mxp_driver
         Instance #: 1
         Version ID: 00.00.0000
            Respawn: ON
      Respawn count: 1
       Last started: Fri Feb 10 11:59:20 2017
      Process state: Run
      Package state: Normal
               core: MAINMEM
```

```
                Max. core: 0
                    Level: 200
                Placement: None
            startup_path:
/opt/cisco/XR/packages/ncs1k-os-support-2.0.0.0-r61101I/rp/startup/mxp_driver.startup
                Ready: 134.140s
        Process cpu time: 0.000 user, 15061.040 kernel, 15061.040 total
JID   TID   Stack  pri  state         NAME              rt_pri
148   3795   0K    20   Sleeping      Infra Agent        0
148   4176   0K    20   Sleeping      lwm_debug_threa    0
148   4177   0K    20   Sleeping      mxp_driver         0
148   4181   0K    20   Sleeping      lwm_service_thr    0
148   4182   0K    20   Sleeping      qsm_service_thr    0
148   4223   0K    20   Sleeping      mxp_driver         0
148   4351   0K    20   Sleeping      pm_ui thread       0
148   4353   0K    20   Sleeping      Infra Agent        0
148   4366   0K    20   Sleeping      Infra Agent        0
148   4378   0K    20   Sleeping      ptah_common_eve    0
148   4439   0K    20   Sleeping      async              0
148   4522   0K    20   Sleeping      Infra Agent        0
148   4543   0K    20   Sleeping      Infra Agent        0
148   4554   0K    20   Sleeping      Infra Agent        0
148   5110   0K    20   Sleeping      PrvAgt Slice 0     0
148   5111   0K    20   Sleeping      PrvAgt Slice 1     0
148   5112   0K    20   Sleeping      PrvAgt Slice 2     0
148   5113   0K    20   Sleeping      PrvAgt Slice 3     0
148   5114   0K    20   Sleeping      Fmea Agent         0
148   5115   0K    20   Sleeping      Pm Agent           0
148   5116   0K    20   Sleeping      Sw Poller Agent    0
148   5117   0K    20   Sleeping      Alarm Agent        0
148   5118   0K    20   Sleeping      Infra Agent        0
148   5119   0K    20   Sleeping      Squelch Agent      0
148   5120   0K    20   Sleeping      Dap Server         0
148   5121   0K    20   Sleeping      Infra Agent        0
148   5122   0K    20   Sleeping      Infra Agent        0
-------------------------------------------------------------------------------
```

Step 3   **show context**

Displays information about process crashes.

Example:

```
RP/0/RP0/CPU0:ios# show context
Thu Apr  23 08:42:32.328 UTC
**************************************************************
Location : 0/RP0
**************************************************************
Core location: 0/RP0:/misc/disk1

Core for pid = 1463 (aaad)
Core for process: aaad_1463.by.11.20150423-083922.sysadmin-vm:0_RP0.009d5.core.gz
Core dump time: 2015-04-23 08:39:23.058000000 +0000
Process:
Core was generated by `/opt/cisco/calvados/bin/aaad'.

Build information:
### XR Information

User = aaaa
Host = agl-ads-2232
Workspace = /nobackup/aaaa/xspeed-new
Lineup = proj:xspeed
XR version = 6.0.0.01I
```

```
[…]
Signal information:
Program terminated with signal 11, Segmentation fault.

Faulting thread: 1463

Registers for Thread 1463
rax:    0xfffffffffffffffc
rbx:    0x23a34e0
[…]

Backtrace for Thread 1463
#0  0x00007fa1fd1c8b43 in epoll_wait+0x33 from /lib64/libc-2.12.so
#1  0x00007fa1ff6992f6 in ?? () from /usr/lib64/libevent-2.0.so.5.0.1
[…]
<snip>
```

CHAPTER **2**

Alarm Troubleshooting

This chapter gives a description, severity, and troubleshooting procedure for each commonly encountered Cisco NCS 1002 alarm and condition. When an alarm is raised, refer to its clearing procedure.

Alarm Logical Objects

Alarms are raised against logical objects. These logical objects represent physical objects such as cards, ports, and logical objects such as trunk.

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

Table 1: Alarm Logical Object Type Definitions

Logical Object	Definition
FT	Fan-tray assembly.
PPM	Pluggable port module (PPM, also called SFP), referring to MXP and TXP cards.
PSU	Power Supply Unit.
Chassis	Chassis equipment.
Client	Ethernet.
Temp Sensor	Temperature Sensor.
Voltage Sensor	Voltage Sensor.
Trunk	DWDM

Alarm Severity

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

- Critical (CR) alarm—Indicates severe, service-affecting trouble that needs immediate correction.

- Major (MJ) alarm—Indicates a serious alarm, but the trouble has less impact on the network.

- Minor (MN) condition—Indicates alarms that do not affect service.

- Not Alarmed (NA) condition—Indicates conditions that are information indicators.

- Not Reported (NR) condition—Indicates a condition that occurs as a secondary result of another event.

Alarms

This section lists the NCS 1002 alarms alphabetically. The severity, description, and troubleshooting procedure accompany each alarm.

ALL-FAN-TRAY-REMOVAL Alarm

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

Logical Objects: FT

The ALL-FAN-TRAY-REMOVAL alarm is raised on the NCS 1002 when all the fan trays are removed from the chassis.

Clear the ALL-FAN-TRAY-REMOVAL Alarm

Insert all three fans into the chassis.

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

CD Alarm

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

Logical Objects: TRUNK

The Chromatic Dispersion (CD) alarm is raised on the NCS 1002 when the detected chromatic dispersion value is above or below the configured threshold values. You can configure the chromatic dispersion threshold values using the **controller optics** *R/S/I/P* **cd-high-threshold** and **controller optics** *R/S/I/P* **cd-low-threshold**

commands in the config mode. The range is -70000 to +70000 ps/nm when the trunk bit rate is 100G. The range is -20000 to +20000 ps/nm when the trunk bit rate is 200G or 250G.

Clear the CD Alarm

Step 1 Verify the value of the chromatic dispersion threshold of the NCS 1002 using the **show controller optics** *R/S/I/P* command.

Step 2 If the value is not within the threshold range, configure the chromatic dispersion threshold using the **controller optics** *R/S/I/P* **cd-high-threshold** and **controller optics** *R/S/I/P* **cd-low-threshold** command in the config mode.

Step 3 If the value is within the range of the chromatic dispersion threshold, contact Cisco Technical Assistance Center (TAC).

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

DAISYDUKE-CPU-FPGA-PCIE-ERROR Alarm

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

Logical Objects: EQUIPMENT

The DAISYDUKE-CPU-FPGA-PCIE-ERROR alarm occurs when the Daisy Duke CPU FPGA is unable to communicate with the CPU controller due to a Peripheral Component Interconnect Express (PCIe) error.

Clear the DAISYDUKE-CPU-FPGA-PCIE-ERROR Alarm

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

DAISYDUKE-CPU-PROCESSOR-HOT Alarm

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

Logical Objects: EQUIPMENT

The DAISYDUKE-CPU-PROCESSOR-HOT alarm occurs when the daisyduke FPGA detects that the temperature of the CPU processor is high.

Clear the DAISYDUKE-CPU-PROCESSOR-HOT Alarm

Verify if all the fans are functioning properly.

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

DGD Alarm

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

Logical Objects: TRUNK

The Differential Group Delay (DGD) alarm is raised on the NCS 1002 when the value of the differential group delay read by the pluggable port module exceeds the configured threshold value. You can configure the threshold value using the **controller optics** *R/S/I/P* **dgd-high-threshold** command in the config mode.

Clear the DGD Alarm

Step 1   Verify the value of the differential group delay threshold of the NCS 1002 using the **show controller optics** *R/S/I/P* command.

Step 2   If the value is not within the threshold range, configure the differential group delay threshold using the **controller optics** *R/S/I/P* **dgd-high-threshold** command in the config mode. The range is from 0 to 18000 (in units of 0.01 ps).

Step 3   If the value is within the range of the differential group delay threshold, contact Cisco TAC.

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

EQPT-FAIL-SLICE Alarm

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

Logical Objects: Slice

The Equipment Fail (EQPT-FAIL) slice alarm is raised on the NCS 1002 when any component or device within the slice fails. The alarm is tagged as Not Service Affecting (NSA) if the device is not in the service path. The failed device is on a port that is not provisioned.

Clear the EQPT-FAIL-SLICE Alarm

Step 1   Reload the host using the **hw-module location 0/RP0 reload** command.

Step 2   If the alarm does not clear, do a traffic-impacting system reload using the **hw-module location all reload** command.

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

FAM-FAULT-TAG-UNIT-UNSUPPORTED ALARM

Default Severity: Critical

Logical Objects: Equipment

The FAM-FAULT-TAG-UNIT-UNSUPPORTED alarm is raised when unsupported control card is inserted in NCS 1002. The unsupported control card is NCS1K-CNTLR2.

Clear the FAM-FAULT-TAG-UNIT-UNSUPPORTED Alarm

Replace the control card with the control card supported in NCS 1002.

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

FAM-FAULT-TAG-PMO-UNIT-UNSUPPORTED ALARM

Default Severity: Critical

Logical Objects: PEM

The FAM-FAULT-TAG-PMO-UNIT-UNSUPPORTED alarm is raised when unsupported power module is inserted in PEM slot. The unsupported power module is NCS1K-2KW-AC2.

Clear the FAM-FAULT-TAG-PMO-UNIT-UNSUPPORTED Alarm

Replace the power module with the power module supported in NCS 1002.

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

FAN FAIL Alarm

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

Logical Objects: FT

The FAN FAIL alarm is raised on the NCS 1002 when one of the three fans fail. When any fan fails, the temperature of the NCS 1002 can rise above its normal operating range. This condition can trigger the TEMP THRESHOLD alarm.

Clear the FAN FAIL Alarm

Verify that a fan is correctly inserted. The fan should run immediately when correctly inserted.

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

FAN MISSING Alarm

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

Logical Objects: FT

The FAN MISSING alarm is raised on the NCS 1002 when one of the three fans is missing or is not correctly inserted. When any fan is missing, the temperature of the NCS 1002 can rise above its normal operating range. This condition can trigger the TEMP THRESHOLD alarm.

Clear the FAN MISSING Alarm

Step 1 Verify that a fan is missing or is not correctly inserted.

Step 2 Insert a fan. The fan should run immediately when correctly inserted.

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

FAN-TRAY-INSERT Alarm

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

Logical Objects: FT

The FAN-TRAY-INSERT alarm is raised on the NCS 1002 when the fan tray is detected in the chassis.

Clear the FAN-TRAY-INSERT Alarm

This alarm clears automatically.

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

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

Logical Objects: FT

The FAN-TRAY-REMOVAL alarm is raised on the NCS 1002 when any of the three fans is removed from the chassis.

Clear the FAN-TRAY-REMOVAL Alarm

Insert the fan to clear the alarm.

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

HI-LASERBIAS Alarm

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

Logical Objects: PPM

The Equipment High Transmit Laser Bias (HI-LASERBIAS) current alarm is raised against the NCS 1002 laser performance. This alarm occurs when the physical pluggable port laser detects a laser bias value beyond the configured high threshold. The alarm indicates that the port laser has reached the maximum laser bias tolerance. You can configure the threshold value using the **controller optics** *R/S/I/P* **lbc-high-threshold** command in the config mode.

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

Clear the HI-LASERBIAS Alarm

Step 1 Verify the value of the laser bias high threshold of NCS 1002 using the **show controller optics** *R/S/I/P* command.

Step 2 If the value is not within the high laser bias threshold range, configure the high laser bias threshold using the **controller optics** *R/S/I/P* **lbc-high-threshold** command in the config mode. The range is from 0 to 100%.

Step 3 If the value is within the range of the high laser bias threshold, physically replace the pluggable module. Replacement is not urgent and can be scheduled during a maintenance window.

If the condition does not clear, log into the Technical 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 Objects: PPM

The Equipment High Receive Power (HI-RXPOWER) alarm is an indicator of the received optical signal power of NCS 1002. This 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. This alarm occurs on the trunk optics controller when the total optical signal power of the received signal exceeds the default or user-defined threshold. You can configure the threshold value using the **controller optics** *R/S/I/P* **rx-high-threshold** command in the config mode.

Clear the HI-RXPOWER Alarm

Step 1   Verify the value of the high receive power threshold of the NCS 1002 using the **show controller optics** *R/S/I/P* command.

Step 2   If the value is not within the high receive power threshold range, configure the high receive power threshold using the **controller optics** *R/S/I/P* **rx-high-threshold** command in the config mode. The range is from -400 to 300 dBm (in units of 0.1 dBm).

Step 3   If the value is within the range of the high receive power threshold, physically verify, by using a standard power meter that the optical input power is overcoming the expected power threshold.

Step 4   Change the threshold value or use an attenuator to reduce the input power to the desired level.

If the condition does not clear, log into the Technical 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 Objects: PPM

The Equipment High Transmit Power (HI-TXPOWER) alarm is an indicator of the transmitted optical signal power of NCS 1002. This 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. This alarm occurs on the trunk optics controller when the total optical signal power of the transmitted signal exceeds the default or user-defined threshold. You can configure the threshold value using the **controller optics** *R/S/I/P* **tx-high-threshold** command in the config mode.

Clear the HI-TXPOWER Alarm

Step 1   Verify the value of the high transmit power threshold of NCS 1002 using the **show controller optics** *R/S/I/P* command.

Step 2   If the value is not within the high transmit power threshold range, configure the high transmit power threshold using the **controller optics** *R/S/I/P* **tx-high-threshold** command in the config mode. The range is from -400 to 300 dBm (in units of 0.1 dBm).

Step 3 If the value is within the range of the high transmit power threshold, physically verify, by using a standard power meter that the optical output power is overcoming the expected power threshold. If so, the pluggable module should be replaced at first opportunity.

If the condition does not clear, log into the Technical 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 Objects: Client

The High Bit Error Rate (HIBER) alarm is raised on the NCS 1002 when the client and trunk ports receive 16 or more invalid sync-headers in 125 microseconds. This alarm occurs when the NCS 1002 is configured with 10 GE or 10 GE Fibre Channel (FC) payloads.

Limitation:

HIBER alarm is detected on Rx for 0.5 seconds. After 0.5 secs, the link is brought down automatically leading to loss of block lock(SYNCLOSS). Due to this limitation, the end user cannot be able to potentially see HIBER through CLI, since Ncs1k/XR Alarm reporting soak time is only 2 seconds (for raising).

Clear the HIBER Alarm

The alarm clears under the following conditions:

- When the card port does not receive a high bit error rate.
- When the optical connectors are cleaned.

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

IMPROPRMVL Alarm

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

Logical Objects: PPM

The Improper Removal (IMPROPRMVL) alarm occurs when a physical pluggable is absent on a service-provisioned port of the NCS 1002.

Clear the IMPROPRMVL Alarm

Step 1 Verify if the pluggable is plugged into the port of the NCS 1002 using the **show inventory** command.

Step 2 If the QSFP or CFP is not plugged into the port, insert the appropriate QSFP or CFP.

Note Before you configure the client data rate of the NCS 1002, ensure that the appropriate QSFP or CFP is plugged into the port of the NCS 1002.

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

LO-RXPOWER Alarm

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

Logical Objects: PPM

The Equipment Low Receive Power (LO-RXPOWER) alarm is an indicator of the received optical signal power of NCS 1002. This alarm occurs on the client optics controller when the measured individual lane optical signal power of the received signal falls below the default or user-defined threshold. This alarm occurs on the trunk optics controller when the total optical signal power of the received signal falls below the default or user-defined threshold. You can configure the threshold value using the **controller optics** *R/S/I/P* **rx-low-threshold** command in the config mode.

Clear the LO-RXPOWER Alarm

Step 1 Verify the value of the receive power of NCS 1002 using the **show controller optics** *R/S/I/P* command.

Step 2 If the value is not within the low receive power threshold range, configure the low receive power threshold using the **controller optics** *R/S/I/P* **rx-low-threshold** command in the config mode. The range is from -400 to 300 dBm (in units of 0.1 dBm).

Step 3 If the value is within the range of the low receive power threshold, physically verify, by using a standard power meter that the optical input power overcomes the expected power threshold. Ensure that a proper threshold has been provisioned for the receive value. If an incorrect threshold has been set, adjust it to a value within the allowed limits.

Step 4 Verify that the Trunk-Rx port is cabled correctly, and clean the fiber connecting the faulty TXP/MXP to the drop port of the DWDM card.

Step 5 Determine whether a bulk attenuator is present and if so, verify that a proper fixed attenuation value has been used.

Step 6 Using a test set, check the optical power value of the drop port of the DWDM card connected to the faulty TXP/MXP. If the read value is different (+1 dBm or 1 dBm) from the ANS setpoint for Padd&drop-Drop power, move to next step.

Step 7 Look for any alarm reported by the DWDM cards belonging to the OCHNC circuit whose destination is the faulty TXP/MXP and first troubleshoot that alarm. Possible alarm related include: amplifier Gain alarms, Automatic Power Control (APC) alarms, and LOS-P alarms on the Add or Drop ports belonging to the OCHNC circuit.

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

LO-TXPOWER Alarm

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

Logical Objects: PPM

The Equipment Low Transmit Power (LO-TXPOWER) alarm is an indicator of the transmitted optical signal power of NCS 1002. This alarm occurs on the client optics controller when the measured individual lane optical signal power of the transmitted signal falls below the default or user-defined threshold. This alarm occurs on the trunk optics controller when the total optical signal power of the transmitted signal falls below the default or user-defined threshold. You can configure the threshold value using the **controller optics** *R/S/I/P* **tx-low-threshold** command in the config mode. The range is from -400 to 300 dBm (in units of 0.1 dBm).

Clear the LO-TXPOWER Alarm

Step 1 Verify the value of the low transmit power threshold of NCS 1002 using the **show controller optics** *R/S/I/P* command.

Step 2 If the value is not within the low transmit power threshold range, configure the low transmit power threshold using the **controller optics** *R/S/I/P* **tx-low-threshold** command in the config mode. The range is from -400 to 300 dBm (in units of 0.1 dBm).

Step 3 If the value is within the range of the low transmit power threshold, physically verify, by using a standard power meter that the optical output power is overcoming the expected power threshold. If so, the pluggable module should be replaced at first opportunity.

If the condition does not clear, log into the Technical 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 Objects: Client

The LOCAL-FAULT alarm is raised on the NCS 1002 client port provisioned with 10 GE, 40 GE, or 100 GE payloads. This alarm occurs when a local fault character sequence is received in the incoming MAC stream as defined in IEEE 802.3.

Clear the LOCAL-FAULT Alarm

Verify that the NCS 1002 receives proper MAC streams from the far-end router or switch.

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

LOM Alarm

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

Logical Objects: TRUNK

The Optical Transport Unit (OTU) Loss of Multiframe (LOM) alarm is an OTN alarm for the trunk port and occurs when the Multi Frame Alignment Signal (MFAS) is corrupted. This alarm is raised when the MFAS overhead field is invalid for more than five frames and persists for more than 3 milliseconds.

Clear the LOM Alarm

Step 1 Ensure that the fiber connector for the card is completely plugged in.

Step 2 If the bit error rate (BER) threshold is correct and at the expected level, use an optical test set to measure the power level of the line to ensure it is within guidelines.

Step 3 If the optical power level is good, verify that optical receive levels are within the acceptable range.

Step 4 If receive levels are good, clean the fibers at both ends according to site practice.

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

Step 6 If the fiber is of the correct type, verify that a single-mode laser is used at the far-end node.

Step 7 Clean the fiber connectors at both ends for a signal degrade according to site practice.

Step 8 Verify that a single-mode laser is used at the far end.

Step 9 If the problem does not clear, the transmitter at the other end of the optical line could be failing and require replacement

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

LOS-P Alarm

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

Logical Objects: TRUNK

The Loss of Signal Payload (LOS-P) alarm for the trunk layer indicates that the PPM or CFP does not get any incoming payload signal. The purpose of the LOS-P alarm is to alert the user that no optical power is being received from the fiber. A common fault condition signaled by this alarm is a fiber cut. In this case, neither the payload nor the overhead signals are received.

Clear the LOS-P Alarm

Step 1 Verify that the trunk port is configured with the proper wavelength. For more information see the *Cisco NCS 1000 Series Configuration Guide*.

Step 2 Verify if there is a loss of received optical power. Compare the actual power levels with the expected power range..

Step 3 Verify the fiber continuity to the port of the NCS 1002 and fix the fiber connection.

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

LOWER-CTRL-FPGA-PCIE-ERROR

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

Logical Objects: EQUIPMENT

The LOWER-CTRL-FPGA-PCIE-ERROR alarm is raised when a control FPGA of the lower board is unreachable because of a Peripheral Component Interconnect Express (PCIe) error.

Clear the LOWER-CTRL-FPGA-PCIE-ERROR Alarm

If the alarm does not clear it indicates that it is a hardware fault.

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

MEA Alarm

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

Logical Objects: PPM

The Missing Equipment Attributes (MEA) alarm for the PPM or QSFP is raised on a pluggable port of the NCS 1002 when there is a mismatch in the configured client data rate and the supported QSFP physical data rate. For example, if the configured client data rate is 10G and the supported data rate of the QSFP is 100G, then this alarm is raised.

Clear the MEA Alarm

Step 1 Verify the supported physical data rate of the QSFP on the NCS 1002 using the **show inventory** command.

Step 2 Verify the configured client data rate on the NCS 1002 using the **show hw-module slice** command.

Step 3 If the above values do not match, insert the appropriate QSFP pluggable or configure the required client data rate using the **hw-module location** *location* **slice** *slice_number* **client bitrate** [**10G** | **40G** | **100G**] command.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/

en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

MIXED-AC-DC-PTS Alarm

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

Logical Objects: EQUIPMENT

The MIXED-AC-DC-PTS alarm occurs when both the AC and DC power trays are detected in the chassis.

Clear the MIXED-AC-DC-PTS Alarm

Use either the AC or DC power module.

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

MKA-LOCALLY-SECURED Alarm

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

Logical Objects: Client

The MACsec Key Agreement-Locally-Secured (MKA-LOCALLY-SECURED) alarm is raised, when MKA session becomes locally secured, due to the loss of an active programmed peer.

A node loses its peer under the following conditions:

- When the node shuts down its interface.

  When the node issues **no macsec** command for more than 6 times.

Clear the MKA-LOCALLY-SECURED Alarm

The alarm clears after confirming the macsec configuraiton and the interface state on the nodes.

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

MKA-START-FAIL-MISSING-PSK Alarm

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

Logical Objects: Client

The MACsec Key Agreement-Start-Fail-Missing-Pre-Shared-Keys alarm is raised on the NCS 1002 interface, when MKA session cannot start due to the application of macsec keychain that has no active keys.

Clear the MKA-START-FAIL-MISSING-PSK Alarm

The alarm clears after configuring the lifetime of the key to current active key and bringing up the mks session.

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

MKA-UNSECURE-MISSING-PSK Alarm

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

Logical Objects: Client

The MACsec Key Agreement-UNSECURE-MISSING-Pre-Shared-Keys alarm is raised, when the existing secured MKA session is brought down. This is due to the insecurity caused by the non-active keys present in the keychain on the NCS 1002 interface.

Clear the MKA-UNSECURE-MISSING-PSK Alarm

The alarm clears after configuring an active key in the keychain for bringing up the mka session. It is also required to have overlapping keys, so that the next key becomes active prior to the expiry of existing key.

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

MORE-THAN-ONE-FAN-TRAY-REMOVED Alarm

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

Logical Objects: EQUIPMENT

The MORE-THAN-ONE-FAN-TRAY-REMOVED alarm occurs when more than one fan tray is removed from the chassis.

Clear the MORE-THAN-ONE-FAN-TRAY-REMOVED Alarm

Ensure that all the three fans are inserted and are functioning properly.

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

NM-I2C-ACCESS-ERROR Alarm

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

Logical Objects: EQUIPMENT

The Node Management Inter-Integrated Circuit Access Error (NM-I2C-ACCESS-ERROR) alarm occurs when there is an I2C error.

Clear the NM-I2C-ACCESS-ERROR Alarm

You must contact TAC if you encounter this alarm.

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

NM-SHUTDOWN-CARD Alarm

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

Logical Objects: EQUIPMENT

The NM-SHUTDOWN-CARD alarm occurs when a card shuts down due to a critical error.

Clear the NM-SHUTDOWN-CARD Alarm

If the alarm does not clear contact TAC as there can be a hardware fault.

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

NOT ABLE TO COMMUNICATE WITH PATCH-PANEL Alarm

Default Severity: Minor (MN)

Logical Objects: Software

This alarm is raised on NCS 1002 when communication with the breakout patch-panel is lost. The alarm is also raised when the connected interface goes down or the patch panel reloads. Also, it is raised when the connected interface goes down or the panel reloads.

Clear the NOT ABLE TO COMMUNICATE WITH PATCH-PANEL Alarm

The alarm clears after establishing communication with the patch panel. Also, check whether the patch panel is reachable and is not reloaded.

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

OSNR Alarm

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

Logical Objects: TRUNK

The optical signal-to-noise ratio (OSNR) alarm is an indicator of the OSNR of NCS 1002. The OSNR alarm occurs when the measured OSNR falls below the threshold. You can configure the threshold value using the **controller optics** *R/S/I/P* **osnr-low-threshold** command in the config mode.

Clear the OSNR Alarm

Step 1   Verify the value of the minimum acceptable OSNR value of NCS 1002 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 config mode. The range is 0 to 4000 (in units of 0.01db).

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

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

OTUK-AIS Alarm

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

Logical Objects: TRUNK

An Alarm Indication Signal (AIS) signal communicates to the receiving node when the transmit node does not send a valid signal. AIS is not an error. The OTUK-AIS alarm is raised by the receiving node on each input when it detects the AIS instead of a real signal.

OTUK-AIS is a generic AIS signal with a repeating AIS PN-11 sequence. This pattern is inserted by the card in the ITU-T G.709 frame (Trunk) when a faulty condition is present on the client side.

Clear the OTUK-AIS Alarm

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

OTUK-BDI Alarm

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

Logical Objects: TRUNK

The Optical Transport Unit Backward Defect Indication (OTUK BDI) alarm is raised when there is a path termination error in the upstream data. This error is read as a BDI bit in the path monitoring area of the digital wrapper overhead.

Clear the OTUK-BDI Alarm

Step 1 At the near-end node, use site practices to clean trunk transmitting fiber toward the far-end node and the client receiving fiber.

Step 2 At the far-end node, determine whether any OTUK-AIS condition, is present on the Trunk-RX. If so, the root cause to be investigated is the Trunk-TX side on the near-end card (the one alarmed for OTUK-BDI) because that is the section where the AIS bit is inserted.

Step 3 If there is no OTUK-AIS at the far-end node, continue to investigate performances of the Trunk-Rx: Look for other OTU-related alarms, such as the OTUK-LOF condition or OTUK-SD condition at the far-end Trunk-RX. If either is present, resolve the condition using the appropriate procedure in this chapter.

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

OTUK-LOF Alarm

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

Logical Objects: TRUNK

The Optical Transport Unit Loss of Frame (OTUK-LOF) alarm is raised when a frame loss is detected by an invalid frame alignment in the received frames. This alarm indicates that the card has lost frame delineation on the input data. Loss of frame occurs when the optical transport unit overhead frame alignment (FAS) area is invalid for more than five frames and that the error persists more than three milliseconds.

This alarm is also raised when the FEC settings on trunk ports of the source and destination cards are different.

Clear the OTUK-LOF Alarm

Verify if the FEC settings on trunk ports of the source and destination cards are same.

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

OTUK-SD Alarm

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

Logical Objects: TRUNK

The Optical Transport Unit Signal Degrade (OTUK-SD) alarm occurs when the quality of signal is so poor that the bit error rate on the incoming optical line passed the signal degrade threshold.

Clear the OTUK SD Alarm

Rectify the reason of poor quality signal.

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

OTUK-SF Alarm

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

Logical Objects: TRUNK

Both hardware and software can generate the Optical Transport Unit Signal Fail (OTUK-SF) alarm based on the summarization of LOS, LOF, and LOM alarms.

Clear the OTUK SF Alarm

OTUK SF alarm gets cleared when none of the defects LOS, LOF, or, LOM exist.

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

OTUK-TIM Alarm

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

Logical Objects: PORT

The OTUK-TIM alarm or the Trail Trace Identifier (TTI) Mismatch alarm is raised on the NCS 1002 when the expected TTI string does not match the received section trace string.

Clear the OTUK-TIM Alarm

Rectify the reason to have different expected and received TTI strings.

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

PATCH-PANEL POWER REDUNDANCY LOST ALARM

Default Severity: Minor (MN)

Logical Objects: Power

The PATCH-PANEL POWER REDUNDANCY LOST alarm is raised when one of the power supply units present in the breakout patch-panel is not functional.

Clear the PATCH-PANEL POWER REDUNDANCY LOST Alarm

The alarm clears when the power supply unit is restored.

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

PEM-MODULE-INSERT Alarm

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

Logical Objects: PEM

The PEM-MODULE-INSERT alarm is raised on the NCS 1002 when the Power Entry Module (PEM) is inserted into the chassis.

Clear the PEM-MODULE-INSERT Alarm

This alarm clears automatically.

If the condition does not clear, log into the Technical 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-MODULE-REMOVAL Alarm

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

Logical Objects: PEM

The PEM-MODULE-REMOVAL alarm is raised on the NCS 1002 when one of the redundant PEM module is removed from the system.

Clear the PEM-MODULE-REMOVAL Alarm

This alarm clears when the redundant PEM module is inserted back into the chassis.

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

POWER MODULE OUTPUT DISABLED Alarm

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

Logical Objects: PEM

The POWER MODULE OUTPUT DISABLED alarm is raised on the NCS 1002 when the power supply is disabled on the active PEM.

Clear the POWER MODULE OUTPUT DISABLED Alarm

This alarm clears when the power supply is enabled.

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

PEM-PWR-TRAY-LVL-RED-LOST

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

Logical Objects: PEM

The PEM-PWR-TRAY-LVL-RED-LOST alarm is raised on the NCS 1002 when one of the two active PEMs is removed.

Clear the PEM-PWR-TRAY-LVL-RED-LOST Alarm

This alarm clears when you insert a power supply on the chassis.

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

PLL-FAIL-SLICE Alarm

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

Logical Objects: SLICE

The PLL-FAIL-SLICE alarm is raised on the slice when a fault is detected in the Phase Lock Loop (PLL) device and it becomes inaccessible.

Clear the PLL-FAIL-SLICE Alarm

Remove the slice configuration and reload the Cisco IOS XR.

If the alarm does not clear it indicates that it is a hardware fault.

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

PPM FAIL Alarm

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

Logical Objects: PPM

The PPM FAIL alarm is raised on the physical pluggable when a fault is detected in the PPM and it becomes inaccessible.

Clear the PPM FAIL Alarm

Replace the pluggable.

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

PKG-K9SEC-REQ Alarm

Default Severity: Minor (MN)

Logical Objects: Chassis equipment

The PKG-K9SEC-REQ alarm occurs when the encrypted slice is configured without installing the k9sec package or the macsec_mka_aipc_driver library or if the k9sec package is removed when encrypted slice is available. The macsec_mka_aipc_driver library is contained in the k9sec package.

Clear the PKG-K9SEC-REQ Alarm

This alarm clears after you install the k9sec package containing the macsec_mka_aipc_driver library.

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

PSU FAIL Alarm

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

Logical Objects: PSU

The PSU FAIL alarm is raised on the NCS 1002 when one of the power modules fail.

Clear the PSU FAIL Alarm

You must log into the Technical Support Website at http://www.cisco.com/cisco/web/support/index.html for more information or call Cisco TAC (1 800 553-2447) immediately.

PSU INSERTED Alarm

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

Logical Objects: PSU

The PSU INSERTED alarm is raised on the NCS 1002 when a power supply is inserted to the device.

Clear the PSU INSERTED Alarm

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

PSU REDUNDANCY LOST Alarm

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

Logical Objects: PSU

The PSU REDUNDANCY LOST alarm is raised on the NCS 1002 when a power supply is removed.

Clear the PSU REDUNDANCY LOST Alarm

The alarm clears when a power supply is inserted on the NCS 1002

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

REMOTE-FAULT Alarm

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

Logical Objects: CLIENT

The REMOTE-FAULT alarm is raised on the NCS 1002 when a remote fault character sequence is received in the incoming MAC stream as defined in IEEE 802.3.

Clear the REMOTE-FAULT Alarm

Step 1 Verify and resolve the client port fault and remote fault errors on the remote or upstream node.

Step 2 Verify and resolve loss of signal synchronization error on the remote or upstream node.

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

RM-DEVICE-OUT-OF-TOL Alarm

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

Logical Objects: FT

The RM-DEVICE-OUT-OF-TOL alarm is raised on the NCS 1002 when the fan is malfunctioned and is not working properly.

Clear the RM-DEVICE-OUT-OF-TOL Alarm

Replace the malfunctioned fan.

If the condition does not clear, log into the Technical 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 Objects: CLIENT

The Signal Loss on Data Interface alarm is raised on the client-side QSFP of the NCS 1002 when there is a loss of Ethernet signal.

Clear the SIGLOSS Alarm

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 get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

SYNCLOSS Alarm

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

Logical Objects: CLIENT

The Loss of Synchronization on Data Interface alarm is raised on the NCS 1002 client and trunk ports when there is a loss of signal synchronization on the port. This alarm is demoted by the SIGLOSS alarm.

Clear the SYNCLOSS Alarm

Step 1   Ensure that the data port connection at the near end of the Ethernet link is operational.

Step 2   Verify the fiber continuity to the port. To do this, follow site practices.

Step 3   For 100 GE, verify that the FEC settings match between the router and NCS 1002.

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

SQUELCHED Alarm

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

Logical Objects: GE, CLIENT

The client signal squelched condition is raised by the NCS 1002 in the following situations:

- Laser-squelch is configured under the client controller.

Note   Laser-squelch is supported only on QSFP+, QSFP28 LR4, and QSFP28 CWDM4 pluggables.

- Laser-squelching occurs on a QSFP pluggable when all the four lanes operating in the 10 GE client mode are turned off after the upstream receive facility has experienced a loss of signal (such as optical LOS, LOF).

- A MXP or TXP client facility detects that an upstream receive facility has experienced a loss of signal (such as optical LOS, LOF). In response, the client facility transmit is turned off (SQUELCHED). The upstream receive facility is the trunk receive on the same slice as the client.

- The client will squelch if the upstream trunk receive (on the trunk port carrying the client payload) experiences a LOS, or LOF (TRUNK) alarm.

- The client will squelch if any one of trunk ports receive LOS, or LOF. In this case, the client port is mapped to two trunk ports. For example, the HundredGigECtrlr 0/0/0/9 is mapped to the CoherentDSP0/0/0/12 and the CoherentDSP0/0/0/13 for a 10 GE to 100 GE hw-module config.

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

- OTUK-LOF Alarm, on page 62
- LOS-P Alarm, on page 56

Far-end Laser Squelch

NCS 1002 supports far-end laser squelch. This feature relays the following:

- Client input signal to the far-end client output signal, especially faults.

- Near-end client-side faults such as SIGOSS, SYNCLOSS, HIBER, and LF to the far-end.

  If a near-end QSFP has a fault on its RX side, the far-end QSFP laser is turned off.

The SQUELCHED alarm is raised on the far-end NCS 1002 if laser-squelch is configured on the far-end NCS 1002 and a fault on the near-end NCS 1002 is observed on the client RX side.

Note   Far-end client laser squelch does not work on headless events such as a reload, CPU OIR, or an mxp_driver restart.

Clear the SQUELCHED Alarm

Determine whether the associated NCS 1002 trunk port reports an LOF or LOS alarm (for the client trunk). If it does, turn to the relevant section in this chapter and complete the troubleshooting procedure.

TEMPERATURE Alarm

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

Logical Objects: EQUIPMENT

The temperature alarms are raised on the NCS 1002 when the temperature is not within the operating range. When this condition occurs, critical devices like DSP, and ETNA automatically shut down.

The alarm can appear in one of the following formats:

- [*sensor name*] : high temperature alarm

- [*sensor name*] : low temperature alarm

The [*sensor name*] : high temperature alarm is raised when the temperature is high and not within the operating range.

The [*sensor name*] : low temperature alarm is raised when the temperature is low and not within the operating range.

All sensors managed at the CPU level have NM as the prefix. NM denotes Node management. All sensors managed at the rack level have RM as the prefix. RM denotes Rack management. Some alarms that come in this category have the alarm tags as: NM-TEMP, RM-TEMP.

Fan Speed and Chassis Inlet Temperature Thresholds

The table below lists the chassis inlet temperature threshold values for the different fan speeds.

Fan speed (rpm)	Rising Min Temperature (°C)	Rising Max Temperature (°C)	Falling Max Temperature (°C)	Falling Min Temperature (°C)
4800	-127	28	27	-127
5500	29	30	29	28
8500	31	36	35	30
10500	37	41	40	36
12500	42	44	43	41
14500	45	127	127	44

Clear the TEMPERATURE Alarm

This alarm clears when the temperature falls within the operating range.

Step 1   Verify the temperature of the NCS 1002.

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

Step 3   If the room temperature is not abnormal, physically ensure that nothing prevents the fan-tray assembly from passing air through the system shelf. You must also check if any fan has failed.

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

TX-POWER-PROV-MISMATCH Alarm

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

Logical Objects: PPM

The Provisioned Optics Transmit Power Not Supported (TX-POWER-PROV-MISMATCH) alarm is raised when the laser transmit power configured is not within the range of output power supported by the CFP2 pluggable. The alarm indicates that the configured Tx power is not supported by the pluggable though the configured power is applied to the Tx laser.

Clear the TX-POWER-PROV-MISMATCH Alarm

Step 1   Verify the value of the configured TX power on NCS 1002 using the show controller optics R/S/I/P command.

Step 2   If the value is not within the output power range supported by the pluggable type, configure the Tx power using the controller optics R/S/I/P transmit-power command in the Optics Controller configuration mode.

The range is from -11.5dBm to -1.5dBm for ONS-CFP2-WDM,-11.5dBm to -1.5dBm for ONS-CFP2-WDM-1KL and -8dBm to 2dBm for ONS-CFP2-WDM-1KE PID types. The PID information can be obtained from inventory details using show inventory command.

If the condition does not clear, log into the Technical 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 Reported (NR), Non-Service-Affecting (NSA)

Logical Objects: TRUNK

The Uncorrected FEC Word condition indicates that the FEC capability cannot correct the frame.

Clear the UNC-WORD Alarm

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 receive levels are good, clean the fibers at both ends.

Step 6   If the condition does not clear, verify that a single-mode fiber is used.

Step 7   Verify if the fiber is of single-mode type.

Step 8   Clean the fiber connectors at both ends for a signal degrade.

Step 9   If the problem does not clear, the transmitter at the other end of the optical line could be failing and requires replacement.

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

UPPER-CTRL-FPGA-PCIE-ERROR Alarm

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

Logical Objects: EQUIPMENT

The UPPER-CTRL-FPGA-PCIE-ERROR alarm is raised when a control FPGA of the upper board is unreachable because of a Peripheral Component Interconnect Express (PCIe) error.

Clear the UPPER-CTRL-FPGA-PCIE-ERROR Alarm

If the alarm does not clear it indicates that it is a hardware fault.

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

VOLTAGE Alarms

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

Logical Objects: EQUIPMENT

The voltage alarms are raised on the NCS 1002 when the voltage is not within the operating range. When this condition occurs, critical devices like DSP, and ETNA automatically shut down.

The alarm can appear in one of the following formats:

- [*sensor name*] : high voltage alarm

- [*sensor name*] : low voltage alarm

The [*sensor name*] : high voltage alarm is raised when the voltage is high and not within the operating range.

The [*sensor name*] : low voltage alarm is raised when the voltage is low and not within the operating range.

All sensors managed at the CPU level have NM as the prefix. NM denotes Node management. All sensors managed at the rack level have RM as the prefix. RM denotes Rack management. Some alarms that come in this category have the alarm tags as: FAM-FAULT-NM-L, FAM-FAULT-NM-H, FAM-FAULT-RM-L, FAM-FAULT-RM-H.

Clear the VOLTAGE Alarms

This alarm clears when the voltage falls within the operating range.

Verify the voltage of the power source. The voltage rating value for AC power ranges between 200 V to 240 V depending on the standards in various countries. The voltage rating value for DC power is 48 V, the fuse rating must not exceed 60 A.

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

WVL-OUT-OF-LOCK Alarm

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

Logical Objects: TRUNK

The Wavelength Out of Lock (WVL-OUT-OF-LOCK) alarm is raised when the trunk port detects that the optical input frequency is out of range.

Clear the WVL-OUT-OF-LOCK Alarm

Step 1   Verify the wavelength configuration.

Step 2   Verify if the CFP is inserted properly.

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

I N D E X