Configuration Guide for Cisco NCS 1001, IOS XR Release 25.x.x

Cisco Network Convergence System 1001
Updated July 27, 2026

Full Cisco Trademarks with Software License

Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Topics included

1 Configure Management Interfaces

Topics:

Plan for dual management Ethernet connectivity, configure Link Layer Discovery Protocol, and verify neighbor data on Cisco NCS 1001.

Management interfaces

This topic explains how management interfaces provide device access for configuration, discovery, monitoring, and operational data collection on Cisco NCS 1001.

Management interfaces are device access points that support management connectivity, neighbor discovery, and operational visibility for Cisco NCS 1001.

Dual management Ethernet interfaces

This topic explains how two independent management Ethernet interfaces support management connectivity through RJ45 and optical SFP ports on Cisco NCS 1001.

Dual management Ethernet interfaces are independent Cisco IOS XR interfaces that let you connect the RJ45 and optical SFP management ports to different switches on the same or different subnets.

Management Ethernet interfaces

Starting with release R6.5.1, different ports from the Ethernet switch–MGMT RJ45 and optical SFP MGMT–connect to the CPU. In Cisco IOS XR, the two management Ethernet interfaces correspond to different management ports.

- **MgmtEth0/RP0/CPU0/0**:RJ45 port.
- **MgmtEth0/RP0/CPU0/1**:SFP port.

Dual interface restrictions

Review these restrictions before you use the optical SFP management interface.

- iPXE is not supported over the optical interface during power-on.
- Upgrades from earlier releases, which use only the SFP management interface, can lose management connectivity. If connectivity is lost, configure the device through the console port.
- Upgrade the BIOS and reload the 0/RP0 location before using both management interfaces.

Example

This example shows the output of the **show running-config** command for management interfaces.

```
RP/0/RP0/CPU0:Device#show running-config
interface MgmtEth0/RP0/CPU0/0
 ipv4 address 192.0.2.10 255.255.255.0
!
interface MgmtEth0/RP0/CPU0/1
 ipv6 address 2001:DB8:1::1/64
 ipv6 enable
!
interface MgmtEth0/RP0/OSC1/0
 shutdown
!
interface MgmtEth0/RP0/OSC2/0
 shutdown
!
interface MgmtEth0/RP0/OSC3/0
 shutdown
!
```

LLDP on management interfaces

This topic explains how Link Layer Discovery Protocol on management interfaces advertises and learns neighbor information for topology discovery and operations.

Link Layer Discovery Protocol (LLDP) support on management interfaces is a neighbor discovery capability that lets a system advertise and learn neighbor information through the management network.

Neighbor discovery

The system advertises LLDP type-length-value (TLV) details over the management network. Other devices use these details to learn about this device.

LLDP advantages

LLDP provides neighbor discovery for non-Cisco devices and supports topology discovery for Operations, Administration, and Maintenance (OAM) workflows.

CDP and LLDP device discovery

This topic compares device discovery behavior for Cisco Discovery Protocol and Link Layer Discovery Protocol on Layer 2 networks for management planning.

Use this comparison to understand which discovery protocol applies to Cisco and non-Cisco devices.

This table compares Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP) for device discovery purposes.

Table 1: Device discovery protocol comparison

Protocol	Scope	Purpose
CDP	Runs over Layer 2 on Cisco devices such as routers, bridges, access servers, and switches.	Lets network management applications discover and learn about Cisco devices connected to the network.
LLDP	Runs over Layer 2 and supports systems that use different network layer protocols.	Lets network management applications discover and learn about non-Cisco devices connected to the network.

Supported LLDP object identifiers

This topic lists the object identifiers that non-Cisco monitoring tools can query through Simple Network Management Protocol for LLDP data.

Use these object identifiers (OIDs) to identify LLDP information that the system supports for non-Cisco monitoring tools.

LLDP provides information about physical network connections that monitoring tools can retrieve through Simple Network Management Protocol (SNMP).

The system supports these LLDP OIDs:

- 1.0.8802.1.1.2.1.4.1.1.4
- 1.0.8802.1.1.2.1.4.1.1.5
- 1.0.8802.1.1.2.1.4.1.1.6
- 1.0.8802.1.1.2.1.4.1.1.7
- 1.0.8802.1.1.2.1.4.1.1.8

- 1.0.8802.1.1.2.1.4.1.1.9
- 1.0.8802.1.1.2.1.4.1.1.10
- 1.0.8802.1.1.2.1.4.1.1.11
- 1.0.8802.1.1.2.1.4.1.1.12

Prerequisites for LLDP configuration

This topic provides support details to review before you configure Link Layer Discovery Protocol on management interfaces and access operational data.

Use these requirements to confirm that LLDP behavior and operational data access meet your management interface needs.

- LLDP full-stack functionality is supported on all three management interfaces in the Cisco NCS 1001 system.
- You can enable or disable LLDP selectively on any management interface.
- You can enable or disable LLDP transmit or receive functionality at the management interface level.
- Information gathered through LLDP can be stored in the device Management Information Database (MIB) and queried with SNMP.
- LLDP operational data is available in both the command-line interface (CLI) and the NETCONF and YANG interface.

LLDP global attributes

This topic provides default values, supported ranges, and descriptions for global Link Layer Discovery Protocol attributes used by management interfaces.

Use these values when you configure LLDP globally for management interfaces.

Table 2: Global LLDP attributes

Attribute	Default	Range	Description
Hold time	120 seconds	0 to 65535 seconds	Specifies how long an LLDP device maintains neighbor information before discarding it.
Reinit	2 seconds	2 to 5 seconds	Specifies the delay for LLDP initialization on an interface.
Timer	30 seconds	5 to 65534 seconds	Specifies the rate at which LLDP packets are sent.

Configure LLDP globally

Use this procedure to enable Link Layer Discovery Protocol globally and set the timing attributes for supported management interfaces on Cisco NCS 1001.

Configure LLDP globally to enable transmit and receive operations on all the interfaces that support LLDP.

You can override global LLDP behavior at the interface level to disable receive or transmit operations.

For more information about global attributes, see LLDP global attributes.

Procedure

1. Enter global configuration mode.

Example

```
RP/0/RP0/CPU0:ios#configure terminal
```

2. Use the **lldp management enable** command to enable LLDP on management interfaces.

Example

```
RP/0/RP0/CPU0:ios(config)#lldp management enable
```

3. Configure LLDP timing attributes.

Example

```
RP/0/RP0/CPU0:ios(config)#lldp holdtime 30
RP/0/RP0/CPU0:ios(config)#lldp reinit 2
```

4. Commit the configuration and exit global configuration mode.

Example

```
RP/0/RP0/CPU0:ios(config)#commit
RP/0/RP0/CPU0:ios(config)#end
```

LLDP is enabled globally for both the **MgmtEth0/RP0/CPU0/0** and **MgmtEth0/RP0/CPU0/1** management interfaces.

Verify LLDP configuration

Use this procedure to verify Link Layer Discovery Protocol configuration, interface state, and neighbor data on management interfaces before troubleshooting.

Verify LLDP configuration to confirm that the device advertises and receives management interface neighbor information.

Procedure

---

1. Use the **show running-config lldp** command to display the running LLDP configuration.

Example

```
RP/0/RP0/CPU0:Device# show running-config lldp
Tue Dec 10 10:36:11.567 UTC
lldp
 timer 30
 reinit 2
 holdtime 120
 management enable
!
```

2. Use the **show lldp interface** command to display LLDP interface state.

Example

```
RP/0/RP0/CPU0:Device# show lldp interface
Thu Nov 7 08:45:22.934 UTC

MgmtEth0/RP0/CPU0/0:
        Tx: enabled
        Rx: enabled
        Tx state: IDLE
        Rx state: WAIT FOR FRAME

MgmtEth0/RP0/CPU0/1:
        Tx: enabled
        Rx: enabled
        Tx state: IDLE
        Rx state: WAIT FOR FRAME
```

3. Use the **show lldp neighbors** command to display LLDP neighbor information.

Example

```
RP/0/RP0/CPU0:Device#show lldp neighbors
Mon Dec 2 11:01:20.143 CET
Capability codes:
        (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
        (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Device ID       Local Intf              Hold-time  Capability     Port ID
[DISABLED]      MgmtEth0/RP0/CPU0/0     120        B               gi19
MYS-130         MgmtEth0/RP0/CPU0/1     120        R
MgmtEth0/RP0/CPU0/1
```

The output shows the LLDP interface state and neighbor information for the management interfaces.

Enable LLDP on a management interface

Use this procedure to enable Link Layer Discovery Protocol on a specific management interface when interface-level control is required on Cisco NCS 1001.

Enable LLDP on a management interface to allow the interface to participate in neighbor discovery.

Procedure

---

1. Enter global configuration mode.

Example

```
RP/0/RP0/CPU0:ios#configure terminal
```

2. Enter the management interface configuration mode.

Example

```
RP/0/RP0/CPU0:ios(config)#interface MgmtEth0/RP0/CPU0/1
```

3. Use the **lldp enable** to enable LLDP on the management interface.

   Example

```
RP/0/RP0/CPU0:ios(config-if)#lldp enable
```

4. Commit the configuration and exit interface configuration mode.

   Example

```
RP/0/RP0/CPU0:ios(config-if)#commit
RP/0/RP0/CPU0:ios(config-if)#end
```

LLDP is enabled on the specified management interface.

Disable LLDP transmit operations

Use this procedure to stop a management interface from transmitting Link Layer Discovery Protocol advertisements when the device must not advertise local discovery data

Disable LLDP transmit operations to prevent a management interface from advertising local neighbor discovery information.

Procedure

1. Enter the global configuration mode.

   Example

```
RP/0/RP0/CPU0:ios#configure terminal
```

2. Enter the management interface configuration mode.

   Example

```
RP/0/RP0/CPU0:ios(config)#interface MgmtEth0/RP0/CPU0/1
```

3. Use the **lldp transmit disable** command to disable LLDP transmit operations.

   Example

```
RP/0/RP0/CPU0:ios(config-if)#lldp transmit disable
```

4. Commit the configuration and exit interface configuration mode.

   Example

```
RP/0/RP0/CPU0:ios(config-if)#commit
RP/0/RP0/CPU0:ios(config-if)#end
```

The management interface no longer transmits LLDP advertisements.

Disable LLDP receive operations

Use this procedure to prevent a management interface from receiving Link Layer Discovery Protocol advertisements when learning neighbor discovery data is not desired.

Disable LLDP receive operations to prevent a management interface from learning neighbor discovery information.

Procedure

1. Enter the global configuration mode.

   Example

   ```
   RP/0/RP0/CPU0:ios#configure terminal
   ```

2. Enter the management interface configuration mode.

   Example

   ```
   RP/0/RP0/CPU0:ios(config)#interface MgmtEth0/RP0/CPU0/1
   ```

3. Use the **lldp receive disable** command to disable LLDP receive operations.

   Example

   ```
   RP/0/RP0/CPU0:ios(config-if)#lldp receive disable
   ```

4. Commit the configuration and exit interface configuration mode.

   Example

   ```
   RP/0/RP0/CPU0:ios(config-if)#commit
   RP/0/RP0/CPU0:ios(config-if)#end
   ```

The management interface no longer receives LLDP advertisements.

LLDP debugging commands

This topic lists the commands that help you inspect traffic and debug Link Layer Discovery Protocol behavior on the device during troubleshooting.

Use these commands when you troubleshoot LLDP functionality.

- **show lldp traffic**
- **debug lldp all**
- **debug lldp errors**
- **debug lldp events**
- **debug lldp packets**

- **debug lldp tlvs**
- **debug lldp trace**
- **debug lldp verbose**

2 Configure Controllers

Topics:

Manage OTS and OTS OCH controllers, span loss, dual IP addressing, and LLDP over OSC functions on Cisco NCS 1001 systems.

Controllers

This topic explains controller identifiers and the rack, slot, instance, and port values that identify the optical controller locations in the system.

A controller identifier is a location value that

- uses the Rack/Slot/Instance/Port format,
- identifies the optical controller that you configure or display, and
- uses values such as **0/1/0/1** for a specific controller location.

Controller identifier fields
Table 3: Controller identifier fields

Field	Value
Rack	0
Slot	1 to 3. These slots support pluggable optical modules.
Instance	0
Port	Depends on the specific pluggable optical module.

OTS controllers

This topic explains Optical Transport Section controllers and the hardware capabilities that determine which optical parameters can be enabled, displayed, or configured.

An Optical Transport Section (OTS) controller is an optical interface controller that

- stores the optical parameters for the OTS interfaces,
- exposes parameters based on hardware capabilities such as photodiode, variable optical attenuator (VOA), amplifier, optical channel monitor (OCM), and
- supports receive and transmit section parameters when the hardware supports them.

When an OTS controller is created, each hardware capability is enabled or disabled. For example, when a photodiode is present, the OTS controller can read the total optical power.

You can configure OTS parameters such as low power threshold, VOA attenuation set point, amplifier gain range, amplifier tilt, amplifier gain set point, channel power, and safety control mode. OTS interface descriptions cannot be added in the same way as descriptions on the optical amplifier module.

Configuration parameters of OTS controller
Table 4: Configuration parameters of OTS controller

Parameter	Description	Hardware capability	Range	Default	Notes
rx-low-threshold (0.1 dBm)	Low receive power threshold.	Photodiode	-400 to +300	-40.0	

Parameter	Description	Hardware capability	Range	Default	Notes
tx-low-threshold (0.1 dBm)	Low transmit power threshold.	Photodiode	-400 to +300	-20.0	
rx-voa-attenuation (0.1 dBm)	RX VOA attenuation set point.	VOA	0 to 200	0.0	
tx-voa-attenuation (0.1 dBm)	TX VOA attenuation set point.	VOA	0 to 200	0.0	
ampli-control-mode	Amplifier control mode.	Amplifier	automatic, manual	automatic	The automatic value is compatible only when the grid is specified through the **hw-module** configuration.
ampli-gain-range	Amplifier gain range.	Amplifier	normal, extended	normal	The amplifier gain range is configurable only when the controller is in shutdown state.
ampli-gain (0.1 dBm)	Amplifier gain set point.	Amplifier	0 to 500	0.0	The actual range depends on the amplifier gain range.
ampli-tilt (0.1 dBm)	Amplifier tilt.	Amplifier	-50 to +50	0.0	
channel-power-max-delta (0.1 dBm)	Maximum difference among measured channel powers.	Amplifier	0-200	3.0	
ampli-channel-power (0.1 dBm)	Amplifier per-channel power set point.	Amplifier	-400 to +300	0.0	
osri	Optical safety remote interlock.	Amplifier	on, off	off	When OSRI is enabled, the laser is deactivated. When OSRI is disabled, the laser is activated.
safety-control-mode	Safety control mode.	Amplifier	auto, disabled	auto	When safety control mode is disabled, amplifier optical power is less than 20 dB for safety.

Configure an OTS controller

Use this procedure to configure OTS controller optical parameters, including thresholds, VOA attenuation, amplifier gain, amplifier tilt, channel power, OSRI, and safety control mode.

Configure OTS controller parameters when the optical interface hardware supports the required capability.

Use the controller identifier in *Rack/Slot/Instance/Port* format. For parameter ranges and defaults, see OTS controllers.

Procedure

1. Enter configuration mode.

   configure

2. Use the **controller ots** command to enter the OTS controller configuration mode.

   controller ots *rack/slot/instance/port*

3. Configure the required OTS parameters.

   Use the commands that apply to the hardware capability in this sequence.

   - **rx enable**
   - **rx-low-threshold** *value*
   - **tx enable**
   - **tx-low-threshold** *value*
   - **rx-voa-attenuation** *value*
   - **tx-voa-attenuation** *value*
   - **ampli-control-mode automatic manual**
   - **ampli-gain-range normal extended**
   - **ampli-gain** *value*
   - **ampli-tilt** *value*
   - **ampli-channel-power** *value*
   - **channel-power-max-delta** *value*
   - **osri on off**
   - **safety-control-mode auto disabled**

   Example

   In this sample, the amplifier gain range is set to extended and amplifier gain set point is set to 29.0 dB.

```
configure
  controller ots 0/3/0/0
  ampli-gain-range extended
  ampli-gain 290
  commit
end
```

   In this sample, the safety control mode of the pre-amplifier is set to auto.

```
configure
  controller ots 0/3/0/0
  safety-control-mode auto
  commit
end
```

In this sample, the safety control mode of the booster amplifier is set to disabled.

```
configure
  controller ots 0/3/0/1
  safety-control-mode disabled
  commit
end
```

4. Commit the configuration.

   commit

5. Exit configuration mode.

   end

The OTS controller uses the configured optical parameter values.

Display OTS controller parameters

Use this procedure to display OTS controller configuration parameters, performance monitoring thresholds, alarms, power values, and summary status information for a controller.

The **show controllers** command displays all the configuration parameters, performance monitoring thresholds, and alarms if no optional keyword is provided. If you include the **summary** keyword, the command displays receive and transmit power values and minimal information to understand port status.

Procedure

Display the OTS controller parameters.

show controllers *controller-type rack/slot/instance/port* **summary**

Use * as a wildcard to display all the controllers associated with a slot, such as **show controllers ots 0/1/0/* summary**.

Example

RP/0/RP0/CPU0:ios#**show controllers ots 0/3/0/1**

```
Wed Aug 23 09:08:27.962 UTC

 Controller State: Up

 Transport Admin State: In Service

 Port Type: Line

 Laser State: Off

 Optics Status::


 Alarm Status:
 -------------
 Detected Alarms:
 RX-LOC

 Alarm Statistics:
```

```
 -----------------
 LOW-RX-PWR = 0
 LOW-TX-PWR = 0
 RX-LOS-P = 0
 RX-LOC = 1
 AMPLI-GAIN-DEG-LOW = 0
 AMPLI-GAIN-DEG-HIGH = 0
 AUTO-LASER-SHUT = 0
 AUTO-POW-RED = 89
 AUTO-AMPLI-CTRL-DISABLED = 0
 AUTO-AMPLI-CFG-MISMATCH = 0
 SWITCH-TO-PROTECT = 0
 AUTO-AMPLI-CTRL-RUNNING = 0

 Parameter Statistics:
 --------------------
 TX Power = -40.00 dBm
 RX Power = -40.00 dBm
 Ampli Gain = -1.00 dB
 Ampli Tilt = 0.00
 Total TX Power = -40.00 dBm
 Total RX Power = -40.00 dBm

 Configured Parameters:
 -------------
 Rx Low Threshold = -25.0 dBm
 Tx Low Threshold = -20.0 dBm
 Ampli Gain = 1.00 dB
 Ampli Tilt = 0.00
 Ampli Channel power = 0.00 dBm
 Channel Power Max Delta = 3.00 dBm
 Ampli Control mode = Manual
 Ampli Gain Range = Normal
 Ampli Safety Control mode = auto
 Osri = OFF
```

RP/0/RP0/CPU0:ios#**show controllers ots 0/1/0/1**

```

Controller State: Down

Transport Admin State: In Service

Port Type: Line

Laser State: Apr

Optics Status::


         Alarm Status:
         -------------
         Detected Alarms:
                 AUTO-POW-RED

         Alarm Statistics:
         -----------------
         LOW-RX-PWR = 0
         LOW-TX-PWR = 0
         RX-LOS-P = 0
         RX-LOC = 1
         AMPLI-GAIN-DEG-LOW = 0
```

```
        AMPLI-GAIN-DEG-HIGH = 0
        AUTO-LASER-SHUT = 0
        AUTO-POW-RED = 1
        AUTO-AMPLI-CTRL-DISABLED = 0
        AUTO-AMPLI-CFG-MISMATCH = 0
        SWITCH-TO-PROTECT = 0
        AUTO-AMPLI-CTRL-RUNNING = 0

        Parameter Statistics:
        ---------------------
        TX Power = -40.00 dBm
        RX Power = -11.90 dBm
        Ampli Gain = -1.00 dB
        Ampli Tilt = -90.00
        Total TX Power = 7.99 dBm
        Total RX Power = -11.90 dBm
        Ampli Gain Range = Normal
        Ampli Safety Control mode = disabled
        Osri = OFF
        TX Enable = Enabled
        RX Enable = Enabled
        RX Span Loss = N/A
        TX Span Loss = N/A
        Rx Low Threshold Current = -25.0 dBm
        Back Reflection = -6.40 dBm

        Configured Parameters:
        ----------
        Rx Low Threshold = -25.0 dBm
        Tx Low Threshold = -20.0 dBm
        Ampli Gain = 12.00 dB
        Ampli Tilt = 0.00
        Ampli Channel power = 0.00 dBm
        Channel Power Max Delta = 3.00 dBm
        Ampli Channel Psd = 31.250 nW/MHz
        Rx Low Threshold Psd = 0.099 nW/MHz
        Ampli Control mode = Manual
        Ampli Safety Control mode = disabled
        Osri = OFF
        TX Enable = Enabled
        RX Enable = Enabled
```

The Back Reflection parameter, in 0.1 dBm, is raised only on port 1. This parameter is raised on the line TX port of the booster amplifier.

The command output shows OTS controller state, alarms, statistics, and configured parameter values.

Span loss calculation

This topic explains how span loss calculation uses EDFA transmit and receive power values to calculate span losses between NCS 1001 systems.

Span loss calculation is an automatic software function that

- calculates span losses between NCS 1001 systems,
- uses transmit and receive total power on EDFA ports, and
- supports protected or nonprotected linear topologies, with or without intermediate inline amplifier (ILA) nodes.

The feature is available for the OTS controller and can be enabled or disabled through the **hw-module** configuration. The calculation runs automatically every five minutes and when there is a configuration change.

Calculation methods and parameters

Span loss calculation first uses remote node configuration and, if unavailable, uses OSC through OSPF.

The **show controllers ots** command displays these span loss parameters for EDFA cards:

- RX Span Loss
- TX Span Loss

Limitation

Span loss calculation considers total power at the transmit end and receive end on EDFA ports. If the PSM card is connected to the span, such as in a path-protection topology, the span boundaries are assumed to be the closer EDFA ports.

Configure span loss calculation

Use this procedure as the parent workflow for enabling span loss calculation, assigning node type, configuring remote nodes, and triggering a calculation.

Configure span loss calculation across the local and remote NCS 1001 systems that participate in the optical span.

Table 5: Feature History

Feature Name	Release Information	Description
IPv6 Support for Span Loss Calculation	Cisco IOS XR Release 7.10.1	You can now perform span loss calculations on IPv6 spans connecting two NCS 1001 nodes. As a result, the advantages of larger address space can be leveraged by configuring IPv6 addresses on the management interfaces used for communication between the two nodes.

Starting with Cisco IOS XR Release 7.10.1, span loss calculation supports IPv6 addresses in addition to IPv4 addresses. The IPv6 addresses must be configured on the management interfaces of IPv6 enabled NCS 1001 nodes.

The feature uses DCN or OSC (OSPF) so NCS systems can exchange power measurements needed to calculate span losses. In both cases, you must enable the feature and specify the node type (TERM or ILA) on each system.

> **Note**
>
> Configure either IPv4 or IPv6, but not both, for span loss calculation.

Span loss calculation with IPv6 is not supported on OSC management interfaces of NCS 1001 nodes. Even with OSPFv3, neighbor discovery returns the IPv4 router ID instead of the IPv6 router ID. This prevents automatic IPv6 address resolution.

Procedure

1. Enable span loss calculation on the TERM node. See Enable span loss calculation on a TERM node.

2. Enable span loss calculation on the ILA node, if the span includes an ILA node. See Enable span loss calculation on an ILA node.
3. Configure the remote node with IPv4 or IPv6 addresses. See Configure a span loss remote node with IPv4 or Configure a span loss remote node with IPv6.
4. Review topology examples for terminal-to-terminal and terminal-to-ILA-to-terminal designs. See Span loss calculation use cases.
5. Wait for 5 minutes for the first automatic calculation or trigger the calculation manually. See Trigger span loss calculation.

Enable span loss calculation on a TERM node

Use this procedure to enable span loss calculation for an EDFA in a TERM node slot and assign the TERM node type.

Procedure

1. Enter configuration mode.

   configure terminal

2. Enable span loss calculation for the EDFA slot.

   hw-module location 0/RP0/CPU0 slot *n* ampli span-loss

3. Assign the TERM node type.

   hw-module location 0/RP0/CPU0 slot *n* ampli node-type TERM

4. Commit the configuration.

   commit

5. Exit the configuration mode.

   end

   Example

```
 #configure terminal
(config)#hw-module location 0/RP0/CPU0 slot 1 ampli span-loss
(config)#hw-module location 0/RP0/CPU0 slot 1 ampli node-type TERM
(config)#commit
(config)#end
```

Enable span loss calculation on an ILA node

Use this procedure to enable span loss calculation for an EDFA in an ILA node slot and assign the ILA node type.

Procedure

1. Enter configuration mode.

   configure terminal

2. Enable span loss calculation for the EDFA slot.

   hw-module location 0/RP0/CPU0 slot *n* ampli span-loss

3. Assign the ILA node type.

   hw-module location 0/RP0/CPU0 slot *n* ampli node-type ILA

4. Commit the configuration.

   commit

5. Exit configuration mode.

   end

   Example

```
 #configure terminal
(config)#hw-module location 0/RP0/CPU0 slot 1 ampli span-loss
(config)#hw-module location 0/RP0/CPU0 slot 1 ampli node-type ILA
(config)#commit
(config)#end
```

Configure a span loss remote node with IPv4

Use this procedure to configure the local IPv4 address, remote IPv4 address, and remote EDFA slot for span loss calculation.

Procedure

---

1. Enter configuration mode.

   configure terminal

2. Configure the local and remote IPv4 span loss endpoints.

   hw-module location 0/RP0/CPU0 slot *n* ampli remote-node local-ipv4 *local-ipv4-address* remote-ipv4 *remote-ipv4-address* remote-slot-id *m*

   where *n* is the slot number (1, 2 or 3) of the local EDFA involved.

   m is the slot number (1, 2 or 3) of the EDFA equipped on the remote node.

   localIPv4-address is the IP address of the local node.

   remoteIPv4-address is the IP address of the remote node.

3. Commit the configuration.

   commit

4. Exit the configuration mode.

   end

   Example

```
#configure terminal
(config)#hw-module location 0/RP0/CPU0 slot 1 ampli remote-node local-ipv4
192.0.2.144 remote-ipv4 192.0.2.146 remote-slot-id 1
```

```
(config)#commit
(config)#end
```

Configure a span loss remote node with IPv6

Use this procedure to configure the local IPv6 address, remote IPv6 address, and remote EDFA slot for span loss calculation.

Use IPv6 only when span loss calculation is not using IPv4 for the same span. IPv6 span loss calculation is not supported on the OSC management interfaces.

Procedure

1. Enter configuration mode.

   configure terminal

2. Configure the local and remote IPv6 span loss endpoints.

   hw-module location 0/RP0/CPU0 slot *n* **ampli remote-node local-ipv6** *local-ipv6-address* **remote-ipv6** *remote-ipv6-address* **remote-slot-id** *m*

   where *n* is the slot number (1, 2 or 3) of the local EDFA involved.

   m is the slot number (1, 2 or 3) of the EDFA equipped on the remote node.

   localIPv6-address is the IP address of the local node.

   remoteIPv6-address is the IP address of the remote node.

3. Commit the configuration.

   commit

4. Exit the configuration mode.

   end

   Example

```
#configure terminal
(config)#hw-module location 0/RP0/CPU0 slot 1 ampli remote-node local-ipv6
2001:DB8:4491:2000::229:144 remote-ipv6 2001:DB8:4491:2000::229:146
remote-slot-id 1
(config)#commit
(config)#end
```

Trigger span loss calculation

Use this procedure to manually trigger span loss calculation instead of waiting for the first automatic calculation cycle on the selected slot.

The system automatically triggers the first calculation after at least 5 minutes.

Procedure

Trigger span loss calculation for the specified slot.

hw-module slot *n* span-loss calculation

The system starts a span loss calculation for the specified slot.

Span loss calculation use cases

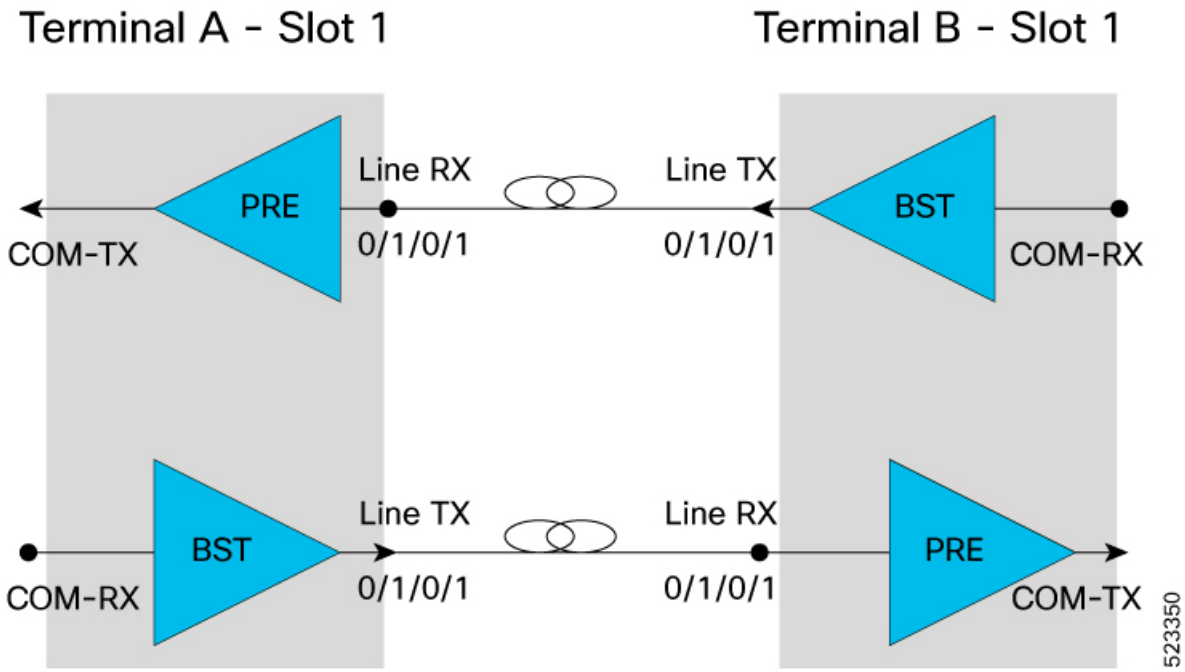
This topic provides terminal-to-terminal and terminal-to-ILA-to-terminal examples for configuring span loss calculation with either IPv4 or IPv6 addresses on spans.

Use these examples to identify how local node, remote node, and remote slot values change by topology.

Terminal-to-terminal use case

Terminal node A (IP address: 192.0.2.144(IPv4) or 2001:DB8:4491:2000::229:144(IPv6)) with a EDFA in slot number 1 connected to the EDFA in slot number 1 of Terminal node B (IP address: 192.0.2.146(IPv4) or 2001:DB8:4491:2000::229:146(IPv6)).

Figure 1: Terminal-to-terminal span loss topology



For each EDFA module, it is necessary to configure remote node feature and the span loss using these CLI commands:

Terminal A configurations using IPv4 and IPv6:

```
#configure terminal (IPv4)
(config)# hw-module location 0/RP0/CPU0 slot 1 ampli remote-node local-ipv4
192.0.2.144  remote-ipv4 192.0.2.146 remote-slot-id 1
config)#hw-module location 0/RP0/CPU0 slot 1 ampli span-loss
```

```
(config)#commit
(config)#end
```

```
#configure terminal (IPv6)
config)# hw-module location 0/RP0/CPU0 slot 1 ampli remote-node local-ipv6
2001:DB8:4491:2000::229:144  remote-ipv6 2001:DB8:4491:2000::229:146
remote-slot-id 1
config)#hw-module location 0/RP0/CPU0 slot 1 ampli span-loss
(config)#commit
(config)#end
```

Terminal B Configurations using IPv4 and IPv6:

```
#configure terminal (IPv4)
(config)# hw-module location 0/RP0/CPU0 slot 1 ampli remote-node local-ipv4
192.0.2.146 remote-ipv4 192.0.2.144 remote-slot-id 1
config)#hw-module location 0/RP0/CPU0 slot 1 ampli span-loss
(config)#commit
(config)#end
```

```
#configure terminal (IPv6)
(config)# hw-module location 0/RP0/CPU0 slot 1 ampli remote-node local-ipv6
2001:DB8:4491:2000::229:146  remote-ipv6 2001:DB8:4491:2000::229:144
remote-slot-id 1
config)#hw-module location 0/RP0/CPU0 slot 1 ampli span-loss
(config)#commit
(config)#end
```

Terminal-to-ILA-to-terminal use case

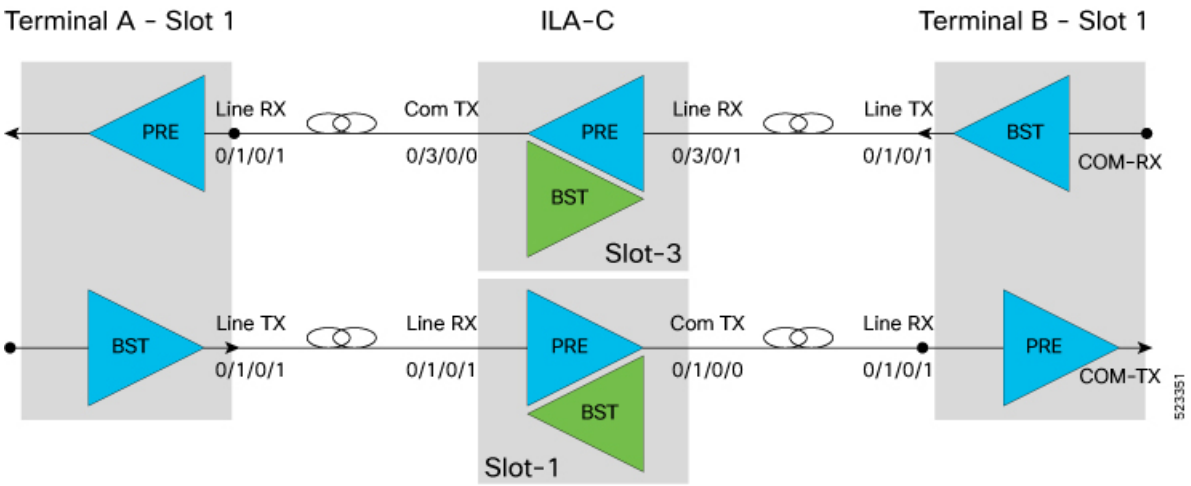
Terminal A (IP address: 192.0.2.144(IPv4) or 2001:DB8:4491:2000::229:144(IPv6)) with a EDFA in slot number 1 with COM-TX port connected to LINE-RX EDFA in slot 1 ILA-C (IP address: 192.0.2.145(IPv4) or 2001:DB8:4491:2000::229:145(IPv6))

ILA C with a EDFA in slot number 1 with COM-TX port connected to LINE-RX EDFA in slot 1 of Terminal B (IP address: 192.0.2.146 (IPv4) or 2001:DB8:4491:2000::229:146)

ILA C with a EDFA in slot number 3 with COM-TX port connected to LINE-RX EDFA in slot 1 Terminal A

Terminal B with a EDFA in slot number 1 with COM-TX port connected to LINE-RX EDFA in slot 3 ILA.

Figure 2: Terminal-to-ILA-to-terminal span loss topology



Terminal A Configuration using IPv4 and IPv6:

```
#configure terminal (IPv4)
(config)# hw-module location 0/RP0/CPU0 slot 1 ampli remote-node local-ipv4
192.0.2.144 remote-ipv4 192.0.2.145 remote-slot-id 1
config)#hw-module location 0/RP0/CPU0 slot 1 ampli span-loss
(config)#commit
(config)#end
```

```
#configure terminal (IPv6)
(config)# hw-module location 0/RP0/CPU0 slot 1 ampli remote-node local-ipv6
2001:DB8:4491:2000::229:144  remote-ipv6 2001:DB8:4491:2000::229:145
remote-slot-id 1
config)#hw-module location 0/RP0/CPU0 slot 1 ampli span-loss
(config)#commit
(config)#end
```

ILA Configuration using IPv4 and IPv6:

```
#configure terminal (IPv4)
(config)# hw-module location 0/RP0/CPU0 slot 1 ampli remote-node local-ipv4
192.0.2.145 remote-ipv4 192.0.2.146 remote-slot-id 1
config)#hw-module location 0/RP0/CPU0 slot 1 ampli span-loss
(config)#commit
(config)#end
```

```
#configure terminal (IPv6)
(config)# hw-module location 0/RP0/CPU0 slot 1 ampli remote-node local-ipv6
2001:DB8:4491:2000::229:145  remote-ipv6 2001:DB8:4491:2000::229:146
remote-slot-id 1
config)#hw-module location 0/RP0/CPU0 slot 1 ampli span-loss
(config)#commit
(config)#end
```

```
#configure terminal (IPv4)
(config)# hw-module location 0/RP0/CPU0 slot 3 ampli remote-node local-ipv4
192.0.2.145 remote-ipv4 192.0.2.144 remote-slot-id 1
config)#hw-module location 0/RP0/CPU0 slot 1 ampli span-loss
(config)#commit
(config)#end
```

```
#configure terminal (IPv6)
(config)# hw-module location 0/RP0/CPU0 slot 3 ampli remote-node local-ipv6
2001:DB8:4491:2000::229:145  remote-ipv6 2001:DB8:4491:2000::229:144
remote-slot-id 1
config)#hw-module location 0/RP0/CPU0 slot 1 ampli span-loss
(config)#commit
(config)#end
```

Terminal B Configuration using IPv4 and IPv6:

```
#configure terminal (IPv4)
(config)# hw-module location 0/RP0/CPU0 slot 1 ampli remote-node local-ipv4
192.0.2.146 remote-ipv4 192.0.2.145 remote-slot-id 3
config)#hw-module location 0/RP0/CPU0 slot 1 ampli span-loss
```

```
(config)#commit
(config)#end
```

```
#configure terminal (IPv6)
(config)# hw-module location 0/RP0/CPU0 slot 3 ampli remote-node local-ipv6
2001:DB8:4491:2000::229:146  remote-ipv6 2001:DB8:4491:2000::229:145
remote-slot-id 3
config)#hw-module location 0/RP0/CPU0 slot 3 ampli span-loss
(config)#commit
(config)#end
```

Display span loss calculation

Use this procedure to display calculated RX span loss and TX span loss values for TERM and ILA node spans.

After the feature is enabled and the first calculation runs, the **show controllers ots** command displays RX Span Loss and TX Span Loss. These values are calculated from the difference between TX Total Power and RX Total Power at the span edge.

Procedure

1. Display span loss for a TERM node line port.

   Example

   ```
   #show controllers ots 0/1/0/1
   RX Span Loss = 15.20 dB
   TX Span Loss = 14.80 dB
   ```

2. For an ILA node, display RX Span Loss on the line port and TX Span Loss on the COM port.

   Example

   ```
   #show controllers ots 0/3/0/1
   RX Span Loss = 12.40 dB
   #show controllers ots 0/3/0/0
   TX Span Loss = 11.90 dB
   ```

Dual IP addresses

This topic explains dual independent XR management interfaces and the requirements for RJ45 and optical SFP management connectivity on NCS systems.

Dual independent XR interfaces are management Ethernet interfaces that

- connect two Ethernet interfaces to different switches in different or same subnets,
- use separate MGMT RJ45 and optical SFP MGMT ports to the CPU from Release 6.5.1, and
- support management connectivity through **MgmtEth0/RP0/CPU0/0** and **MgmtEth0/RP0/CPU0/1**.

Management Ethernet interfaces

- **MgmtEth0/RP0/CPU0/0** represents the RJ45 port.
- **MgmtEth0/RP0/CPU0/1** represents the SFP port.

iPXE is not supported at power-on over the new optical interface. If you upgraded from a previous release and used only SFP, management connectivity may be lost. In this case, configure the system through the console port. Before using both interfaces, upgrade the BIOS and reload the **0/RP0** location.

```
RP/0/RP0/CPU0:router#show running-config
interface MgmtEth0/RP0/CPU0/0
 ipv4 address 192.0.2.10 255.255.255.0
!
interface MgmtEth0/RP0/CPU0/1
 ipv6 address 2001:DB8:0:1::10/64
 ipv6 enable
!
interface MgmtEth0/RP0/OSC1/0
 shutdown
```

OTS OCH controllers

This topic explains OTS OCH controllers, channel granularity, wavelength information, and the low-power threshold parameters available on OCM hardware interfaces.

An Optical Transport Section Optical Channel (OTS OCH) controller is a channel-level controller that

- represents the optical channel monitor (OCM) device on an OTS optical interface,
- provides channel granularity over the OTS interface, and
- stores wavelength information with controller numbers that start at 1 and match ITU channel identifiers.

The system creates 48 OTS OCH controllers for a 100 GHz grid and 96 OTS OCH controllers for a 50 GHz grid.

Configuration parameters for OTS OCH controllers
Table 6: Configuration parameters for OTS OCH controllers

Parameter	Description	Hardware capability	Range	Default
rx-low-threshold (0.1 dBm)	Low receive power threshold.	OCM	-500 to +300	-25.0
tx-low-threshold (0.1 dBm)	Low transmit power threshold.	OCM	-500 to +300	-25.0

Configure an OTS OCH controller

Use this procedure to configure receive and transmit low-power thresholds on an OTS OCH controller for optical channel monitoring and operation.

Use the controller identifier for the OTS OCH controller that you want to configure.

Procedure

1. Enter configuration mode.

   configure

2. Use the **controller ots-och** command to enter OTS OCH controller configuration mode.

   controller ots-och *rack/slot/instance/port*

3. Configure the low-power thresholds.

   rx-low-threshold *value*

   tx-low-threshold *value*

4. Commit the configuration.

   commit

5. Exit the configuration mode.

   end

Example

```
configure
  controller ots-och 0/1/0/0
  rx-low-threshold -30
  tx-low-threshold -35
  commit
end
```

Display OTS OCH controller parameters

Use this procedure to display OTS OCH controller configuration parameters, thresholds, alarms, power values, wavelength information, and summary status for channels.

The **show controllers** command displays all the configuration parameters, performance monitoring thresholds, and alarms if no optional keyword is provided. If you include the **summary** keyword, the command displays RX and TX power values and wavelength details.

Procedure

Display OTS OCH controller parameters.

show controllers *controller-type rack/slot/instance/port/channel-number* **summary**

Use ***** as a wildcard to display all OTS OCH controllers associated with an OTS controller, such as **show controllers ots-och 0/1/0/* summary**.

Example

```
Fri Feb 24 13:20:18.456 CET
```

```
 Controller State: Up

 Transport Admin State: Maintenance

 Port Type: Line

 Laser State: Unnown

 Optics Status::


         Alarm Status:
         -------------
         Detected Alarms:None


         Alarm Statistics:
         -----------------
          LOW-RX-PWR = 0
          LOW-TX-PWR = 0


         Parameter Statistics:
         ---------------------
         TX Power = -3.30 dBm
         RX Power = -21.10 dBm
         TX psd = 13.586 nW/MHz
         RX psd = 0.220 nW/MHz
         Channel Central Frequency = 196100.0 GHz
         Channel Width = 50.0 GHz

         Configured Parameters:
         -------------
         Rx Low Threshold = -25.0 dBm
         Tx Low Threshold = -25.0 dBm
```

RP/0/RP0/CPU0:ios#**show controllers ots-och 0/2/0/0/* summary**

```
Fri Oct  9 10:37:50.109 CEST

 Port               Type    Status       TX Power     RX Power      TX psd
     RX psd    Central Frequency Channel Width
                                              (dBm)        (dBm)      nW/MHz)
    (nW/MHz)        (GHz)              (GHz)
 ------------------  ----    -------      ---------    ---------     ---------
     -------     ---------------   -------------
  Ots-Och0_2_0_0_1    Com      N/A      -18.30        -19.30         0.392
      0.333        196100.0          75.0
  Ots-Och0_2_0_0_2    Com      N/A      -19.10        -19.80         0.094
      0.068        196025.0          75.0
  Ots-Och0_2_0_0_3    Com      N/A      -18.00        -18.90         0.450
      0.392        195950.0          75.0
  Ots-Och0_2_0_0_4    Com      N/A      -16.90        -17.60         0.318
      0.290        195875.0          75.0
  Ots-Och0_2_0_0_5    Com      N/A      -18.10        -19.20         0.326
      0.290        195800.0          75.0
  Ots-Och0_2_0_0_6    Com      N/A      -19.50        -19.90         0.059
      0.041        195725.0          75.0
  Ots-Och0_2_0_0_7    Com      N/A      -18.60        -19.00         0.471
      0.450        195650.0          75.0
  Ots-Och0_2_0_0_8    Com      N/A      -17.00        -17.60         0.304
```

```
     0.318         195575.0          75.0
 Ots-Och0_2_0_0_9    Com      N/A      -18.50        -19.20         0.318
     0.297         195500.0          75.0
Ots-Och0_2_0_0_10    Com      N/A      -17.60        -18.00         0.318
     0.297         195425.0          75.0
Ots-Och0_2_0_0_11    Com      N/A      -18.50        -19.00         0.401
     0.374         195350.0          75.0
Ots-Och0_2_0_0_12    Com      N/A      -17.70        -18.00         0.188
     0.253         195275.0          75.0
Ots-Och0_2_0_0_13    Com      N/A      -18.90        -19.70         0.304
     0.271         195200.0          75.0
Ots-Och0_2_0_0_14    Com      N/A      -20.50        -20.90         0.242
     0.236         195125.0          75.0
Ots-Och0_2_0_0_15    Com      N/A      -24.00        -27.40         0.031
     0.011         195050.0          75.0
Ots-Och0_2_0_0_16    Com      N/A      -17.80        -18.40         0.215
     0.242         194975.0          75.0
Ots-Och0_2_0_0_17    Com      N/A      -18.50        -19.10         0.318
     0.290         194900.0          75.0
Ots-Och0_2_0_0_18    Com      N/A      -16.90        -17.30         0.333
     0.297         194825.0          75.0
Ots-Och0_2_0_0_19    Com      N/A      -18.10        -18.90         0.410
     0.366         194750.0          75.0
Ots-Och0_2_0_0_20    Com      N/A      -17.00        -17.50         0.357
     0.366         194675.0          75.0
Ots-Och0_2_0_0_21    Com      N/A      -18.50        -19.30         0.326
     0.290         194600.0          75.0
Ots-Och0_2_0_0_22    Com      N/A      -17.20        -17.70         0.259
     0.265         194525.0          75.0
Ots-Och0_2_0_0_23    Com      N/A      -18.40        -19.10         0.410
     0.392         194450.0          75.0
Ots-Och0_2_0_0_24    Com      N/A      -16.50        -16.90         0.450
     0.430         194375.0          75.0
Ots-Och0_2_0_0_25    Com      N/A      -24.30        -28.90         0.040
     0.000         194300.0          75.0
Ots-Och0_2_0_0_26    Com      N/A      -16.60        -16.90         0.326
     0.297         194225.0          75.0
Ots-Och0_2_0_0_27    Com      N/A      -18.10        -18.70         0.420
     0.410         194150.0          75.0
Ots-Och0_2_0_0_28    Com      N/A      -16.80        -16.90         0.383
     0.392         194075.0          75.0
Ots-Och0_2_0_0_29    Com      N/A      -19.10        -19.80         0.333
     0.311         194000.0          75.0
Ots-Och0_2_0_0_30    Com      N/A      -16.90        -17.10         0.284
     0.311         193925.0          75.0
Ots-Och0_2_0_0_31    Com      N/A      -18.70        -19.20         0.374
     0.383         193850.0          75.0
Ots-Och0_2_0_0_32    Com      N/A      -17.20        -17.40         0.374
     0.392         193775.0          75.0
Ots-Och0_2_0_0_33    Com      N/A      -18.60        -19.10         0.410
     0.410         193700.0          75.0
Ots-Och0_2_0_0_34    Com      N/A      -17.30        -17.60         0.311
     0.311         193625.0          75.0
Ots-Och0_2_0_0_35    Com      N/A      -18.90        -19.10         0.392
     0.401         193550.0          75.0
Ots-Och0_2_0_0_36    Com      N/A      -18.00        -18.20         0.265
     0.265         193475.0          75.0
Ots-Och0_2_0_0_37    Com      N/A      -19.50        -20.00         0.304
     0.318         193400.0          75.0
Ots-Och0_2_0_0_38    Com      N/A      -17.80        -17.90         0.265
     0.311         193325.0          75.0
Ots-Och0_2_0_0_39    Com      N/A      -18.60        -19.00         0.383
```

```
     0.392         193250.0          75.0
Ots-Och0_2_0_0_40    Com      N/A      -16.80        -17.00         0.383
     0.392         193175.0          75.0
Ots-Och0_2_0_0_41    Com      N/A      -18.70        -19.10         0.440
     0.450         193100.0          75.0
Ots-Och0_2_0_0_42    Com      N/A      -16.80        -17.10         0.374
     0.349         193025.0          75.0
Ots-Och0_2_0_0_43    Com      N/A      -18.90        -19.40         0.401
     0.420         192950.0          75.0
Ots-Och0_2_0_0_44    Com      N/A      -17.00        -17.40         0.450
     0.440         192875.0          75.0
Ots-Och0_2_0_0_45    Com      N/A      -18.50        -18.80         0.392
     0.392         192800.0          75.0
Ots-Och0_2_0_0_46    Com      N/A      -17.40        -17.60         0.284
     0.271         192725.0          75.0
Ots-Och0_2_0_0_47    Com      N/A      -24.40        -31.50         0.064
     0.000         192650.0          75.0
Ots-Och0_2_0_0_48    Com      N/A      -19.20        -19.60         0.410
     0.430         192575.0          75.0
Ots-Och0_2_0_0_49    Com      N/A      -18.70        -19.40         0.392
     0.383         192500.0          75.0
Ots-Och0_2_0_0_50    Com      N/A      -17.10        -17.60         0.374
     0.326         192425.0          75.0
Ots-Och0_2_0_0_51    Com      N/A      -19.10        -19.50         0.401
     0.401         192350.0          75.0
Ots-Och0_2_0_0_52    Com      N/A      -20.40        -20.50         0.357
     0.311         192275.0          75.0
Ots-Och0_2_0_0_53    Com      N/A      -24.70        -34.20         0.042
     0.000         192200.0          75.0
Ots-Och0_2_0_0_54    Com      N/A      -17.60        -18.10         0.201
     0.236         192125.0          75.0
Ots-Och0_2_0_0_55    Com      N/A      -18.50        -19.10         0.401
     0.392         192050.0          75.0
Ots-Och0_2_0_0_56    Com      N/A      -17.20        -17.80         0.341
     0.284         191975.0          75.0
Ots-Och0_2_0_0_57    Com      N/A      -25.60        -30.40         0.050
     0.000         191900.0          75.0
Ots-Och0_2_0_0_58    Com      N/A      -17.40        -17.90         0.220
     0.188         191825.0          75.0
Ots-Och0_2_0_0_59    Com      N/A      -19.40        -20.40         0.333
     0.290         191750.0          75.0
Ots-Och0_2_0_0_60    Com      N/A      -27.10        -38.90         0.023
     0.000         191675.0          75.0
Ots-Och0_2_0_0_61    Com      N/A      -26.00        -38.90         0.031
     0.000         191600.0          75.0
Ots-Och0_2_0_0_62    Com      N/A      -19.50        -20.10         0.133
     0.045         191525.0          75.0
Ots-Och0_2_0_0_63    Com      N/A      -19.20        -19.90         0.401
     0.392         191450.0          75.0
Ots-Och0_2_0_0_64    Com      N/A      -17.30        -17.60         0.333
     0.333         191375.0          75.0
```

From Release 7.3.1, the Central Frequency and Channel Width columns include a decimal place.

LLDP over OSC

This topic provides release information and sample neighbor output for LLDP support on optical supervisory channel management interfaces in point-to-point links.

Use LLDP over OSC to gather point-to-point local link discovery information about neighboring devices in the network.

Feature history
Table 7: Feature history

Feature name	Release	Description
LLDP over OSC	Cisco IOS XR Release 7.3.1	LLDP is supported on the OSC management interface for point-to-point local link discovery through the OSC channel. It enables you to gather information about neighboring devices in the network.

Neighbor output

The **show lldp neighbors** command displays OSC interface neighbors after LLDP is enabled on an OSC interface.

```
RP/0/RP0/CPU0:MYS-130#show lldp neighbors
Capability codes:
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Device ID  Local Intf             Hold-time  Capability  Port ID
MYS-131    MgmtEth0/RP0/OSC3/1    120        R           MgmtEth0/RP0/OSC1/0
```

3 Configure Optical Modules

Topics:

Configure Optical Amplifier Module and Protection Switching Module and troubleshoot module-related operations.

Clear the card configurations

Use this procedure to clear card-level, OTS controller, and optics controller configurations before you replace a configured optical module with a different module type.

Clear existing card and controller settings before you replace a configured optical module with a different module type in the same slot.

Before installing a new, different type of optical module, clear the configurations of the old module. A Cisco NCS 1001 slot configuration can include card configuration, OTS controller configuration, and optics controller configuration for EDFA cards.

Procedure

1. Clear the configuration in the previous card.

   no hw-module location 0/RP0/CPU0 slot *slot-number*

2. Clear the configuration for each OTS controller.

   no controller ots *rack/slot/instance/port*

3. If the previous card was an EDFA card, clear each optics controller configuration.

   no controller optics *rack/slot/instance/port*

After clearing the old card configuration, the slot is ready for the replacement optical module.

Optical amplifier module

Describes the NCS1K-EDFA optical amplifier module, including preamplifier and booster functions, OSC support, OCM monitoring, front-panel callouts, controller-to-port mappings, and COM-CHECK safety behavior.

The optical amplifier module (NCS1K-EDFA) is an NCS 1001 optical module that provides preamplifier and booster amplification for line-system deployments.

- Preamplifier (LINE-RX to COM-TX): Provides a single preamplifier variant with switchable gain ranges according to link loss.
  - Range 1 provides 0 to 24 dB gain, and tilt control provides 24 to 27 dB gain with uncontrolled tilt.
  - Range 2 provides 20 to 34 dB gain, and tilt control provides 34 to 37 dB gain with uncontrolled tilt.
  - The COM-TX port provides 23 dBm output power.
- Booster amplifier (COM-RX to LINE-TX): Provides true variable gain booster amplification.
  - The booster amplifier supports gain range 1 to 20. Gain range 20 to 25 has uncontrolled tilt.
  - The LINE-TX port provides 23 dBm output power.
- The add or drop OSC channel supports both 1510 nm and 1610 nm wavelengths with a tolerance of +/-10 nm.
- The OCM assesses channel presence, gain regulation, and per-channel power monitoring.

Feature history

Table 8: Feature history

Feature name	Release information	Feature description
Amplifier behavior	Cisco IOS XR Release 7.3.1	Grid mode configuration for the optical amplifier supports 75GHz spaced channels. You can optimize the optical spectrum and granularity using gridless configuration. You can provision channels with arbitrary channel frequencies and channel widths. Up to 96 channels can be configured using gridless configuration. Modified commands include: • hw-module • show controllers

EDFA front view

Figure 3: EDFA front view

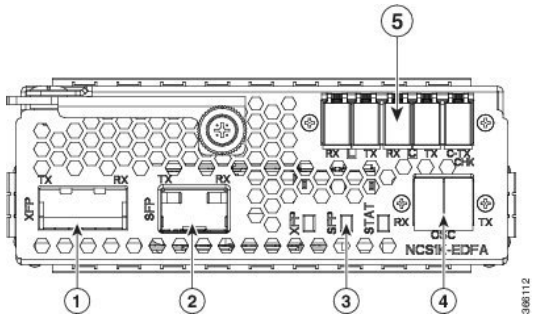


Table 9: EDFA front view callouts

1	XFP for OSC and additional OTDR feature
2	SFP for OSC (Optical Service Channel)
3	Status LED
4	Service channel input and output ports [OSC – RX, TX]
5	PRE and BST amplifier input and output ports [L (LINE) – RX, TX] [C (COM) – RX, TX] [COM – CHECK]

Controller and optical port mappings

This table describes the mapping of controllers and optical ports for the optical amplifier module.

Table 10: Controller and optical port mappings

Controller	Optical ports
Ots 0/slot/0/0	• COM-RX (booster input) • COM-TX (preamplifier output)
Ots 0/slot/0/1	• LINE-RX (preamplifier input) • LINE-TX (booster output)
Ots 0/slot/0/2	• OSC-RX • OSC-TX
Ots 0/slot/0/3	COM-CHECK

COM-CHECK configuration

The COM-CHECK configuration supports safety behavior for high-power preamplifier deployments.

- Safety measures protect the fiber intranode between the preamplifier and the mux or demux section when the total output power on the COM-TX port is up to 23 dB. These measures compensate for extremely long spans.
- If the output power on COM-TX is less than or equal to 20 dB, the COM-CHECK port can be turned off and does not require a physical connection between the pre COM-CHECK and demux monitor port.
- In some cases, such as spans with high power requirements, safety on the preamplifier is necessary.
- The COM-CHECK PD9 is the safety port.
- The COM-RX controller, such as Ots 0/s/0/0, is not part of safety.
- The safety restart process is similar to the booster case, with some difference in the **APR Check** phase.

Amplifier configuration

This topic describes manual and automatic amplifier control methods, UDC port association by slot, and how UDC traffic passes through amplifier OSC add and drop filters.

NCS 1001 supports manual and automatic methods to control optical amplifier settings.

NCS 1001 supports two methods to control amplifiers:

- Manual—the user controls all the amplifier settings.
- Automatic—the internal amplifier power regulator controls all the amplifier settings.

UDC port configuration

UDC port configuration uses these slot associations and traffic-handling rules.

- There are three UDC RJ-45 ports on the faceplate of NCS 1001. UDC1 is associated with slot 1, UDC2 is associated with slot 2, and UDC3 is associated with slot 3.
- UDC ports are Gigabit Ethernet ports that carry any Ethernet traffic.
- UDC traffic is added and dropped through OSC filters in the NCS1K-EDFA optical amplifier module.

- NCS 1001 tags and untags UDC traffic based on the configured UDC VLAN.
- The system supports tagged, multiple-tagged, and untagged traffic.
- Full utilization is not available, because four bytes of tag data are added to each packet.

These diagrams describe the application of UDC that can be used by EPNM to manage NCS 1000 series at the remote site.

Figure 4: UDC application for remote management - scenario one

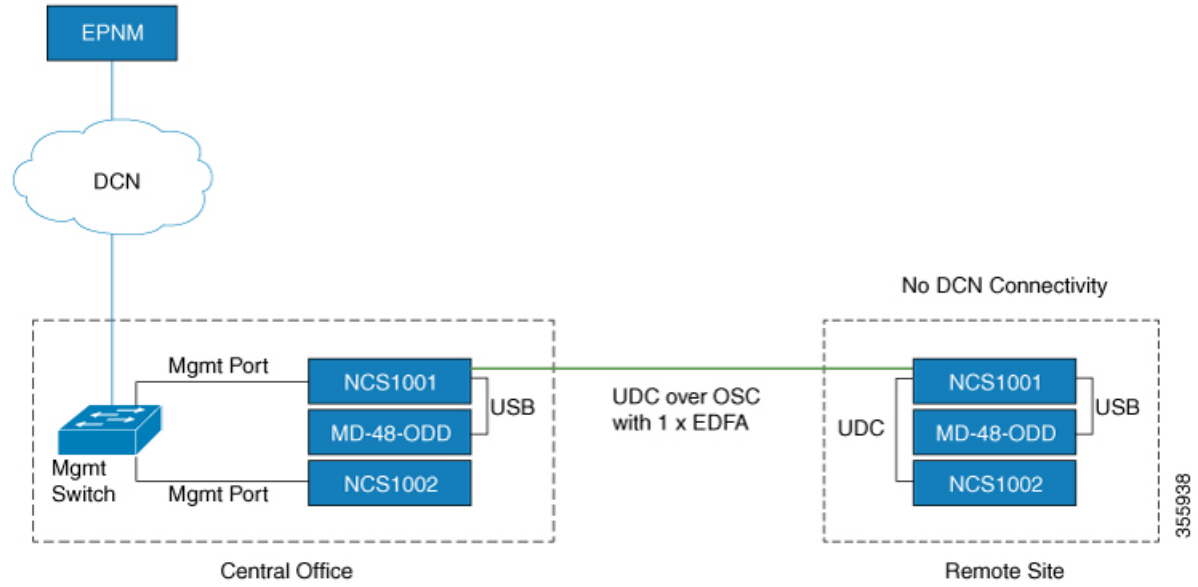
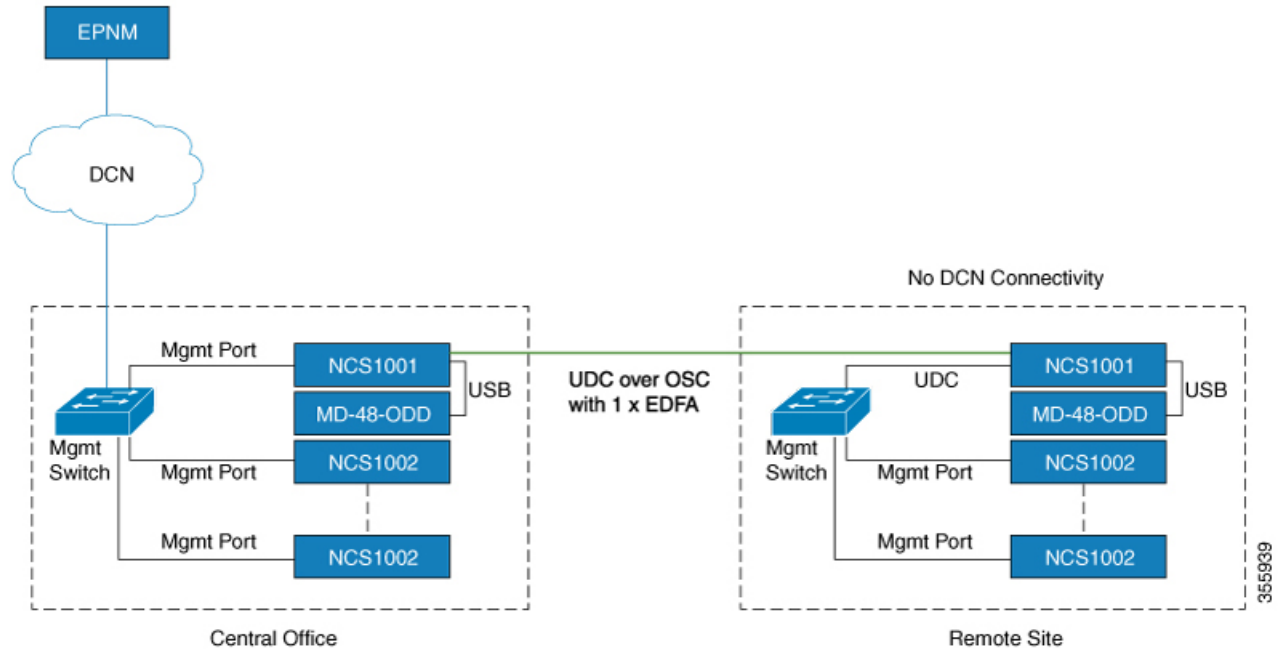


Figure 5: UDC application for remote management - scenario two



Configure an amplifier module

Use this task to complete the required CLI configuration for an amplifier module and confirm that the intended NCS 1001 behavior is available after the changes are committed.

Configure the amplifier module slot, node type, grid mode, and UDC VLAN settings.

For details about amplifier module configuration parameters, see Amplifier module configuration parameters.

Procedure

Use this command to configure the amplifier module.

hw-module location 0/RP0/CPU0 slot *slot-number* **ampli node-type** *value* **grid-mode** *value* **udc-vlan** *value*

Example

In this sample, the amplifier module is inserted in slot 3 and udc-vlan is set to 4000.

```
configure
      hw-module location 0/RP0/CPU0 slot 3 ampli
         [
             grid-mode 100GHz
             udc-vlan 4000
         ]
commit
end
```

The configuration is committed and the optical module uses the requested settings.

Amplifier module configuration parameters

This topic provides information about the amplifier module parameters used to set grid mode, node type, and UDC VLAN values when configuring an NCS 1001 optical amplifier module.

Use this reference to choose values for the amplifier module configuration command.

This table provides information about the supported configuration parameters for the amplifier module.

Table 11: Amplifier module configuration parameters

Parameter	Description	Range or values	Default
grid-mode	Defines the optical spectrum on the interfaces of the amplifier module.	• 100 GHz–Configures the amplifier with 100GHz grid channels and 48-channel spacing. • 50 GHz–Configures the amplifier with 50GHz grid channels and 96-channel spacing. • 75 GHz–Configures the amplifier with 75GHz grid channels and 64-channel spacing. **Note** The NCS1K-MD-64-C optical passive multiplexer and demultiplexer module, introduced in Release 7.3.1, allows you to configure the amplifier with 75GHz grid channels. • gridless–Configures the amplifier in flex spectrum mode.	50GHz
node-type	Defines the type of node in which the amplifier operates.	TERM, ILA	TERM
udc-vlan	Defines the VLAN associated with the selected slot and its UDC port.	2 to 4080	

Configure flex channels on the amplifier module

Use this task to complete the required CLI configuration for flex channels on the amplifier module and confirm that the intended NCS 1001 behavior is available after the changes are committed.

You can optimize the optical spectrum and granularity using the gridless configuration. In gridless configuration, the fixed ITU-T grid that defines specific channel frequencies and channel widths is not considered. You can provision channels with arbitrary channel frequencies and channel widths. You can configure up to 96 channels using the gridless configuration.

Table 12: Flex channel configuration parameters

Parameter	Description	Range
flex-chan-id	Defines the channel identifier.	1 to 96
chan-central-freq	Defines the central frequency of the channel.	191350 to 196100 in multiples of 125

Parameter	Description	Range
chan-width	Defines the width of the channel.	500 (50.0 GHz) to 8000 (800.0 GHz) in multiples of 12.5 GHz

Procedure

1. Use these commands to configure flex channels on the amplifier module.

   Example

```
configure
hw-module location 0/RP0/CPU0 slot 2 ampli flex-mode
hw-module location 0/RP0/CPU0 slot 2 ampli grid-mode gridless
hw-module location 0/RP0/CPU0 slot 2 ampli flex-channel-id 5 chan-central-freq
 1931750 chan-width 6500
commit
end
```

2. Use the **show controllers ots-och summary** command to verify the configured flex channel summary.

   Example

```
show controllers ots-och 0/2/0/0/5 summary
```

3. Use the **show controllers ots-och** command to verify the configured flex channel details.

   Example

```
show controllers ots-och 0/2/0/0/5
```

The configuration is committed and the optical module uses the requested settings.

In this sample, the amplifier module is configured in flex spectrum.

```
configure
      hw-module location 0/RP0/CPU0 slot 2 ampli flex-mode
      hw-module location 0/RP0/CPU0 slot 2 ampli grid-mode gridless
      hw-module location 0/RP0/CPU0 slot 2 ampli flex-channel-id 5
      chan-central-freq 1931750 chan-width 6500
commit
end
```

This sample shows the configured channel with its frequency and width.

RP/0/RP0/CPU0#**show controllers ots-och 0/2/0/0/5 summary**

```
Fri Oct  9 10:43:44.002 CEST
       Port        Type   Status   TX Power   RX Power
                                     (dBm)       (dBm)
      ----------------- -----   -------   ---------  ---------
      Ots-Och0_2_0_0_5    Com     N/A     -8.60       -8.90
```

```
      TX psd     RX psd         Central         Channel Width
      (nW/MHz)   (nW/MHz)       Frequency(GHz)    (GHz)
      ---------  ------------   -------------    --------------
        0.410       0.450         193175.0         650.0
```

RP/0/RP0/CPU0#**show controllers ots-och 0/2/0/0/5**

```
Fri Oct  9 10:46:33.046 CEST

 Controller State: Up

 Transport Admin State: Maintenance

 Port Type: Com

 Laser State: Unknown

 Optics Status::


         Alarm Status:
         -------------
         Detected Alarms: None


         Alarm Statistics:
         -----------------
         LOW-RX-PWR = 0
         LOW-TX-PWR = 0
         RX-LOS-P = 0
         RX-LOC = 0
         AMPLI-GAIN-DEG-LOW = 0
         AMPLI-GAIN-DEG-HIGH = 0
         AUTO-LASER-SHUT = 0
         AUTO-POW-RED = 0
         AUTO-AMPLI-CTRL-DISABLED = 0
         AUTO-AMPLI-CFG-MISMATCH = 0
         SWITCH-TO-PROTECT = 0
         AUTO-AMPLI-CTRL-RUNNING = 0

         Parameter Statistics:
         ---------------------
         TX Power = -8.60 dBm
         RX Power = -8.90 dBm
         TX psd = 0.440 nW/MHz
         RX psd = 0.450 nW/MHz
         Channel Central Frequency = 193175.0 GHz
         Channel Width = 650.0 GHz

         Configured Parameters:
         ----------------------
         Rx Low Threshold = -25.0 dBm
         Tx Low Threshold = -25.0 dBm
```

Modify central frequency and channel width on the amplifier module

Use this task to complete the required CLI configuration for central frequency and channel width on the amplifier module and confirm that the intended NCS 1001 behavior is available after the changes are committed.

You can change the central frequency, channel width, or both for a configured channel ID. The channel ID cannot be arbitrarily changed before unconfiguring the channel.

Procedure

1. Change the central frequency of the configured channel.

   Example

   ```
   hw-module location 0/RP0/CPU0 slot 1 ampli flex-channel-id 24
            chan-central-freq 1949000 chan-width 500
   ```

2. Change the channel width of the same channel.

   Example

   ```
   hw-module location 0/RP0/CPU0 slot 1 ampli flex-channel-id 24
            chan-central-freq 1949000 chan-width 1500
   ```

3. Change both the central frequency and channel width of the channel.

   Example

   ```
   hw-module location 0/RP0/CPU0 slot 1 ampli flex-channel-id 24
            chan-central-freq 1932625 chan-width 6125
   ```

The configuration is committed and the optical module uses the requested settings.

In-line amplifier

This topic describes how in-line amplifier mode uses the pre-amplifier path, disables the booster path, and reports port power values for supported NCS 1001 slots.

The optical amplifier module (NCS1K-EDFA) can be configured in In-line amplifier (ILA) mode. ILA mode is used when it is not possible to connect to terminal nodes with a single span. ILA mode is supported only in slots 1 and 3.

ILA mode supports only the operation of pre-amplifier in both directions. The booster module is switched off in ILA mode. ILA mode supports gain range 1 and 2 of the pre-amplifier and provides 23 dBm output power pre-amplification.

In ILA mode, the LINE-RX and COM-TX ports of the optical amplifier module are enabled, while the LINE-TX and COM-RX ports are disabled. The OCM reports the values for LINE-RX and COM-TX ports, and the values for LINE-TX and COM-RX ports are set to -40.00 dBm. In ILA mode, the LINE-RX port terminates on the optical amplifier module's LINE-RX, and the LINE-TX port terminates on the external OSC module (15216-FLD-OSC=).

Configure an amplifier module in ILA manual mode

Use this task to complete the required CLI configuration for an amplifier module in ILA manual mode and confirm that the intended NCS 1001 behavior is available after the changes are committed.

When the amplifier is set to ILA, all the configurations are performed only on the pre-amplifier. After the node is set to ILA, the amplifier gain, RX-low threshold, and the amplifier tilt can be configured on the pre-amplifier.

Procedure

Use these commands to configure the required settings.

configure hw-module location 0/RP0/CPU0 slot *slot-number* **ampli node-type** *value* **commit end controller** *controllertype Rack/Slot/Instance/Port* **ampli-control-mode {automatic | manual} ampli-gain** *value* **rx-low-threshold** *value* **ampli-tilt** *value* **commit end**

Example

In this sample, the amplifier module is configured in ILA manual mode. The node type is set to ILA. This parameter switches off the booster side and activate safety between slots 1 and 3.

```
configure
            hw-module location 0/RP0/CPU0 slot 3 ampli node-type iLA
            commit
            end
            controller ots 0/3/0/0
            ampli-control-mode manual
            ampli-gain 200
            rx-low-threshold -300
            ampli-tilt -10
            commit
end
```

The configuration is committed and the optical module uses the requested settings.

Configure an amplifier module in ILA automatic mode

Use this task to complete the required CLI configuration for an amplifier module in ILA automatic mode and confirm that the intended NCS 1001 behavior is available after the changes are committed.

The configurations performed on the amplifier module in ILA automatic mode are similar to the configurations performed on the terminal node. The configurations are performed only on the pre-amplifier as the booster is switched off in ILA mode.

Procedure

Use these commands to configure the required settings.

configure hw-module location 0/RP0/CPU0 slot *slot-number* **ampli grid-mode** *value* **node-type** *value* **commit end controller** *controllertype Rack/Slot/Instance/Port* **ampli-control-mode {automatic | manual} ampli-channel-power** *value* **ampli-tilt** *value* **rx-low-threshold** *value* **channel-power-max-delta** *value* **ampli-gain** *value* **ampli-gain-range {normal | extended} commit end**

Example

In this sample, the amplifier module is configured in ILA automatic mode.

```
configure
            hw-module location 0/RP0/CPU0 slot 3 ampli
            grid-mode 50GHz
            node-type iLA
            commit
            end
            controller ots 0/3/0/0
```

```
            ampli-control-mode automatic
            ampli-channel-power 30
            ampli-tilt -10
            rx-low-threshold -331
            ampli-gain 220
            ampli-gain-range extended
            commit
      end
```

This is a sample of **show running-config** command.

```
line console
      exec-timeout 0 0
      !
      line default
      exec-timeout 0 0
      session-timeout 0
      !
      ntp
      server 10.58.228.1
      update-calendar
      !
      hw-module location 0/RP0/CPU0 slot 1
      ampli udc-vlan 11
      ampli grid-mode 50GHz
      ampli node-type ILA
      !
      hw-module location 0/RP0/CPU0 slot 3
      ampli udc-vlan 10
      ampli grid-mode 50GHz
      ampli node-type ILA
      !
      interface MgmtEth0/RP0/CPU0/0
      ipv4 address 10.58.229.143 255.255.252.0
      !
      interface MgmtEth0/RP0/OSC1/0
      shutdown
      !
      interface MgmtEth0/RP0/OSC2/0
      shutdown
      !
      interface MgmtEth0/RP0/OSC3/0
      shutdown
      !
      controller Ots0/1/0/0
      ampli-tilt -12
      ampli-control-mode automatic
      ampli-channel-power 22
      channel-power-max-delta 45
      !
      controller Ots0/1/0/1
      rx-low-threshold -250
      !
      controller Ots0/3/0/0
      ampli-tilt -12
      ampli-control-mode automatic
      ampli-channel-power 22
      channel-power-max-delta 45
      !
      controller Ots0/3/0/1
      rx-low-threshold -250
```

```
      !
      router static
      address-family ipv4 unicast
        0.0.0.0/0 10.58.228.1
      !
      !
      netconf-yang agent
      ssh
      !
      ssh server v2
      end
```

The configuration is committed and the optical module uses the requested settings.

Gridless OCM support

This topic describes gridless OCM support for flexible channel widths, PSD-based amplifier gain calculation, channel-width limitations, and command examples for supported widths.

The Gridless OCM (Optical Channel Monitor) support feature enables transponders to use channel widths between 50 GHz and 100 GHz. In R7.1.1, the channel width can be set between 50 GHz to 800 GHz in increments of 25 GHz. In the gridless mode, the amplifier gain is calculated using the power spectral density parameter and not the per channel power parameter. The flex grid enables support for the 600G interface on NCS 1004

Limitation

The setting of a channel width disables the nearest channels.

Configure the channel width

The channel width can be set from 1000 GHz to 8000 GHz.

This command configures the channel width as 100 GHz. This means that the channels are spaced on eight slices at 12.5 GHz each.

```
hw-module location 0/RP0/CPU0 slot 1 ampli flex-mode
      channel-id 1 channel-width 1000
```

This command configures the channel width as 800 GHz. This means that the channels are spaced on eight slices at 100 GHz each.

```
hw-module location 0/RP0/CPU0 slot 1 ampli flex-mode
      channel-id 10 channel-width 8000
```

Enable automated OTS-OCH thresholds on an amplifier

Use this task to complete the required CLI configuration for automated OTS-OCH thresholds on an amplifier and confirm that the intended NCS 1001 behavior is available after the changes are committed.

You can enable or disable automated OTS-OCH thresholds on each EDFA card installed on the node. This setting applies to the EDFA OTS controllers and all related OTS-OCH controller ports.

Before you begin

This feature works only if the user has configured span loss calculation. See Span loss calculation on page 24.

When the automatic threshold function is enabled on the amplifier, the threshold value to set is determined using this formula:

rx-low-threshold= (Remote AmplChannel - RXSpanloss)-User Threshold Offset.

Where

Remote AmplChannel is the amplifier channel power set on the remote node for ots controller tx port of remote EDFA.

RXSpanloss is the RX Span Loss calculated on the local node.

User Threshold Offset is the ampli-auto-rxlow-threshold threshold-offset set on the local node for EDFA in slot 1.

Modifying any of the parameters in the formula does not automatically recalculate the rx-low threshold value. To update the rx-low threshold value, you must execute this CLI command:

hw-module slot *<n>* **ampli-auto-rxlow-threshold threshold-offset** *<value>*

Example: **hw-module slot 1ampli-auto-rxlow-threshold threshold-offset 400**

These parameters are used to configure the command:

- *<n>* **(1, 2, 3)** : This parameter designates the specific slot where the EDFA card is installed within the device.
- *<value>* **(0-800)**: This parameter specifies the adjustment to the amplifier RX-LOW threshold, given in tenths of dBm.

Procedure

1. Configure the required settings.

   Example

   ```
   hw-module location 0/RP0/CPU0 slot slot number ampli auto-threshold
   ```

2. Use the **show running hw-module** command to verify that automatic thresholds are enabled.

   Example

   ```
   show running hw-module location 0/RP0/CPU0 slot 1 ampli
   ```

The configuration is committed and the optical module uses the requested settings.

This sample enables autothreshold on an EDFA inserted in slot 1.

```
RP/0/RP0/CPU0:MYS-237#configure terminal
RP/0/RP0/CPU0:MYS-237(config)#hw-module location 0/RP0/CPU0 slot 1 ampli
auto-threshold
RP/0/RP0/CPU0:MYS-237(config)#commit
RP/0/RP0/CPU0:MYS-237(config)#end
```

This sample checks whether the auto-threshold is configured.

```
#show running hw-module location 0/RP0/CPU0 slot 1 ampli
      ….
       ampli span-loss
       ampli node-type TERM
       ampli remote-node local-ipv4 10.58.xxx.xxx remote-ipv4 10.58.xxx.xxx
```

```
remote-slot-id 3
       ampli auto-threshold
```

Protection switching module

This topic describes the NCS1K-PSM protection switching module, including TX and RX switching functions, front-panel callouts, protected and working path ports, and controller-to-port mappings.

The protection switching module (NCS1K-PSM) is an NCS 1001 optical module that switches traffic between working and protected optical paths.

- TX section functions include these behaviors:
  - Splits input optical channels to both working and protection lines.
  - Forces the switch at the remote site by opening one of the two line paths. This is achieved by placing the related variable optical attenuator into automatic VOA shutdown.
- RX section functions include these behaviors:
  - Selects signals from the working or protection line, and monitors each line through a photodiode.
  - Balances the two line losses by changing the variable optical attenuator attenuation value when the switch changes state.

PSM front view

Figure 6: PSM front view

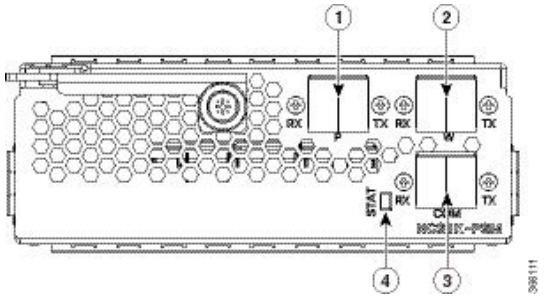


Table 13: PSM front view callouts

1	Protected path input and output port [P - RX, TX]
2	Working path input and output port [W - RX, TX]
3	COM input and output port [COM - RX, TX]
4	Status LED

Controller and optical port mappings

This table describes the mapping of controllers and optical ports for the protection switching module.

Table 14: Controller and optical port mappings

Controller	Optical ports
Ots 0/slot/0/0	COM-TX
Ots 0/slot/0/1	Working path input and output port [W - RX, TX]
Ots 0/slot/0/2	Protected path input and output port [P - RX, TX]

Configure a protection switching module

Use this task to configure PSM protection parameters, such as lockout, path protection, section protection, unidirectional switching, and automatic threshold settings.

Configure the PSM slot with the protection behavior required for the working or protected path.

For details about supported PSM parameters, see PSM module configuration parameters. For details about PSM section and path protection topologies, see PSM section and path protection.

Procedure

1. Enter configuration mode.

   Example

   ```
   configure terminal
   ```

2. Use the **hw-module location** command to configure the required PSM parameter on the selected slot.

   Example

   ```
   hw-module location 0/RP0/CPU0 slot 2 psm lockout-from "working"
   ```

3. Commit the configuration.

   Example

   ```
   commit
   ```

The PSM configuration is committed for the selected slot.

What to do next

For details about manual switching, see Switch a PSM path manually. For details about manual threshold values, see PSM manual threshold guidelines.

PSM module configuration parameters

This topic provides information about the PSM configuration parameters used to control lockout behavior, path and section protection, unidirectional switching, and automatic threshold settings.

Use this reference to choose the PSM parameter for the required protection switching behavior.

This table provides information about the PSM configuration parameters.

Table 15: PSM module configuration parameters

Parameter	Description	Values
lockout-from	Excludes the selected port from protection. Triggers a switch when the active port is specified in the lockout. For example, configuring lockout-from working triggers a switch to protect when the working port is active. Configuring lockout-from protected triggers a switch to working when the protected port is active.	Working, Protected
path-protection	Enables PSM path protection.	
section-protection	Enables PSM section protection.	
uni-dir	Enables PSM unidirectional switching.	
auto-threshold	Enables the PSM automatic threshold setting.	

Switch a PSM path manually

Use this task to manually switch a PSM path to the working or protected path when operational conditions require user-controlled switching.

Apply a manual switch command to move traffic to the working or protected PSM path.

A user-command switch from the path without the ILA node is bidirectional. If the ILA and terminal nodes are in section protection, manual and lockout switch commands from the path with the ILA node are unidirectional.

Note

An FPD upgrade on FW_PSMv1 from FW 1.43 and FW 1.44 to FW 1.45 affects traffic.

Procedure

Use the **hw-module** command to switch the selected PSM slot to the working or protected path.

hw-module slot *slot-number* **manual-switch-to working | protected**

The selected PSM slot switches traffic to the requested path.

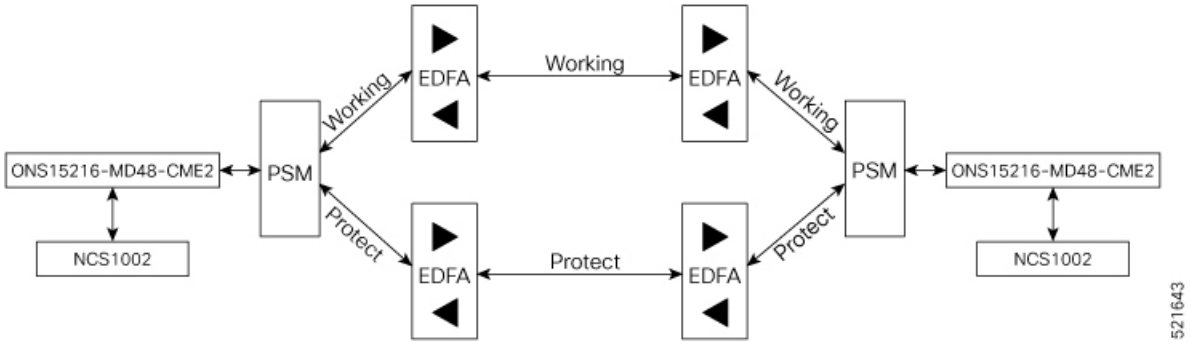
PSM section and path protection

This topic describes how PSM section protection and path protection use PSM parameters, slot placement, EDFA connections, topology diagrams, and topology-specific switching behavior.

PSM section and path protection are protection schemes that use PSM parameters on paired modules to control working and protected optical paths.

Section protection topology

Figure 7: Section protection topology

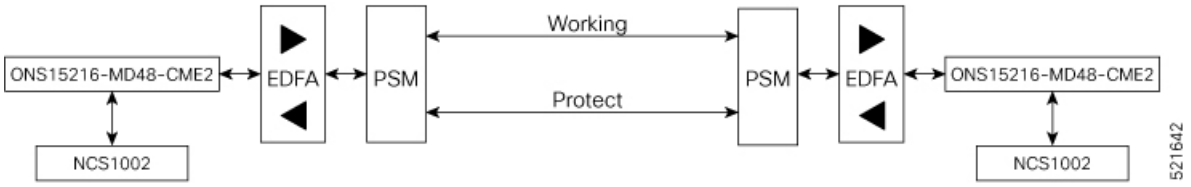


Section protection topology is available from Release 6.2.1. You can set the section protection parameter on both PSMs. Insert the PSM in slot 2 for a section protection topology. Connect the EDFA in slot 1 to the protected port on the PSM. Connect the EDFA in slot 3 to the working port of the PSM.

> **Note**
>
> To measure the correct switching time when testing section protection, wait 120 seconds between any two switching events or between a switching event and restoration. This waiting period allows the EDFAs to stabilize after the first switch. It also prevents power at the PSM from oscillating around the threshold.

Path protection topology

Figure 8: Path protection topology



Path protection topology is available from Release 6.3.2. You can set the path protection parameter on both the PSMs.

PSM manual threshold guidelines

This topic lists the threshold values, recommendations, known issues, and related controller considerations for PSM path protection with manually configured RX-low thresholds.

Use this reference to choose manual RX-low threshold values for PSM path protection and three-way topology deployments.

The switch operates in all conditions when autothreshold is enabled. When path protection is configured with a manual threshold, use these guidelines:

- During the first installation, set the PSM RX-low threshold three dB less than the minimum power for a single channel. The value must allow the PSM to switch on with a single channel or when the EDFA is in APR (+8 dBm).
- When the system is running with the final number of channels, set the PSM RX-low threshold three dB less than the target power.

- After a fiber cut and restore, set the PSM RX-low threshold to a value similar to the value used during the first installation so the PSM can switch on.

PSM autothreshold configuration is highly recommended for a three-way topology.

In a three-way topology, incorrect manual threshold configuration can cause these issues:

- The switch may not be bidirectional.
- A double switch can occur on PSM path protection when it is set in three-way configuration.

You can configure parameters such as **rx-enable** and **tx-enable** in OTS controllers 1 or 2. These controllers represent the working or protected port of the PSM card.

For details about OTS controllers, see Configure an OTS controller on page 20.

PSM autothreshold behavior

This topic describes how PSM autothreshold calculates RX-low threshold values, handles stable and unstable received power, and restores configured values during LOS-P alarm conditions.

Use this reference to understand how PSM autothreshold changes current RX-low thresholds for working and protected RX ports.

PSM threshold behavior depends on whether autothreshold is enabled.

- When autothreshold is not enabled, the active RX-low threshold value on PSM working and protected RX ports is either the value configured by the user or the default value.
- The current threshold equals the configured value if the configured values are available in the show controller command output.
- The current threshold is -38 dBm when the user has not configured a value for the threshold parameters.

When autothreshold is enabled on the PSM card, the RX-low threshold values configured by the user for ports 1 and 2 are ignored.

- If optical power at the Working-RX and Protected-RX ports remains within ±1 dB for two minutes, the related RX-low threshold automatically becomes the RX power minus three dB.
- If power is not stable, the related thresholds do not change.
- W-RX and P-RX thresholds are regulated independently.

LOS-P alarm behavior changes how autothreshold maintains or restores RX-low threshold values.

- When a LOS-P alarm is detected on the working or protected RX port with autothreshold enabled, the related threshold remains the same. This behavior occurs when RX power is less than the related threshold on the working or protected RX port.
- When the LOS-P alarm clears within the first 30 seconds, the autothreshold mechanism applies. After two minutes of stable RX power, the RX-low threshold becomes the new RX power minus three dB.
- When LOS-P is present after 30 seconds, the RX-low threshold automatically moves to the values configured by the user.
- When LOS-P clears, the ordinary autothreshold mechanism is applied again if RX power is higher than the related current threshold.

Configure rx-low threshold for PSM

Use this task to configure the correct rx-low threshold procedure for a PSM working or protected RX port based on manual or automatic amplifier control mode.

Configure the **rx-low-threshold** before you enable auto-threshold on PSM ports.

The PSM auto-threshold feature monitors the W-RX and P-RX ports of the PSM module for actual received power. When the received power is stable, the feature sets the **rx-low-threshold** value of the W-RX and P-RX ports to the current power value. The threshold is then set to three dB lower than the received power. If a loss of signal (LOS) occurs at the W-RX or P-RX ports due to a fiber cut or a temporary power disruption, the feature restores the **rx-low-threshold** value to the configured value.

```
RP/0/RP0/CPU0:ios#show controllers ots 0/2/0/1
      Parameter Statistics:
      ----------------------
               RX Power = -4.00 dBm
               Rx Low Threshold Current = -7.0 dBm   <<< current value
(auto-threshold)

      Configured Parameters:
      ----------------------
               Rx Low Threshold = -38.0 dBm <<< configured value (user
configured)
```

We recommend configuring both the **rx-low-threshold** and **auto-threshold** values of the PSM module according to these guidelines:

Procedure

1. Configure the working rx-low threshold in manual mode. For details about the working rx-low threshold in manual mode, see Configure the working RX-low threshold in manual mode.
2. Configure the protected rx-low threshold in manual mode. For details about the protected rx-low threshold in manual mode, see Configure the protected RX-low threshold in manual mode.
3. Configure the working rx-low threshold in automatic mode. For details about the working rx-low threshold in automatic mode, see Configure the working RX-low threshold in automatic mode.
4. Configure the protected rx-low threshold in automatic mode. For details about the protected rx-low threshold in automatic mode, see Configure the protected RX-low threshold in automatic mode.

The selected PSM port has an RX-low threshold that matches the amplifier control mode and observed power values.

Configure the working rx-low-threshold in manual mode

Use this task to calculate and configure the rx-low threshold for the selected PSM port from the relevant amplifier power value.

Configure the **rx-low-threshold** for the selected PSM port using the value required by the amplifier control mode.

Procedure

1. Use the **show hw-module slot 3 channel-trail-view active** command and identify the required power value.

Example

```
Channel Trail View - Active - dBm
          ========================================
                                                                                BST:
 0/COM=>1/LINE              PRE: 1/LINE=>0/COM
          Och Name       Wavelength(nm)Freq(GHz) Width(GHz)Rx pwr(dBm) Tx
pwr(dBm) Rx pwr(dBm)  Tx pwr(dBm)

_____________________________________________________________________________________

          Ots-Och0_2_0_0_1  1528.77    196100.0    50.0     -6.10       -4.90
       -2.50          6.20
          Ots-Och0_2_0_0_2  1529.16    196050.0    50.0     -5.90       -4.60
       -2.20          6.50
          Ots-Och0_2_0_0_3  1529.55    196000.0    50.0     -6.00       -4.80
       -2.30          6.30
          Ots-Och0_2_0_0_4  1529.94    195950.0    50.0     -6.10       -4.90
       -2.40          6.20
          Ots-Och0_2_0_0_5  1530.33    195900.0    50.0     -6.30       -5.20
       -2.60          6.00
          Ots-Och0_2_0_0_6  1530.72    195850.0    50.0     -6.50       -5.30
       -2.80          5.90
```

Examine the **PRE: 1/LINE=>0/COM** column in the command output and choose the lowest channel **Tx pwr** value from all the active channels.

2. Enter the configuration mode.

Example

```
configure
```

3. Use the **controller ots** command to configure the rx-low threshold value.

Example

```
controller ots 0/2/0/1 rx-low-threshold 49
```

Set the threshold value manually to the lowest channel Tx power minus 1 dBm. In this example, channel Ots-Och0_2_0_0_6 is at the lowest Tx power 5.90 dBm. Therefore, the threshold value on the PSM W/RX port is 5.90 minus 1, which equals 4.90 dBm.

If the system works without any grid mode configuration, the **channel-trail-view** command is not available because channel mapping configuration is not available.

To identify the lowest channel Tx pwr value, use this show command.

show controllers ots0/3/0/0 spectrum-info

```
Tx power :

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

       spectrum-slice num                          Tx-power values (dBm)

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

         1 - 8              -47.20 -47.20 -47.20 -36.40     -47.20 -47.20
-47.20 -47.20
```

```
          9 - 16              -47.20 -47.20 -43.70 -43.70     -47.20 -36.60
-47.20 -43.20
         17 - 24              -47.20 -35.80 -47.20 -47.10     -41.90 -43.20
-42.20 -40.30
         25 - 32              -40.30 -47.20 -41.70 -41.70     -37.50 -47.20
-47.20 -41.90
         33 - 40              -41.90 -47.20 -45.90 -42.10     -42.10 -46.30
-41.60 -39.10
         41 - 48              -41.20 -47.20 -35.80 -45.10     -45.30 -45.30
-40.10 -40.10
         49 - 56              -45.50 -42.60 -45.30 -47.20     -47.20 -40.50
-47.20 -45.80
         57 - 64              -38.60 -40.30 -40.30 -47.20     -47.20 -39.40
-43.10 -43.10
         65 - 72              -42.20 -42.20 -47.20 -47.20     -38.80 -47.20
-47.20 -41.30
         73 - 80              -47.20 -43.00 -40.10 -40.10     -47.20 -36.10
-39.40 -45.70
         81 - 88              -47.20 -41.50 -39.00 -42.50     -47.20 -47.20
-34.30 -47.20
         89 - 96              -47.20 -47.20 -39.90 -39.70     -47.20 -47.20
-47.20 -47.20
         97 - 104             -47.20 -45.10 -39.90 -41.30     -47.20 -39.80
-37.80 -42.00
```

All the slice power values are expressed in PSD (Power Spectral Density) units of measure [dBm/12.5GHz]. Each slice value is converted to linear mW using the formula 10^(N/10). For example, -20 dBm is equal to 0.01 mW(calculated as 10^(-20/10)), and 0 dBm is equal to 1 mW (calculated as 10^0).

Each slice group that composes a channel is algebraically added to obtain the integral channel power. For example, the first channel of 50 GHz occupies the slice range 1 to 4, and the second channel occupies 5 to 8. The first channel of 75 GHz occupies the slice range 1 to 5 and 6 to 11. The first channel of 100 GHz occupies the slice range 1 to 6 and 7 to 14.

Each channel power that falls below the **rx-low-threshold** value is excluded from the list of active channels. The channel that has the least value above the **rx-low-threshold** value is chosen.

Configure the protected rx-low-threshold in manual mode

Use this task to calculate and configure the rx-low-threshold for the selected PSM port from the relevant amplifier power value.

Configure the **rx-low-threshold** for the selected PSM port using the value required by the amplifier control mode.

Procedure

1. Use the **show hw-module slot 1 channel-trail-view active** command and identify the required power value.

   Example

```
Channel Trail View - Active - dBm
          ========================================
                                                                          BST:
 0/COM=>1/LINE              PRE: 1/LINE=>0/COM
          Och Name      Wavelength(nm)Freq(GHz)  Width(GHz)Rx pwr(dBm)  Tx
pwr(dBm)   Rx pwr(dBm)   Tx pwr(dBm)
```

```
--------------------------------------------------------------------------------------------------

          Ots-Och0_2_0_0_1 1528.77    196100.0    50.0      -6.10        -4.90
        -2.50          5.00
          Ots-Och0_2_0_0_2 1529.16    196050.0    50.0      -5.90        -4.60
        -2.20          5.20
          Ots-Och0_2_0_0_3 1529.55    196000.0    50.0      -6.00        -4.80
        -2.30          5.10
          Ots-Och0_2_0_0_4 1529.94    195950.0    50.0      -6.10        -4.90
        -2.40          5.00
          Ots-Och0_2_0_0_5 1530.33    195900.0    50.0      -6.30        -5.20
        -2.60          5.00
          Ots-Och0_2_0_0_6 1530.72    195850.0    50.0      -6.50        -5.30
        -2.80          4.80
```

Examine the **PRE: 1/LINE=>0/COM** column in the command output and choose the lowest channel **Tx pwr** value from all the active channels.

2. Enter configuration mode.

   Example

   ```
   configure
   ```

3. Use the **controller ots** command to configure the RX-low threshold value.

   Example

   ```
   controller ots 0/2/0/2 rx-low-threshold 38
   ```

   Set the threshold value manually to the lowest channel Tx power minus 1 dBm. In this example, channel Ots-Och0_2_0_0_6 is at the lowest Tx power 4.80 dBm. Therefore, the threshold value on the PSM W/RX port is 4.80 minus 1, which equals 3.80 dBm.

Configure the working rx-low-threshold in automatic mode

Use this task to calculate and configure the rx-low-threshold for the selected PSM port from the relevant amplifier power value.

Configure the rx-low-threshold for the selected PSM port using the value required by the amplifier control mode.

Procedure

1. Use the **show controllers ots 0/3/0/0** command and identify the required power value.

   Example

   ```
   Configured Parameters:

            -------------------------
                     Ampli Channel power = 0.00 dBm
   ```

   Examine the **ampli-channel-power Tx** value in the command output.

2. Enter configuration mode.

Example

```
configure
```

3. Use the **controller ots** command to configure the rx-low-threshold value.

Example

```
controller ots 0/2/0/1 rx-low-threshold -10
```

Set the threshold value manually to ampli-channel-power minus 1 dBm. In this example, **ampli-channel-power Tx** value is 0 dBm. Therefore, the threshold value on the PSM W/RX port is 0 minus 1, which equals -1 dBm.

Configure the protected rx-low-threshold in automatic mode

Use this task to calculate and configure the rx-low-threshold for the selected PSM port from the relevant amplifier power value.

Set the **rx-low-threshold** for the selected PSM port using the value required by the amplifier control mode.

Procedure

1. Use the **show controllers ots 0/1/0/0** command and identify the required power value.

Example

```
Configured Parameters:

          -------------------------
                   Ampli Channel power = 2.00 dBm
```

Examine the **ampli-channel-power Tx** value in the command output.

2. Enter configuration mode.

Example

```
configure
```

3. Use the **controller ots** command to configure the rx-low-threshold value.

Example

```
controller ots 0/2/0/2 rx-low-threshold 10
```

Set the threshold value manually to ampli-channel-power minus 1 dBm. In this example, **ampli-channel-power Tx** value is 2 dBm. Therefore, the threshold value on the PSM W/RX port is 2 minus 1, which equals 1 dBm.

Enable autothreshold for PSM

Use this task to complete the required CLI configuration for autothreshold for PSM and confirm that the intended NCS 1001 behavior is available after the changes are committed.

Before you begin

Configure rx-low-threshold for PSM

Procedure

Use the **hw-module location** command to enable autothreshold for PSM.

Example

```
configure
hw-module location 0/RP0/CPU0 slot 1 psm auto-threshold
commit
end
```

The configuration is committed and the optical module uses the requested settings.

Configure a relative switch threshold for PSM

Use this task to complete the required CLI configuration for a relative switch threshold for PSM and confirm that the intended NCS 1001 behavior is available after the changes are committed.

A relative switch threshold lets you configure the delta threshold on PSM that triggers the working path to switch to the protected path. You can configure this threshold only if **auto-threshold** or **revertive wtr** are not configured.

Procedure

Use the **hw-module location** command to configure a relative switch threshold for PSM.

Example

```
configure terminal
hw-module location 0/RP0/CPU0 slot 1 psm relative-switch-threshold 120
relative-switch-threshold-offset -150
commit
end
```

The configuration is committed and the optical module uses the requested settings.

PSM virtual photodiode

This topic describes how the PSM virtual photodiode calculates COM-RX power from available transmit photodiodes and reports fallback values when both related ports are unavailable.

The PSM virtual photodiode provides an optical power reading even when photodiodes are not available. The PSM does not have a photodiode on the COM-RX port. Two photodiodes are present on the Working-TX port and the Protected-TX port, located after the VOA

Details

The power value on COM-RX is real if at least one of the W-TX or P-TX power values is not equal to -40 dB (the related port is in AVS).

If both the power of W-TX and P-TX equal -40 dB (both related VOAs are in AVS-Automatic VOA Shutdown), it is impossible to calculate the real power on the COM-RX port, so the value is displayed as -40 dB.

The feature does not require any configuration. Only the *show controllers ots 0/<slot>/0/0* command is changed to display the RX power on the COM-RX port. The RX low power alarm is not managed on the COM-RX port.

Example for show controller

```
RP/0/RP0/CPU0:ios#show controllers ots 0/2/0/0
Wed Jan 24 14:33:22.898 CET

 Controller State: Up

 Transport Admin State: In Service

 Port Type: Com

 Laser State: Unknown

 Optics Status::


 Alarm Status:
 -------------
 Detected Alarms: None


 Alarm Statistics:
 -----------------
 LOW-RX-PWR = 0
 LOW-TX-PWR = 0
 RX-LOS-P = 0
 RX-LOC = 0
 AMPLI-GAIN-DEG-LOW = 0
 AMPLI-GAIN-DEG-HIGH = 0
 AUTO-LASER-SHUT = 0
 AUTO-POW-RED = 0
 AUTO-AMPLI-CTRL-DISABLED = 0
 AUTO-AMPLI-CFG-MISMATCH = 0
 SWITCH-TO-PROTECT = 0
 AUTO-AMPLI-CTRL-RUNNING = 0

 Parameter Statistics:
 ---------------------
 TX Power = 15.30 dBm
 RX Power = 5.30 dBm
 tx-enable = 1
 rx-enable = 1

 Configured Parameters:
 -------------
 tx-enable = 1
 rx-enable = 1
```

PSM three-way protection

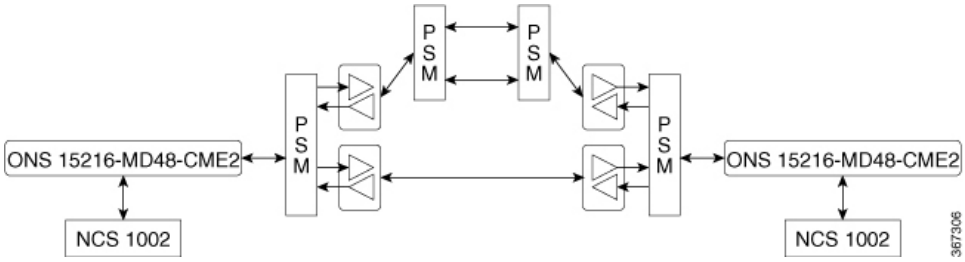
This topic describes the three-way protection topology formed by combining section and path protection, including threshold recommendations and limitations for switching behavior.

NCS 1001 supports PSM three-way protection scheme formed by combining a section protection scheme with a path protection scheme. No configuration change is required in PSM to implement the three-way protection scheme. The path protection scheme is inserted into one of the two paths in the section protection scheme.

Topology

Use the PSM automatic threshold configuration for the outer section protection.

Figure 9: Three-way protection network topology



Limitations

The three-way protection scheme has these limitations:

- For each PSM, switching the bi-directionality is not definite.
- Manual switching used to change the active path is sometimes unsuccessful.

Apply the lockout configuration on all four PSMs of the protection scheme to control switching from one path to another. Apply the lockout configuration on both the local and the corresponding remote PSM to ensure bi-directionality.

PSM revertive switch

This topic describes how PSM revertive switching returns traffic to the primary path after a fiber cut clears and explains WTR and threshold hysteresis behavior.

When a loss of signal (LOS) alarm occurs on the primary path because of a fiber cut, traffic moves from the primary path to the secondary path. The PSM revertive switch feature allows traffic to return to the primary path when the fiber cut is resolved and the LOS alarm is cleared. This switch back to the primary path is not immediate; it depends on several parameters.

Parameters of PSM revertive switch

- WTR (Wait To Restore): WTR is the time delay, in seconds, introduced after the LOS alarm on the primary path is cleared. When the WTR timer elapses, traffic moves to the primary path.
- Threshold hysteresis: The threshold hysteresis parameter prevents transient or fluctuating power readings near the threshold monitoring the primary RX port.

  If set, the threshold hysteresis parameter works with the WTR timer. After the fiber cut is fixed and the alarm is cleared, the system starts the WTR timer only when the power on the primary RX port is higher than the combined value of the rx-low-threshold and threshold hysteresis (rx-low-threshold-delta).

> **Note**
>
> The suggested values for WTR and threshold hysteresis parameters are 120 seconds and one dBm, respectively. You must choose both parameter values appropriately based on conditions, such as the power received, the type of PSM protection scheme, whether manual threshold values are provisioned on PSM, or if auto-threshold is enabled.

Limitations

- PSM revertive switch feature is supported only on section protection or path protection schemes.
- PSM revertive switch feature is not supported on PSM three-way protection scheme.
- PSM revertive switch feature is not supported on section protection or path protection schemes involving one or more ILA nodes.
- The PSM revertive switch feature is triggered only when traffic switches from the primary path to the secondary path because of a fiber cut. It does not activate if the switch occurs due to user commands, such as manual-to or lock-out-from.

Configure a PSM revertive switch

Use this task to complete the required CLI configuration for a PSM revertive switch and confirm that the intended NCS 1001 behavior is available after the changes are committed.

Procedure

1. Use this command to configure PSM revertive switch.

   hw-module location 0/RP0/CPU0 slot *psm-slot-number* **psm revertive wtr** *wtr-value* **primary-path** *path*

   wtr-value must be an integer. The primary path is set to WORKING by default. The user can change this path from WORKING to PROTECTED but cannot delete it.

   Example

   ```
   configure
   hw-module location 0/RP0/CPU0 slot 2 psm
   revertive wtr 120
   primary-path WORKING
   commit
   end
   ```

2. Use this command to configure the threshold hysteresis for the selected OTS controller.

   controller *rack/slot/instance/port* **rx-low-threshold-delta** *rx-low-threshold-delta-value*

   rx-low-threshold-delta is the threshold hysteresis. The value 10 is expressed in units of 0.1 dBm. In this example, the value of threshold hysteresis is set as 1.0 dBm.

   Example

   ```
   configure terminal
   ```

```
controller 0/2/0/1 rx-low-threshold-delta 10
commit
end
```

3. Use this command to verify the revertive switch and threshold hysteresis values.

   show controllers ots *rack/slot/instance/port*

   Example

```
RP/0/RP0/CPU0:ios# show controllers ots 0/2/0/1
        Controller State: Up

       Transport Admin State: In Service

       Port Type: Working

       Port Status: Standby

       Laser State: Unknown

       Optics Status::

               Alarm Status:
               -------------
               Detected Alarms:

               Alarm Statistics:
               -----------------
               LOW-RX-PWR = 0
               LOW-TX-PWR = 0
               RX-LOS-P = 735
               RX-LOC = 0
               AMPLI-GAIN-DEG-LOW = 0
               AMPLI-GAIN-DEG-HIGH = 0
               AUTO-LASER-SHUT = 0
               AUTO-POW-RED = 0
               AUTO-AMPLI-CTRL-DISABLED = 0
               AUTO-AMPLI-CFG-MISMATCH = 0
               SWITCH-TO-PROTECT = 4
               AUTO-AMPLI-CTRL-RUNNING = 0

               Parameter Statistics:
               ---------------------
               TX Power = -16.70 dBm
               RX Power = -21.00 dBm
               RX Voa Attenuation = 0.00 dB
               TX Voa Attenuation = 0.00 dB
               TX Enable = Enabled
               RX Enable = Enabled
               Rx Low Threshold Current = -38.0 dBm
               Wait Time to Restore = 120 secs


               Configured Parameters:
               -------------
               Rx Low Threshold = -38.0 dBm
               RX Voa Attenuation = 0.0 dB
               TX Voa Attenuation = 0.0 dB
               TX Enable = Enabled
```

```
                RX Enable = Enabled
                Rx Low Threshold Delta = 1.0 dBm
```

The configuration is committed and the optical module uses the requested settings.

Optical service channel

This topic describes the optical service channel wavelengths and the traffic types carried for UDC ports and remote management on the NCS 1001.

The Optical Service Channel (OSC) is an out-of-band channel that is added to and removed from the optical amplifier module. OSC supports 1510 nm and 1610 nm wavelengths.

Details

OSC provides a communication channel for these types of traffic.

- Traffic coming from a UDC port
- Traffic for remote management of NCS 1001

Configure remote management

Use this task to configure OSC interfaces and static routes so that local and remote NCS 1001 nodes can be managed across OSC links.

Configure remote management reachability between local and remote NCS 1001 nodes.

The Remote Management feature, introduced in R6.3.1, allows you to configure the IP addresses of local and remote nodes to enable remote management of NCS 1001.

Three OSC interfaces are configured to support remote management. They provide static routes to remote nodes. Each interface is statically associated with a slot: OSC1 with slot 1, OSC2 with slot 2, and OSC3 with slot 3.

Procedure

1. Configure the management and OSC interfaces. For details about management and OSC interfaces, see Configure management and OSC interfaces.
2. Configure static routes for remote node reachability. For details about static routes, see Configure static routes.

The NCS 1001 node has management reachability to remote nodes across the OSC links.

Configure management and OSC interfaces

Use this task to complete the required CLI configuration for management and OSC interfaces.

Procedure

Use these commands to configure management and OSC interfaces.

interface mgmtEth *rack/slot/instance/port*

ipv4 address *ipv4-address subnet-mask*

These are samples of configuring the management and OSC interfaces.

Example

```
configure
      interface MgmtEth 0/RP0/CPU0/0
      ipv4 address 10.58.227.198 255.255.255.0
      shutdown
      exit
```

```
configure
      interface MgmtEth 0/RP0/OSC1/0
      ipv4 address 10.1.1.1 255.255.255.0
      shutdown
      exit
```

```
configure
      interface MgmtEth 0/RP0/OSC2/0
      ipv4 address 10.1.2.1 255.255.255.0
      shutdown
      exit
```

```
configure
      interface MgmtEth 0/RP0/OSC3/0
      ipv4 address 10.1.3.1 255.255.255.0
      shutdown
      exit
```

Configure static routes

Use this task to complete the required CLI configuration for static routes.

This procedure configures all the static routes into the NCS 1001 node.

Procedure

Use the **router static address-family** command to configure static routes.

router static address-family ipv4 unicast 0.0.0.0/0 *default-gateway*

This sample shows the NCS 1001 node connected to three different nodes using static routes.

Example

```
configure
      router static address-family ipv4 unicast
      0.0.0.0/0 MgmtEth 0/RP0/CPU0/0 10.58.227.1
      10.1.1.0/24 MgmtEth 0/RP0/OSC1/0 10.1.1.2
      10.1.2.0/24 MgmtEth 0/RP0/OSC2/0 10.1.2.2
      10.1.3.0/24 MgmtEth 0/RP0/OSC3/0 10.1.3.2
      exit
```

Configure network topology discovery

Use this task to configure OSPF routes and verify routing table entries so compatible NCS 1001 nodes can be discovered across OSC links.

Configure topology discovery for compatible NCS 1001 nodes connected through OSC links.

The network topology discovery feature enables discovery of NCS 1001 nodes that are connected to each other through OSC links, without the need to configure static routes. This feature is based on the OSPF protocol and is introduced in Release 6.3.2

You must configure OSPF on NCS 1001 nodes by defining the name, router ID, and interfaces in Area 0. You can optionally configure the interfaces as passive. OSPF and OSPFv3 protocols are supported.

These network topologies are supported:

- Point-to-Point
- Point-to-Point with ILA nodes (up to three ILA nodes)

Procedure

1. Configure management and OSC interfaces. For details, see Configure management and OSC interfaces on page 69.
2. Configure OSPF routes. For details, see Configure OSPF routes.
3. Verify the OSPF routing table. For details, see Verify the OSPF routing table.

The NCS 1001 node can discover compatible nodes through OSPF over OSC links.

Configure OSPF routes

Use this task to complete the required CLI configuration for OSPF routes.

Procedure

Use these commands to configure OSPF routes.

router ospf *process-id*

router-id *ip-address*

area *area-id*

This is a sample of configuring OSPF routes.

Example

```
configure
      interface MgmtEth0/RP0/CPU0/0
       ipv4 address 10.1.1.2 255.255.255.0
      !
      interface MgmtEth0/RP0/OSC1/0
       shutdown
      !
      interface MgmtEth0/RP0/OSC2/0
       ipv4 address 10.1.3.2 255.255.255.0
      !
```

```
interface MgmtEth0/RP0/OSC3/0
 ipv4 address 10.1.4.2 255.255.255.0
!
router ospf remote
 router-id 10.1.1.2
 area 0
  interface MgmtEth0/RP0/CPU0/0
   passive enable
  !
  interface MgmtEth0/RP0/OSC2/0
  !
  interface MgmtEth0/RP0/OSC3/0
  !
 !
!
end
```

Verify the OSPF routing table

Use this task to complete the required CLI verification for the OSPF routing table

Procedure

Use the **show ospf routes** command to verify the OSPF routing table.

Example

```
RP/0/RP0/CPU0:ios# show ospf routes
Sat Jul 29 09:54:25.937 UTC

          Topology Table for ospf local with ID 10.1.4.1

          Codes: O - Intra area, O IA - Inter area
                 O E1 - External type 1, O E2 - External type 2
                 O N1 - NSSA external type 1, O N2 - NSSA external type 2

          O    10.1.1.0/24, metric 1
                 10.1.1.2, directly connected, via MgmtEth0/RP0/CPU0/0
          O    10.1.3.0/24, metric 1
                 10.1.3.2, directly connected, via MgmtEth0/RP0/OSC2/0
          O    10.1.7.0/24, metric 2
                 10.1.3.1, from 10.58.227.198, via MgmtEth0/RP0/OSC2/0
          O    10.58.227.0/24, metric 1
                 10.1.3.1, from 10.58.227.198, via MgmtEth0/RP0/OSC2/0
```

The command output shows whether the expected OSPF routes are present.

Network troubleshooting commands

This topic provides information about common management and OSPF routing issues with the commands used to check interface state, static routing, subnets, passive interfaces, and learned routes.

Troubleshooting must be performed by checking the status of the interfaces, subnets, static routing, and OSPF sections.

Problem	Command
Interfaces are in down state.	**show interfaces MgmtEth** *rack/slot/instance/port*
Route to default gateway is not defined.	**show running-config**
The design phase included incorrect IP addresses or subnets.	**show running-config**
Static routes were defined incorrectly and overwrite OSPF routes.	Compare the output of **show ip route** command with the **show ospf routes** command
The OSPF configuration does not include all the interfaces.	**show running-config**
The OSPF configuration sets certain interfaces to passive mode.	**show running-config**

Troubleshoot UDC port configurations

Use this task to clear UDC port statistics, display switch port information, verify counters, and configure Clear-On-Read behavior for affected port pairs.

Troubleshoot UDC port configurations by clearing statistics and checking port attributes, port state, VLAN lists, and port counters.

Table 16: Feature History

Feature Name	Release	Description
Troubleshooting User Data Channel (UDC) Port Configurations	Cisco IOS XR Release 7.8.1	The **hw-module** and **show hw-module** commands have been enhanced with additional keywords to improve the troubleshooting of issues on UDC ports. Apart from viewing the UDC port state, VLAN list, and port statistics, you can clear UDC port configurations and enable or disable configurations on each UDC port.

From Release 7.8.1, the **hw-module eth-switch** and **show hw-module eth-switch** commands provide options to troubleshoot UDC ports and view the current configuration.

> **Note**
>
> The `hw-module eth-switch clear-stats` command clears all the counters on the selected port and turns off the `Clear-On-Read` attribute. You can re-enable `Clear-On-Read` with the `enable-clear-on-read` attribute.

Procedure

1. Clear the statistics configured for UDC port 1.

Example

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#hw-module eth-switch clear-stats port Rj45Udc1
RP/0/RP0/CPU0:ios(config)#commit
```

2. Clear the statistics configured for all the ports.

Example

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#hw-module eth-switch clear-stats all
RP/0/RP0/CPU0:ios(config)#commit
```

3. Display the configured attributes of the UDC ports.

Example

```
RP/0/RP0/CPU0:ios#show hw-module eth-switch ports-attrs
```

This output shows the attributes of all the configured ports.

```
Thu Nov 10 13:24:16.932 CET
Ports Attributes:
Port SfpUdc3  # 0 (enable)      Link UP         Full-Duplex  9604 [1 Gbps]
6(1000BASE_X)     Clear-On-Read
Port SfpUdc2  # 4 (enable)      Link UP         Full-Duplex  9604 [1 Gbps]
6(1000BASE_X)     Clear-On-Read
Port SfpUdc1  # 8 (enable)      Link UP         Full-Duplex  9604 [1 Gbps]
6(1000BASE_X)     Clear-On-Read
Port Rj45Udc1 # 12 (enable)     Link DOWN       Half-Duplex  9600 [1 Gbps]
3(SGMII)     Clear-On-Read
Port Rj45Udc2 # 16 (enable)     Link DOWN       Half-Duplex  9600 [1 Gbps]
3(SGMII)     Clear-On-Read
Port Rj45Udc3 # 20 (enable)     Link DOWN       Half-Duplex  9600 [1 Gbps]
3(SGMII)     Clear-On-Read
Port CpuMgmt  # 24 (enable)     Link UP         Full-Duplex  1522 [1 Gbps]
6(1000BASE_X)
Port          # 25 (enable)     Link UP         Full-Duplex  1522 [1 Gbps]
6(1000BASE_X)
Port Rj45Mgmt # 26 (enable)     Link UP         Full-Duplex  1522 [1 Gbps]
3(SGMII)
Port SfpMgmt  # 27 (enable)     Link DOWN       Half-Duplex  1522 [1 Gbps]
3(SGMII)
```

The command output displays the link state, duplex mode, maximum transmission unit, speed, interface type, and `Clear-On-Read` status for each configured port.

4. Display the counters that are related to the `CpuMgmt` port.

Example

```
RP/0/RP0/CPU0:ios#show hw-module eth-switch stats port CpuMgmt
```

This output displays the counter values for the `CpuMgmt` port.

```
Mon May 16 09:10:24.491 UTC

****************** START ******************
 PORT MAC COUNTERS - Test cmd [1] [Port:0x18]
  goodPktsSent          0
  goodPktsRcv           0
  ucPktsSent            17
  ucPktsRcv             2
  mcPktsSent            1489
  mcPktsRcv             0
  brdcPktsSent          349
  brdcPktsRcv           1
  goodOctetsSent        200863
  goodOctetsRcv         474
  pkts64Octets          614
  pkts65to127Octets     872
  pkts128to255Octets    86
  pkts256to511Octets    286
  pkts512to1023Octets   0
  pkts1024tomaxOoctets  0
  pkts1024to1518Octets  0
```

The command output displays MAC counter values, including packets, octets, and packet-size counters for the `CpuMgmt` port.

5. Enable MAC counters Clear-On-Read for the `Rj45Udc1` port.

   Enabling or disabling MAC counters Clear-On-Read affects the corresponding port pairs: `SfpUdc3 #0` and `SfpUdc2 #4`, and `Rj45Udc1 #12` and `Rj45Udc2 #16`. Configuring this attribute on `Rj45Udc1 #12` also affects `Rj45Udc2 #16` and the other way around.

   Example

   ```
   RP/0/RP0/CPU0:ios#configure
   RP/0/RP0/CPU0:ios(config)#hw-module eth-switch port Rj45Udc1
   enable-clear-on-read
   RP/0/RP0/CPU0:ios(config)#commit
   ```

6. Verify the hardware module Ethernet switch port attributes.

   Example

   ```
   RP/0/RP0/CPU0:ios#show hw-module eth-switch ports-attrs
   Ports Attributes:
   Port SfpUdc3  # 0 (enable)      Link UP         Full-Duplex  9604 [1 Gbps]
   6(1000BASE_X)
   Port SfpUdc2  # 4 (enable)      Link UP         Full-Duplex  9604 [1 Gbps]
   6(1000BASE_X)
   Port SfpUdc1  # 8 (enable)      Link UP         Full-Duplex  9604 [1 Gbps]
   6(1000BASE_X)
   Port Rj45Udc1 # 12 (enable)     Link UP      Half-Duplex  9600 [1 Gbps]
   3(SGMII)     Clear-On-Read
   Port Rj45Udc2 # 16 (enable)     Link UP      Half-Duplex  9600 [1 Gbps]
   3(SGMII)     Clear-On-Read
   Port Rj45Udc3 # 20 (enable)     Link UP         Full-Duplex  9600 [1 Gbps]
   3(SGMII)
   Port CpuMgmt  # 24 (enable)     Link UP         Full-Duplex  1522 [1 Gbps]
   6(1000BASE_X)
   ```

```
Port          # 25 (enable)     Link UP         Full-Duplex  1522 [1 Gbps]
6(1000BASE_X)
Port Rj45Mgmt # 26 (enable)     Link UP         Full-Duplex  1522 [100 Mbps]
 3(SGMII)
Port SfpMgmt  # 27 (enable)     Link DOWN       Half-Duplex  1522 [1 Gbps]
3(SGMII)
```

The command output shows whether `Clear-On-Read` is enabled for the expected UDC ports.

The UDC port statistics and Clear-On-Read behavior are updated and verified from the hardware module Ethernet switch command output.

4 Configure OTDR Module

Topics:

Understand OTDR module capabilities, cabling, configuration modes, event-based automatic scans, scan status and output, photodiode power levels, IPv6 support, and machine learning event classification on Cisco NCS 1001 systems.

OTDR

This topic describes the OTDR line card, its physical and logical ports, supported measurement modes, and operating limits for Cisco NCS 1001 fiber inspection.

The Optical Time Domain Reflectometer (OTDR) is a Cisco NCS 1001 line card that measures optical fiber characteristics between optical nodes.

The line card contains two bidirectional OTDRs and two filters that combine C-band, optical supervisory channel (OSC), and OTDR signals. Each internal OTDR can measure both transmit (TX) and receive (RX) fibers by using an internal optical switch.

The OTDR line card connects to the OSC port on the optical amplifier. Measurement data is stored in an .SOR file and can be exported from Cisco NCS 1001 by using SCP, TFTP, or SFTP.

The OTDR line card:

- provides information about insertion loss and reflection points on the optical fiber,
- inspects the transmission fiber,
- identifies discontinuities or defects on the fiber,
- measures the distance and magnitude of insertion loss and reflection loss events, and
- improves scan performance through scan parameters that match the fiber plant, such as span length, reflection contribution, and major events.

OTDR card front view

Figure 10: Front view of OTDR card

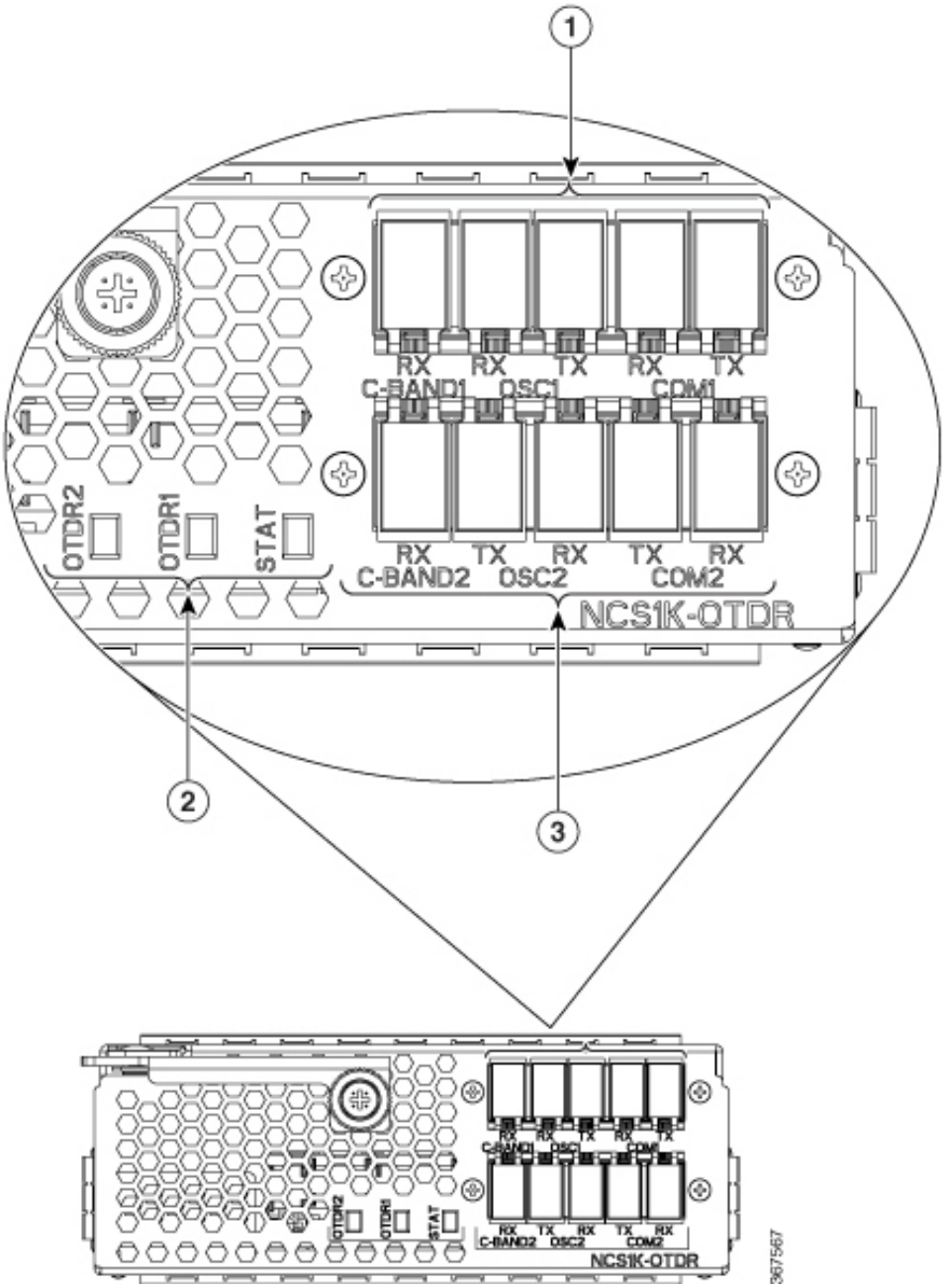


Table 17: OTDR front-panel callouts

Callout	Description
1	OTDR1 interface
2	LED status
3	OTDR2 interface

Logical ports

The OTDR card associates physical ports with these logical OTS controller ports.

Table 18: OTDR physical ports and associated logical ports

OTDR port	Logical port
C-Band-1 RX	controller OTS 0/slot/0/0
COM1 (RX, TX)	controller OTS 0/slot/0/1
OSC1 (RX, TX)	controller OTS 0/slot/0/2
C-Band-2 RX	controller OTS 0/slot/0/3
COM2 (RX, TX)	controller OTS 0/slot/0/4
OSC2 (RX, TX)	controller OTS 0/slot/0/5

For command output that displays these logical ports and photodiode power levels, see view the logical ports and photodiode power levels.

OTDR modes

OTDR supports automatic and expert modes.

Table 19: OTDR modes

Mode	Description
Automatic	Uses automated training and measurement phases. Training measures optical return loss (ORL) and prepares the internal OTDR measurement parameters before the measurement starts.
Expert	Requires the user to configure the OTDR scan parameters. The mode does not run a training phase and does not automatically adjust the scan parameters.

OTDR limitations

- When Cisco NCS 1001 uses the OTDR line card, the OSC channel uses 1610 nm and OTDR uses 1518 nm.
- OTDR supports up to 20 dB span loss or 100 km fiber length.
- Do not start OTDR measurements simultaneously from two different nodes because the results and graph are not valid.
- OTDR measurement during an OTDR-HIGH-REFLECTION alarm, with reflections approximately greater than -25 dB, can provide low event accuracy.
- OTDR graphs can be truncated for fiber spools from 1.00 km to 1.05 km, 25.0 km to 25.6 km, or 80.0 km to 83.9 km.
- OTDR supports up to -14 dB reflection. The OTDR-HIGH-REFLECTION alarm is raised when R(dB) - 2*NL(dB) is greater than -20 dB, where R is reflectivity and NL is loss.

LOS-P alarm handling

> **Note**
>
> When an EDFA module is connected to the OTDR module without an OSC channel between them, an LOS-P alarm is raised on OTS 0/x/0/2 of the EDFA module. Configure the OTS controller under maintenance or shut down the EDFA receive direction on port 0/x/0/2 to suppress the alarm and resume normal OTDR operation.

Example: Configure the OTS controller under maintenance.

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#controller ots 0/3/0/2
RP/0/RP0/CPU0:ios(config-ots)#sec-admin-state maintenance
RP/0/RP0/CPU0:ios(config-ots)#commit
```

Example: Shut down the EDFA port in the receive direction.

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#controller ots 0/3/0/2
RP/0/RP0/CPU0:ios(config-ots)#rx-enable 0
RP/0/RP0/CPU0:ios(config-ots)#commit
```

Cable a terminal node for OTDR

Use this procedure to connect OTDR and EDFA ports in a terminal node so that OSC and OTDR signals are carried through the expected fiber path.

Connect the OTDR and EDFA ports in the correct order for port 1. If needed, repeat the sequence for the second OTDR port.

In a terminal-node configuration, both the EDFA and OTDR line cards are installed in the same Cisco NCS 1001 system. The OTDR filter combines the EDFA OSC SFP signal with the OTDR signal. It then feeds the combined signal into the EDFA OSC input.

Procedure

1. Connect an LC/LC fiber from the OTDR COM TX port to the EDFA OSC RX port.
2. Connect an LC/LC fiber from the EDFA OSC TX port to the OTDR COM RX port.
3. Connect an LC/LC fiber from the OTDR OSC TX port to the pluggable RX port inserted into the EDFA.
4. Connect an LC/LC fiber from the pluggable TX port inserted into the EDFA to the OTDR OSC RX port.

   The port 1 terminal-node cabling path is complete. If you need to connect a second OTDR port, repeat the sequence.

   Figure 11: Cabling for terminal configuration with one EDFA module

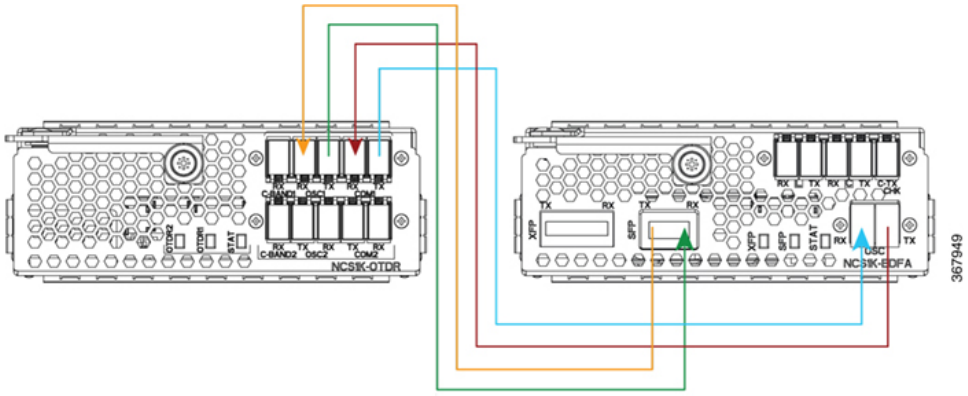
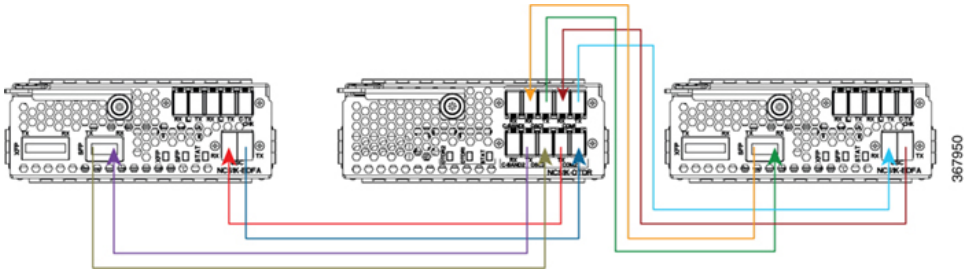


Figure 12: Cabling for terminal configuration with two EDFA modules



The terminal node cabling supports OTDR measurement through the EDFA OSC path.

Cable an ILA node for OTDR

Use this procedure to connect a single OTDR card to the EDFA cards in an ILA node so both ILA directions support OTDR measurements.

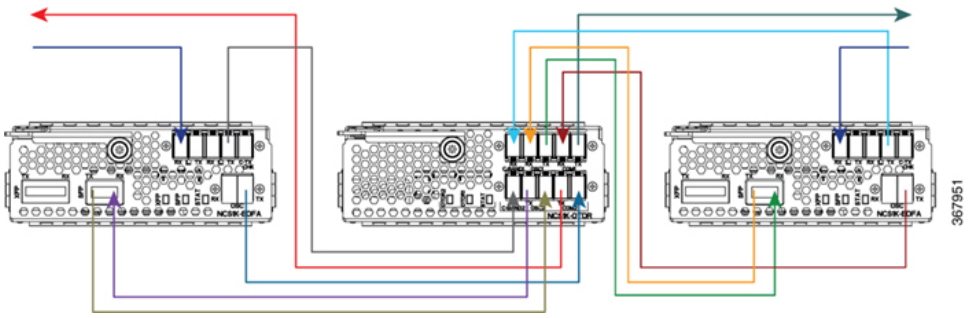
Connect OTDR port 1 to the EDFA in slot 1 and OTDR port 2 to the EDFA in slot 3.

In an Intermediate Line Amplifier (ILA) node, one OTDR card supports both ILA directions. Two EDFA cards and one OTDR line card are installed in the same Cisco NCS 1001 system.

Procedure

1. Cable OTDR port 1 to the EDFA in slot 1.
   a) Connect an LC/LC fiber from OTDR port 1 COM TX to the fiber span Line TX that faces EDFA slot 1.
   b) Connect an LC/LC fiber from EDFA slot 1 COM TX to C-band 1 RX.
   c) Connect an LC/LC fiber from OTDR OSC TX port 1 to the OSC pluggable RX port inserted into EDFA slot 1.
   d) Connect an LC/LC fiber from the OSC pluggable TX port inserted into EDFA slot 1 to OTDR OSC RX port 1.
   e) Connect an LC/LC fiber from EDFA slot 1 OSC TX to OTDR COM RX port 1.
2. Cable OTDR port 2 to the EDFA in slot 3.
   a) Connect an LC/LC fiber from OTDR port 2 COM TX to the fiber span Line TX that faces EDFA slot 3.
   b) Connect an LC/LC fiber from EDFA slot 3 COM TX to C-band 2 RX.
   c) Connect an LC/LC fiber from OTDR OSC TX port 2 to the OSC pluggable RX port inserted into EDFA slot 3.
   d) Connect an LC/LC fiber from the OSC pluggable TX port inserted into EDFA slot 3 to OTDR OSC RX port 2.
   e) Connect an LC/LC fiber from EDFA slot 3 OSC TX to OTDR COM RX port 2.

Figure 13: Cabling for ILA configuration



The OTDR card is connected to both ILA directions.

Cable an ILA node with 15216-FLD-OSC for OTDR

Use this procedure to connect ILA cabling through the 15216-FLD-OSC module when the deployment still uses that module in the OSC path.

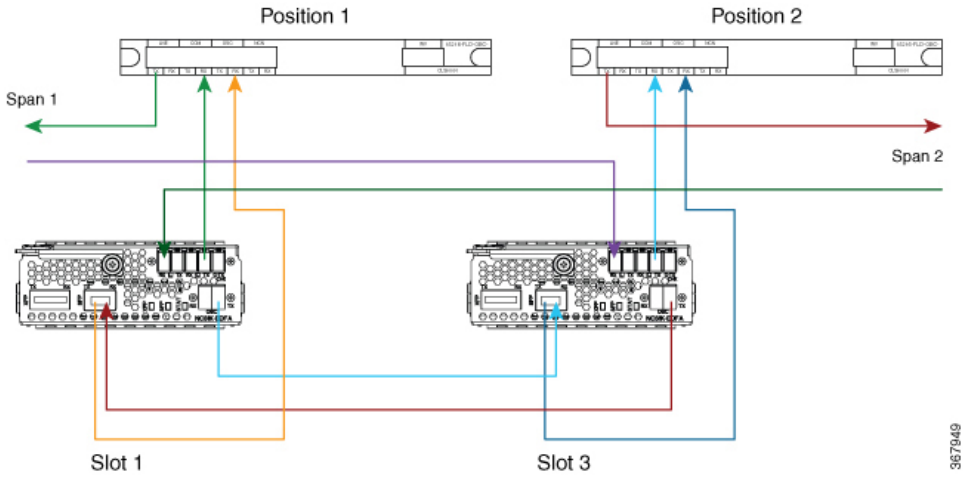
Connect the span, EDFA, OSC pluggable, and 15216-FLD-OSC ports sequentially.

The NCS1K-OTDR module replaces the need for the 15216-FLD-OSC module in the recommended ILA configuration.

Procedure

1. Connect the EDFA slot 1 line and COM paths.
   a) Connect an LC/LC fiber from RX-span 2 to the LINE RX port of EDFA slot 1.
   b) Connect an LC/LC fiber from the COM TX port of EDFA slot 1 to the COM RX port of 15216-FLD-OSC position 1.
   c) Connect an LC/LC fiber from TX-span 1 to the LINE TX port of 15216-FLD-OSC position 1.
2. Connect the EDFA slot 1 OSC path.
   a) Connect an LC/LC fiber from the OSC pluggable TX port inserted into EDFA slot 1 to the OSC RX port of 15216-FLD-OSC position 1.
   b) Connect an LC/LC fiber from the OSC TX port of EDFA slot 1 to the OSC pluggable RX port inserted into EDFA slot 3.
3. Connect the EDFA slot 3 OSC path.
   a) Connect an LC/LC fiber from the OSC TX port of EDFA slot 3 to the OSC pluggable RX port inserted into EDFA slot 1.
   b) Connect an LC/LC fiber from the OSC pluggable TX port inserted into EDFA slot 3 to the OSC RX port of 15216-FLD-OSC position 2.
4. Connect the EDFA slot 3 line and COM paths.
   a) Connect an LC/LC fiber from RX-span 1 to the LINE RX port of EDFA slot 3.
   b) Connect an LC/LC fiber from the COM TX port of EDFA slot 3 to the COM RX port of 15216-FLD-OSC position 2.
   c) Connect an LC/LC fiber from TX-span 2 to the LINE TX port of 15216-FLD-OSC position 2.

Figure 14: Cabling for ILA configuration with 15216-FLD-OSC



The ILA node cabling through the 15216-FLD-OSC module is complete.

Clear the card configurations

Use this procedure to clear card-level, OTS controller, and optics controller configurations before you replace a configured optical module with an OTDR module.

Clear the previous optical module configuration to prevent the replacement OTDR module from inheriting configuration from the old card.

Before installing a new, different type of optical module, clear the configurations of the old module. A Cisco NCS 1001 slot configuration can include card configuration, OTS controller configuration, and optics controller configuration for EDFA cards.

Follow these steps to clear the card configurations:

Procedure

1. Clear the configuration in the previous card.

   no hw-module location 0/RP0/CPU0 slot *slot-number*

2. Clear the configuration for each OTS controller.

   no controller ots *rack/slot/instance/port*

3. If the previous card was an EDFA card, clear each optics controller configuration.

   no controller optics *rack/slot/instance/port*

After clearing the old card configuration, the slot is ready for the replacement OTDR module.

Configure OTDR

Use this procedure to configure OTDR optical parameters for TX and RX directions after the OTDR card is inserted into Cisco NCS 1001.

Configure OTDR parameters when the default values must be changed for the fiber span.

When the OTDR card is inserted, it has default optical parameters for both the ports and both the TX and RX directions.

Procedure

1. Enter configuration mode.

   Example

   ```
   configure
   ```

2. Use the hw-module location command to enter OTDR slot configuration mode.

   Example

   ```
   hw-module location 0/RP0/CPU0 slot 2
   ```

3. Configure the OTDR parameters for the required port and direction.

   Configure only the parameter values that must differ from the default values.

   See OTDR configuration parameters for the parameter descriptions, ranges, and defaults.

   Example

   ```
   otdr port 1 direction tx total-loss 200
   otdr port 1 direction tx back-scattering -820
   otdr port 1 direction tx refractive-index 1498962
   otdr port 1 direction tx mode-expert pulse-width 1000
   otdr port 1 direction tx mode-expert measure-time 180
   otdr port 1 direction tx mode-expert capture-length 80
   otdr port 1 direction tx mode-expert capture-offset 0
   otdr port 1 direction tx mode-expert fiber-resolution 25
   otdr port 1 direction tx mode-expert loss-relative-threshold 20
   otdr port 1 direction tx mode-expert reflection-relative-threshold 20
   otdr port 1 direction rx total-loss 200
   otdr port 1 direction rx mode-expert pulse-width 1000
   otdr port 1 direction rx mode-expert measure-time 180
   otdr port 1 direction rx mode-expert capture-length 80
   otdr port 1 direction rx mode-expert capture-offset 0
   otdr port 1 direction rx mode-expert fiber-resolution 25
   otdr port 1 direction rx mode-expert loss-relative-threshold 20
   otdr port 1 direction rx mode-expert reflection-relative-threshold 20
   otdr port 1 orl-abs-threshold 280
   otdr port 1 loss-abs-threshold 15
   otdr port 1 reflection-abs-threshold -300
   commit
   end
   ```

4. Commit the configuration and exit configuration mode.

Example

```
commit
end
```

The OTDR parameters are configured for the selected port and direction.

OTDR configuration parameters

This topic lists the OTDR parameter descriptions, valid ranges, and default values used when configuring OTDR manually.

Use these values when configuring OTDR optical parameters for the selected port and direction.

Table 20: OTDR configuration parameters

Parameter	Description	Range	Default
total-loss (in 0.1 dB)	Loss from the near-end OTDR port to the far-end OTDR port, including span loss and additional EDFA filter loss.	0 to 500	200
back-scattering	Backscattering value in the TX direction.	-100.0 to 0.0	-82.0
refractive-index	Refractive index value in the TX direction.	1.000000 to 2.000000	1.498962
mode-expert pulse-width (ns)	Pulse duration during the measurement.	8 to 100000	1000
mode-expert measure-time (sec)	Time required to perform a complete optical scan.	1 to 360	180
mode-expert capture-length (km)	Distance of the measurement endpoint.	1 to 150	80
mode-expert capture-offset (km)	Start point of the measurement.	0 to 150	0
mode-expert fiber-resolution (m)	Distance between measurement steps.	0 to 100	25
orl-abs-threshold (in 0.1 dB)	Threshold to compare with the ORL measurement returned by the OTDR run.	140 to 400	280
loss-abs-threshold (in 0.1 dB)	Threshold to compare with loss events returned by the OTDR run.	1 to 300	15
reflection-abs-threshold (in 0.1 dB)	Threshold to compare with reflection events returned by the OTDR run.	-500 to 0	-300

Parameter	Description	Range	Default
loss-sensitivity (in 0.1 dB)	Limit under which the loss is not considered a real loss.	4 to 50	6
reflection-sensitivity (in 0.1 dB)	Limit under which the reflection is not considered a real reflection.	-400 to -140	-300
loss-relative-threshold (in 0.1 dB)	Threshold to compare the OTDR loss value plus the relative loss threshold with the baseline value.	1 to 300	2
reflection-relative-threshold (in 0.1 dB)	Threshold to compare the OTDR reflection value plus the relative reflection threshold with the baseline value.	1 to 300	2

Note

From Release 7.5.1, the plus sign labels in positive range values are removed in the Cisco NCS 1001 CLI help description.

Note

For back-scattering and refractive-index, Cisco NCS 1001 accepts any value within the defined range. Set the actual value based on the fiber characteristics and optimal values for the specific fiber type in your network.

Display OTDR measurement status

Use this procedure to display training, measurement, direction, and next-scan status for all OTDR ports on a slot during scan verification.

Display OTDR measurement status to confirm whether automatic or expert scans are running, completed, aborted, or unknown.

The command displays a table with status for all the OTDR ports and directions.

Procedure

Use the show hw-module command to display OTDR status for the slot.

Example

```
show hw-module slot 2 otdr status
 Automatic Mode
```

```
Wed Oct 16 09:06:46.148 CEST
  Port | Rx/Tx |  Date/Time|     Training |   OTDR Measurement| Next scan (min)
-------+-------+-------------------+------------------+-------------------+-

   1   |   Tx  |           |      UNKNOWN  |       UNKNOWN     |       0
   1   |   Rx  |           |      UNKNOWN  |       UNKNOWN     |       0
   2   |   Tx  |           |      UNKNOWN  |       UNKNOWN     |       0
   2   |   Rx  |           |      UNKNOWN  |       UNKNOWN     |       0

The next scan is related to the periodic scan. When the periodic scan is not
set, the next scan value is 0.
 Expert Mode

Port | Rx/Tx |      Date/Time        |     Training       |   OTDR Measurement
-----------+-------+-------------------+------------------+-------------------


   1   |   Tx  |   20180503-181159   |     UNKNOWN          | PROGRESS    10%


   1   |   Rx  |                     |     UNKNOWN          |       UNKNOWN

   2   |   Tx  |                     |     UNKNOWN          |       UNKNOWN

   2   |   Rx  |                     |     UNKNOWN          |       UNKNOWN
```

If periodic scan is not set, the next-scan value is 0.

Configure OTDR in automatic mode

Use this procedure to configure automatic mode OTDR parameters so the device can run training and measurement phases with default or customized scan values.

Configure automatic mode to have OTDR prepare measurement parameters and run scans through automated training and measurement phases.

Automatic mode provides default values for scan parameters. Adjust values only if the fiber span requires a different measurement behavior.

Procedure

1. Enter configuration mode.

   Example

   ```
   configure
   ```

2. Use the **hw-module location** command to enter OTDR automatic mode configuration for the slot, port, and direction.

   Example

   ```
   hw-module location 0/RP0/CPU0 slot 3 otdr port 1 direction tx scan auto
   ```

3. Configure automatic mode parameters.

See OTDR automatic-mode parameters for parameter descriptions, ranges, and defaults.

Example

```
loss-sensitivity 5
loss-relative-threshold 10
reflection-sensitivity -300
reflection-relative-threshold 5
total-loss 300
periodic-scan minutes 40
```

4. Commit the configuration and exit configuration mode.

Example

```
commit
end
```

OTDR automatic mode is configured for the selected port and direction.

OTDR automatic mode parameters

This table lists parameter descriptions, valid ranges, and default values for OTDR automatic mode configuration, including relative thresholds and periodic scan settings.

Use these values when configuring OTDR in automatic mode.

Table 21: OTDR automatic mode parameters

Parameter	Description	Range	Default
loss-sensitivity (in 0.1 dB)	Limit under which the loss is not considered a real loss.	4 to 50	6
loss-relative-threshold (in 0.1 dB)	Threshold to compare the OTDR loss value plus the relative loss threshold with the baseline value.	1 to 300	2
reflection-sensitivity (in 0.1 dB)	Limit under which the reflection is not considered a real reflection.	-400 to -140	-300
reflection-relative-threshold (in 0.1 dB)	Threshold to compare the OTDR reflection value plus the relative reflection threshold with the baseline value.	1 to 300	2
total-loss (in 0.1 dB)	Loss from the near-end OTDR port to the far-end OTDR port, including span loss and additional EDFA filter loss.	1 to 500	200

Parameter	Description	Range	Default
periodic scan (minutes)	Automatically starts OTDR scans and repeats the scan after the periodic scan time elapses.	30 to 600000	30

Note

From Release 7.5.1, the plus sign labels in positive range values are removed in the Cisco NCS 1001 CLI help description.

Start OTDR measurement in automatic mode

Use this procedure to start an OTDR automatic mode scan for a selected slot, port, and direction after scan parameters are configured.

Start automatic measurement after the OTDR automatic mode parameters are configured.

The scan continues in the background after the command starts the action.

Procedure

Use the **hw-module** command to start the OTDR automatic mode scan.

hw-module slot *slot-number* **otdr port** *port-number* **direction** *direction* **scan auto**

Example

```
hw-module slot 3 otdr port 1 direction tx scan auto
```

The system displays the message "Otdr action will continue in the background."

What to do next

To see the measurement status, use the **show hw-module slot** *slot-number* **otdr status** command.

OTDR measurement in automatic mode based on events

This topic explains which events start OTDR automatic scans and how the supported deployment scenarios determine the autoscan configuration for node pairs.

OTDR automatic measurement can start on both TX and RX directions between two nodes when specific network events occur.

- An automatic scan starts when a loss of signal (LOS) alarm is raised or cleared on the line port of an EDFA, such as controller OTS 0/x/0/1. If an automatic scan is already running, a new LOS state change aborts the current scan and starts a new one.
- An automatic scan also starts when the difference between the current span-loss value and the previous span-loss sample exceeds the configured span-loss delta value.

hw-module location 0/RP0/CPU0 slot <n> ampli span-loss span-loss-delta 20

Supported deployment scenarios

OTDR modules can be deployed in four different scenarios:

- Node A connects to Node B, and each node has its own OTDR module.
- Node A connects to Node B, and a single OTDR module is installed in either Node A or Node B.
- Node A connects to Node B, and a single OTDR module is installed in a different Node C.
- Node A connects to Node B, and OTDR modules are installed in different Nodes C and D.

Note

Nodes A and B can be terminal nodes or ILA nodes.

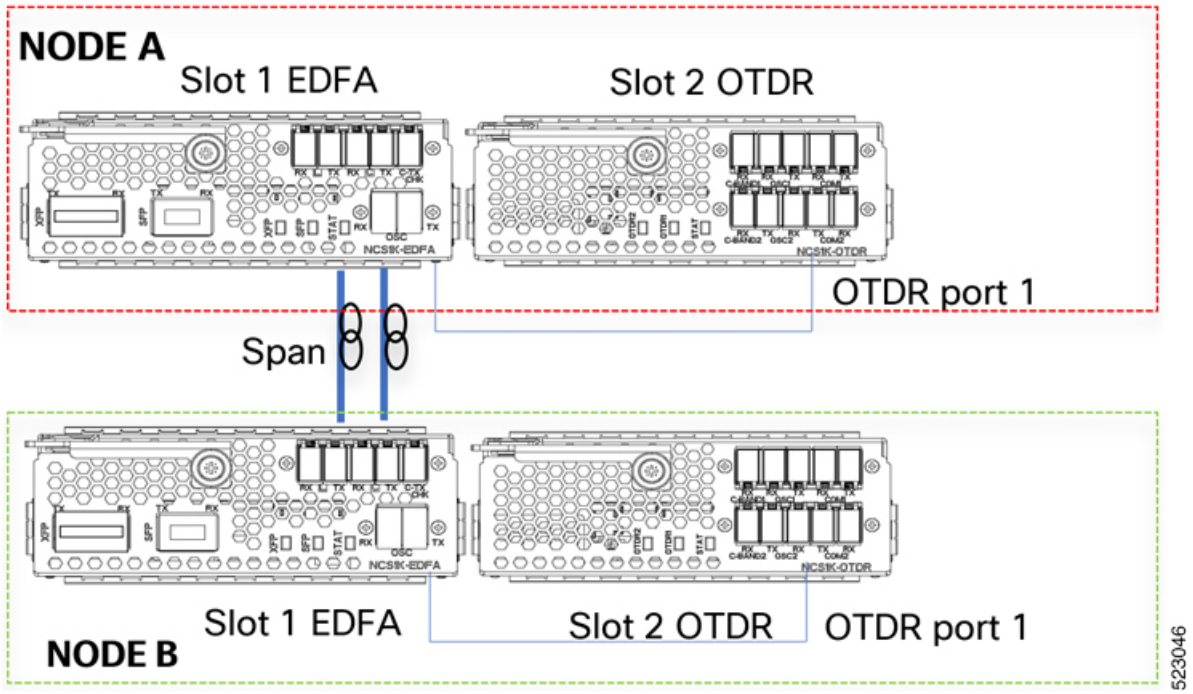
Configure OTDR autoscan for scenario 1

Use this procedure when Node A and Node B each have a local OTDR module connected to the local EDFA that faces the shared fiber span.

Configure the remote node and OTDR autoscan commands for the selected event-based automatic scan scenario.

In scenario 1, OTDR modules are installed in both nodes. Each OTDR connects to its local EDFA, and both EDFAs face the same fiber span.

Figure 15: Scenario 1 EDFA remote node configuration



Procedure

1. Configure the remote node feature for each EDFA module on Node A and Node B.

   Example

```
Node A:
hw-module location 0/RP0/CPU0 slot 1 ampli remote-node local-ipv4 <IP Node
A> remote-ipv4 <IP Node B> remote-slot-id 1

Node B:
hw-module location 0/RP0/CPU0 slot 1 ampli remote-node local-ipv4 <IP Node
B> remote-ipv4 <IP Node A> remote-slot-id 1
```

2. Configure OTDR autoscan for each EDFA module on Node A and Node B.

   Example

```
Node A:
hw-module location 0/RP0/CPU0 slot 1 ampli otdr-autoscan otdr-module-ipv4-addr
 <IP Node A> otdr-slot-id 2 otdr-port-id 1 ampli-far-end-ipv4-addr <IP Node
B> ampli-far-end-slot-id 1 scan-type AUTO

Node B:
hw-module location 0/RP0/CPU0 slot 1 ampli otdr-autoscan otdr-module-ipv4-addr
 <IP Node B> otdr-slot-id 2 otdr-port-id 1 ampli-far-end-ipv4-addr <IP Node
A> ampli-far-end-slot-id 1 scan-type AUTO
```

3. Configure the remote node OTDR autoscan for each OTDR module on Node A and Node B.

   Example

```
Node A:
hw-module location 0/RP0/CPU0 slot 2 otdr port 1 otdr-autoscan
otdr-module-ipv4-addr <IP Node A> ampli-far-end-ipv4-addr <IP Node A>
ampli-far-end-slot-id 1 scan-type AUTO

Node B:
hw-module location 0/RP0/CPU0 slot 2 otdr port 1 otdr-autoscan
otdr-module-ipv4-addr <IP Node B> ampli-far-end-ipv4-addr <IP Node B>
ampli-far-end-slot-id 1 scan-type AUTO
```

The event-based OTDR automatic scan configuration is ready for the selected scenario.

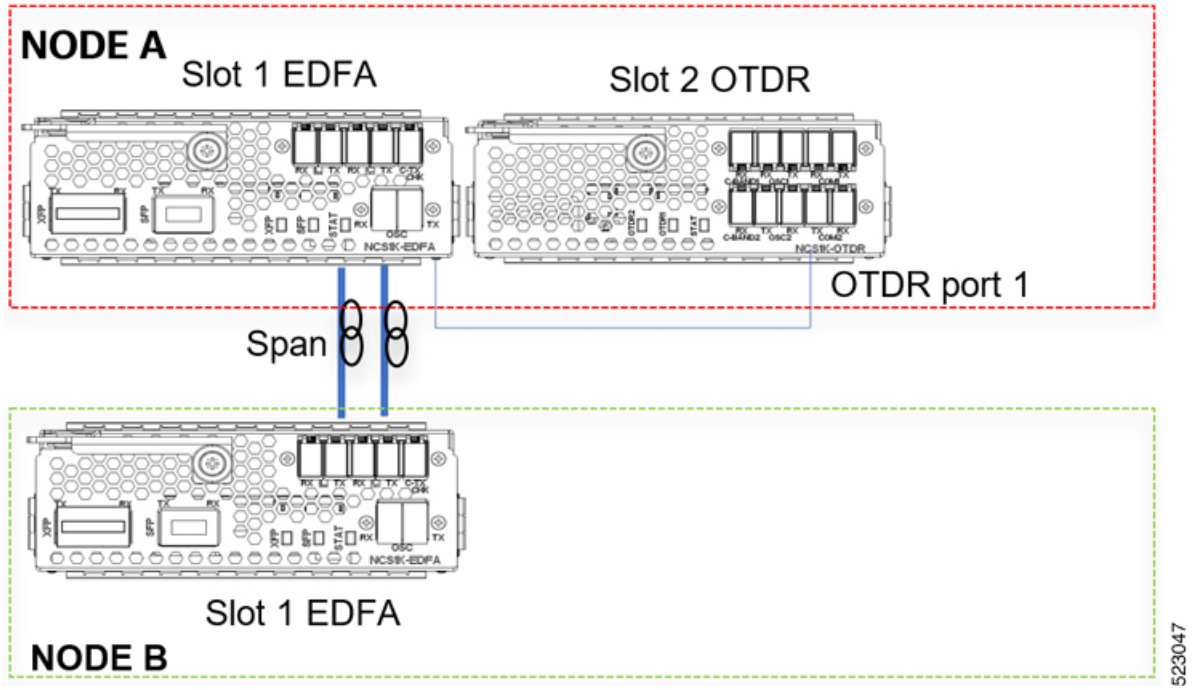
Configure OTDR autoscan for scenario 2

Use this procedure when a single OTDR module is installed in one of the two nodes and connects to one EDFA that faces the fiber span.

Configure the remote node and OTDR autoscan commands for the selected event-based automatic scan scenario.

In scenario 2, one OTDR module is installed in Node A or Node B. The OTDR connects to only one EDFA that faces the fiber span.

Figure 16: Scenario 2 EDFA remote node configuration



Procedure

1. Configure the remote node feature for each EDFA module on Node A and Node B.

   Example

   ```
   Node A:
   hw-module location 0/RP0/CPU0 slot 1 ampli remote-node local-ipv4 <IP Node
   A> remote-ipv4 <IP Node B> remote-slot-id 1

   Node B:
   hw-module location 0/RP0/CPU0 slot 1 ampli remote-node local-ipv4 <IP Node
   B> remote-ipv4 <IP Node A> remote-slot-id 1
   ```

2. Configure OTDR autoscanfor the EDFA connected to the single OTDR module in the same node.

   Example

   ```
   Node A:
   hw-module location 0/RP0/CPU0 slot 1 ampli otdr-autoscan otdr-module-ipv4-addr
    <IP Node A> otdr-slot-id 2 otdr-port-id 1 ampli-far-end-ipv4-addr <IP Node
   A> ampli-far-end-slot-id 1 scan-type AUTO
   ```

3. Configure OTDR autoscan on the single OTDR module.

   Example

   ```
   Node A:
   hw-module location 0/RP0/CPU0 slot 2 otdr port 1 otdr-autoscan
   otdr-module-ipv4-addr <IP Node A> ampli-far-end-ipv4-addr <IP Node A>
   ampli-far-end-slot-id 1 scan-type AUTO
   ```

> **Note**
>
> Both the EDFA and OTDR configurations share the same IP address as there is only one OTDR module connected to single EDFA in the same node.

The event-based OTDR automatic scan configuration is ready for the selected scenario.

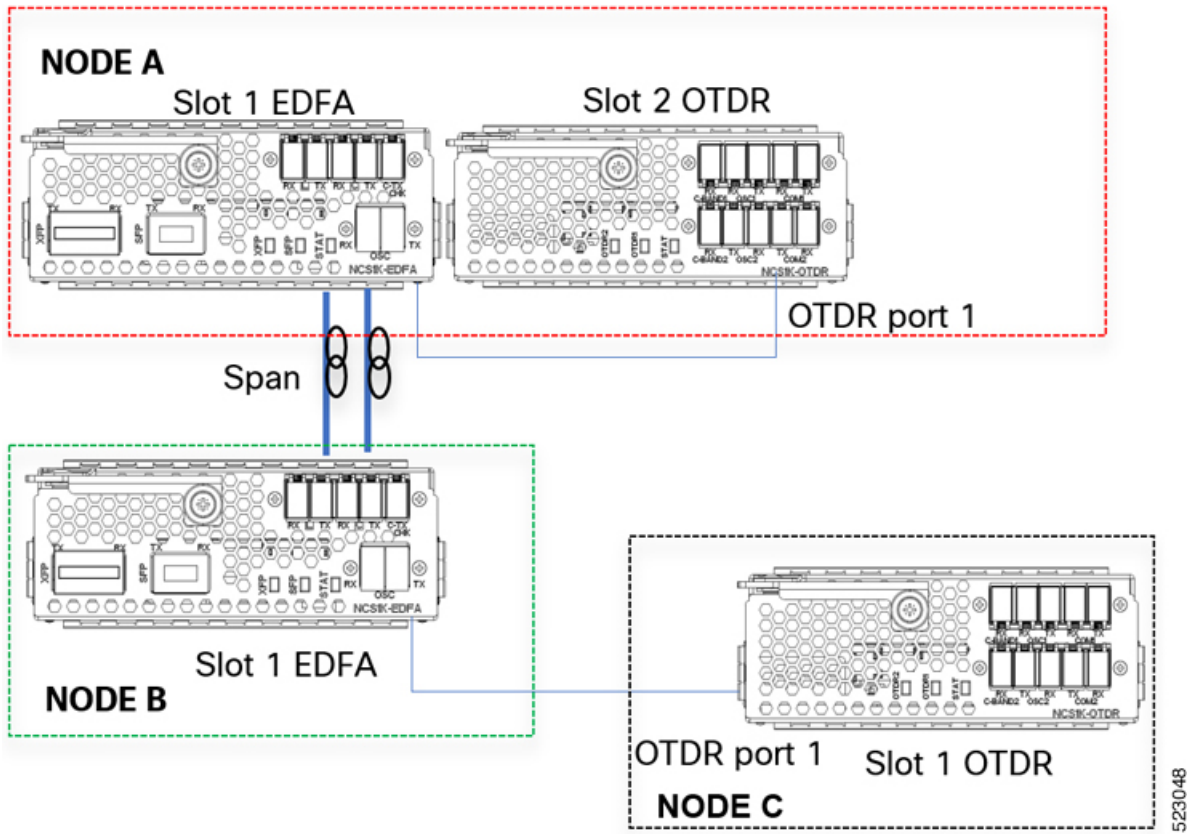
Configure OTDR autoscan for scenario 3

Use this procedure when a single OTDR module is installed in a third node and connects to EDFAs in different nodes.

Configure the remote node and OTDR autoscan commands for the selected event-based automatic scan scenario.

In scenario 3, a single OTDR module is installed in Node C and connects to the EDFA in Node B.

Figure 17: Scenario 3 EDFA remote node configuration



Procedure

1. Configure the remote node feature for each EDFA module on Node A and Node B.

Example

```
Node A:
hw-module location 0/RP0/CPU0 slot 1 ampli remote-node local-ipv4 <IP Node
A> remote-ipv4 <IP Node B> remote-slot-id 1

Node B:
hw-module location 0/RP0/CPU0 slot 1 ampli remote-node local-ipv4 <IP Node
B> remote-ipv4 <IP Node A> remote-slot-id 1
```

2. Configure OTDR autoscan for each EDFA module on Node A and Node B.

Example

```
Node A:
hw-module location 0/RP0/CPU0 slot 1 ampli otdr-autoscan otdr-module-ipv4-addr
 <IP Node A> otdr-slot-id 2 otdr-port-id 12 ampli-far-end-ipv4-addr <IP Node
 B> ampli-far-end-slot-id 1 scan-type AUTO

Node B:
hw-module location 0/RP0/CPU0 slot 1 ampli otdr-autoscan otdr-module-ipv4-addr
 <IP Node C> otdr-slot-id 1 otdr-port-id 12 ampli-far-end-ipv4-addr <IP Node
 A> ampli-far-end-slot-id 1 scan-type AUTO
```

3. Configure OTDR autoscan for each OTDR module on Node A and Node C.

Example

```
Node A:
hw-module location 0/RP0/CPU0 slot 2 otdr port 1 otdr-autoscan
otdr-module-ipv4-addr <IP Node A> ampli-far-end-ipv4-addr <IP Node A>
ampli-far-end-slot-id 1 scan-type AUTO

Node C:
hw-module location 0/RP0/CPU0 slot 1 otdr port 1 otdr-autoscan
otdr-module-ipv4-addr <IP Node C> ampli-far-end-ipv4-addr <IP Node B>
ampli-far-end-slot-id 1 scan-type AUTO
```

The event-based OTDR automatic scan configuration is ready for the selected scenario.

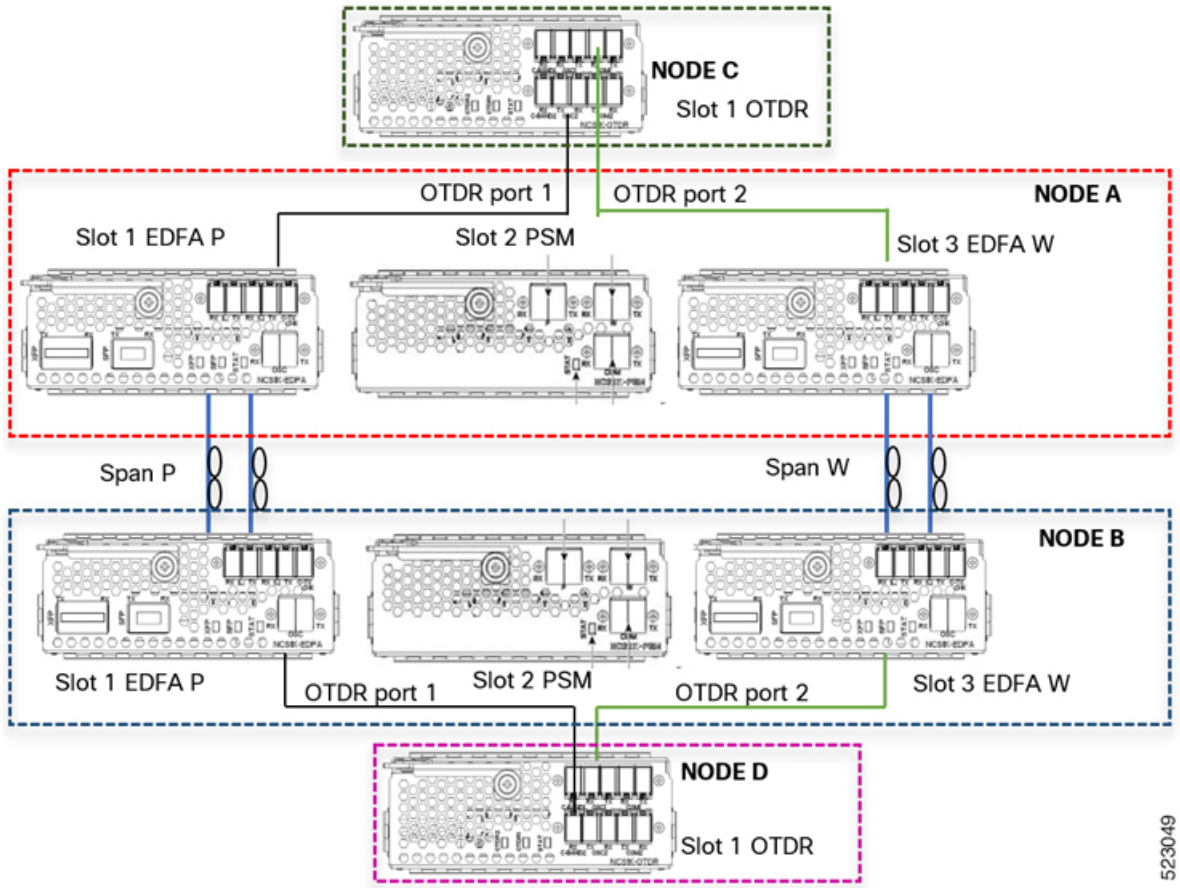
Configure OTDR autoscan for scenario 4

Use this procedure when two OTDR modules are installed in dedicated nodes and each OTDR node connects to its own EDFA node.

Configure the remote node and OTDR autoscan commands for the selected event-based automatic scan scenario.

In scenario 4, OTDR modules are installed in Nodes C and D. Each OTDR node connects to its section-protection EDFA node.

Figure 18: Scenario 4 EDFA remote node configuration



Procedure

1. Configure the EDFA remote node feature for each EDFA module on Node A and Node B.

   Example

```
Node A:
hw-module location 0/RP0/CPU0 slot 1 ampli remote-node local-ipv4 <IP Node
A> remote-ipv4 <IP Node B> remote-slot-id 1
hw-module location 0/RP0/CPU0 slot 3 ampli remote-node local-ipv4 <IP Node
A> remote-ipv4 <IP Node B> remote-slot-id 3

Node B:
hw-module location 0/RP0/CPU0 slot 1 ampli remote-node local-ipv4 <IP Node
B> remote-ipv4 <IP Node A> remote-slot-id 1
hw-module location 0/RP0/CPU0 slot 3 ampli remote-node local-ipv4 <IP Node
B> remote-ipv4 <IP Node A> remote-slot-id 3
```

2. Configure OTDR autoscan for each EDFA module on Node A and Node B.

   Example

```
Node A:
hw-module location 0/RP0/CPU0 slot 1 ampli otdr-autoscan otdr-module-ipv4-addr
 <IP Node C> otdr-slot-id 1 otdr-port-id 1 ampli-far-end-ipv4-addr <IP Node
B> ampli-far-end-slot-id 1 scan-type AUTO
hw-module location 0/RP0/CPU0 slot 3 ampli otdr-autoscan otdr-module-ipv4-addr
```

```
 <IP Node C> otdr-slot-id 1 otdr-port-id 2 ampli-far-end-ipv4-addr <IP Node
B> ampli-far-end-slot-id 3 scan-type AUTO

Node B:
hw-module location 0/RP0/CPU0 slot 1 ampli otdr-autoscan otdr-module-ipv4-addr
 <IP Node D> otdr-slot-id 1 otdr-port-id 1 ampli-far-end-ipv4-addr <IP Node
A> ampli-far-end-slot-id 1 scan-type AUTO
hw-module location 0/RP0/CPU0 slot 3 ampli otdr-autoscan otdr-module-ipv4-addr
 <IP Node D> otdr-slot-id 1 otdr-port-id 2 ampli-far-end-ipv4-addr <IP Node
A> ampli-far-end-slot-id 3 scan-type AUTO
```

3. Configure OTDR autoscan for each OTDR module on Node C and Node D.

Example

```
Node C:
hw-module location 0/RP0/CPU0 slot 1 otdr port 1 otdr-autoscan
otdr-module-ipv4-addr <IP Node C> ampli-far-end-ipv4-addr <IP Node A>
ampli-far-end-slot-id 1 scan-type AUTO
hw-module location 0/RP0/CPU0 slot 1 otdr port 2 otdr-autoscan
otdr-module-ipv4-addr <IP Node C> ampli-far-end-ipv4-addr <IP Node A>
ampli-far-end-slot-id 3 scan-type AUTO

Node D:
hw-module location 0/RP0/CPU0 slot 1 otdr port 1 otdr-autoscan
otdr-module-ipv4-addr <IP Node D> ampli-far-end-ipv4-addr <IP Node B>
ampli-far-end-slot-id 1 scan-type AUTO
hw-module location 0/RP0/CPU0 slot 1 otdr port 2 otdr-autoscan
otdr-module-ipv4-addr <IP Node D> ampli-far-end-ipv4-addr <IP Node B>
ampli-far-end-slot-id 3 scan-type AUTO
```

The event-based OTDR automatic scan configuration is ready for the selected scenario.

Configure OTDR in automatic mode based on events

Use this procedure as a command sequence example when the EDFA and OTDR modules are present on the same near-end and far-end nodes.

Configure the EDFA module and OTDR module autoscan parameters on both the near-end and far-end nodes.

The sample assumes that both the EDFA and OTDR modules are present on the same node.

Procedure

---

1. Configure the EDFA module for OTDR autoscan.

Example

```
configure
hw-module location 0/RP0/CPU0 slot 3 ampli
otdr-autoscan
otdr-module-ipv4-addr 192.0.2.1
otdr-slot-id 2
otdr-port-id 1
ampli-far-end-ipv4-addr 198.51.100.10
ampli-far-end-slot-id 3
```

```
scan-type auto
commit
end
```

Example

```
configure
hw-module location 0/RP0/CPU0 slot 3 ampli
otdr-autoscan
otdr-module-ipv6-addr 2001:DB8:4491:2000::229:144
otdr-slot-id 2
otdr-port-id 1
ampli-far-end-ipv6-addr 2001:DB8:4491:2000::228:145
ampli-far-end-slot-id 3
scan-type auto
commit
end
```

2. Configure the OTDR module for OTDR autoscan.

Example

```
configure
hw-module location 0/RP0/CPU0 slot 2 otdr port 1
otdr-autoscan
otdr-module-ipv4-addr 192.0.2.1
ampli-far-end-ipv4-addr 198.51.100.10
ampli-far-end-slot-id 3
scan-type auto
commit
end
```

Example

```
configure
hw-module location 0/RP0/CPU0 slot 2 otdr port 1
otdr-autoscan
otdr-module-ipv6-addr 2001:DB8:4491:2000::229:144
ampli-far-end-ipv6-addr 2001:DB8:4491:2000::228:145
ampli-far-end-slot-id 3
scan-type auto
commit
end
```

The sample EDFA and OTDR autoscan command sequence is complete.

IPv6 support for OTDR auto scan

This topic explains how IPv6 support extends OTDR automatic scan to Cisco NCS 1001 nodes that use IPv6 management addresses.

Starting with Release 7.10.1, you can use IPv6 addresses to perform OTDR automatic scans between Cisco NCS 1001 nodes that support IPv6 and have IPv6 addresses configured on their management interfaces.

Feature History

Table 22: Feature history

Feature name	Release information	Description
IPv6 support for OTDR auto scan	Cisco IOS XR Release 7.10.1	OTDR auto scan can be enabled on Cisco NCS 1001 nodes configured with IPv6 addresses, which lets OTDR auto scan work on IPv4 and IPv6 nodes.

To configure OTDR auto scan using IPv6 addresses, replace **local-ipv4** and **remote-ipv4** with **local-ipv6** and **remote-ipv6**. Also, update the corresponding IPv4 address variables with IPv6 address variables in the relevant commands in the section OTDR measurement in automatic mode based on events.

Note

Configure OTDR auto scan with either IPv4 or IPv6 addresses. Do not use both address types at the same time in the configuration.

Limitation

OTDR measurement with IPv6 is not supported on OSC management interfaces. Even when OSPFv3 is used, neighbor discovery returns the IPv4 router ID instead of the IPv6 router ID. As a result, IPv6 addressing is difficult to resolve automatically.

TCP/IP ACLs for span loss and OTDR autoscan traffic

This section explains how optional TCP/IP access control lists (ACLs) restrict span loss calculation and OTDR autoscan traffic between Cisco NCS 1001 nodes.

TCP/IP ACLs for span loss and OTDR autoscan traffic are optional security controls that

- control bidirectional traffic between Cisco NCS 1001 nodes,
- restrict traffic on TCP port 30000 for span loss calculation and TCP port 30010 for OTDR autoscan, and
- limit node-to-node communication to the management network where the Cisco NCS 1001 nodes are located.

The span loss calculation and OTDR autoscan features operate without ACL configuration. In production environments, configure ACLs to restrict the communication path to the local node private subnet or the management network.

ACL traffic requirements

Permit both ingress and egress traffic on TCP ports 30000 and 30010 to support bidirectional communication between nodes.

Table 23: Port usage for span loss and OTDR autoscan

TCP port	Application traffic
30000	Span loss calculation data
30010	OTDR autoscan data

Table 24: ACL address roles

Traffic direction	Source address	Destination address
Ingress	Remote node	Local management address
Egress	Local node	Remote node

Important

Permit both ingress and egress traffic on ports 30000 and 30010 for proper bidirectional communication between nodes.

Configure span loss and OTDR autoscan ACLs

Use this procedure to configure IPv4 and IPv6 ACLs and apply them to the management interface for span loss and OTDR autoscan traffic.

Restrict bidirectional span loss calculation and OTDR autoscan traffic between Cisco NCS 1001 nodes to the required management subnets.

Before you begin

Identify the local node subnet, remote node subnet, wildcard masks for IPv4, prefix lengths for IPv6, and the management interface where the ACLs must be applied.

Note

ACL configuration is optional. Span loss calculation and OTDR autoscan can operate without ACL restrictions, but ACLs are recommended in production environments to enhance network security. Allow TCP ports 30000 and 30010 in both ingress and egress directions.

Follow these steps to configure span loss and OTDR autoscan ACLs:

Procedure

1. Create the IPv4 ACL and permit traffic on TCP ports 30000 and 30010.

Example

```
RP/0/RP0/CPU0:ios(config)# ipv4 access-list span-loss-otdr-acl
RP/0/RP0/CPU0:ios(config-ipv4-acl)# permit tcp <remote-node-subnet>
<wildcard-mask> <local-node-subnet> <wildcard-mask> eq 30000
RP/0/RP0/CPU0:ios(config-ipv4-acl)# permit tcp <remote-node-subnet>
<wildcard-mask> <local-node-subnet> <wildcard-mask> eq 30010
RP/0/RP0/CPU0:ios(config-ipv4-acl)# permit tcp <local-node-subnet>
<wildcard-mask> <remote-node-subnet> <wildcard-mask> eq 30000
RP/0/RP0/CPU0:ios(config-ipv4-acl)# permit tcp <local-node-subnet>
<wildcard-mask> <remote-node-subnet> <wildcard-mask> eq 30010
```

This example permits traffic within the 192.0.2.0/24 subnet.

```
RP/0/RP0/CPU0:ios(config)# ipv4 access-list span-loss-otdr-acl
RP/0/RP0/CPU0:ios(config-ipv4-acl)# permit tcp 192.0.2.0 0.0.0.255 192.0.2.0
 0.0.0.255 eq 30000
RP/0/RP0/CPU0:ios(config-ipv4-acl)# permit tcp 192.0.2.0 0.0.0.255 192.0.2.0
 0.0.0.255 eq 30010
```

2. Create the IPv6 ACL and permit traffic on TCP ports 30000 and 30010.

   Example

```
RP/0/RP0/CPU0:ios(config)# ipv6 access-list span-loss-otdr-acl-v6
RP/0/RP0/CPU0:ios(config-ipv6-acl)# permit tcp
<remote-node-subnet>/<prefix-length> <local-node-subnet>/<prefix-length> eq
30000
RP/0/RP0/CPU0:ios(config-ipv6-acl)# permit tcp
<remote-node-subnet>/<prefix-length> <local-node-subnet>/<prefix-length> eq
30010
RP/0/RP0/CPU0:ios(config-ipv6-acl)# permit tcp
<local-node-subnet>/<prefix-length> <remote-node-subnet>/<prefix-length> eq
30000
RP/0/RP0/CPU0:ios(config-ipv6-acl)# permit tcp
<local-node-subnet>/<prefix-length> <remote-node-subnet>/<prefix-length> eq
30010
```

   This example permits traffic within the 2001:DB8::/32 subnet.

```
RP/0/RP0/CPU0:ios(config)# ipv6 access-list span-loss-otdr-acl-v6
RP/0/RP0/CPU0:ios(config-ipv6-acl)# permit tcp 2001:DB8:4491:2000::/64
2001:DB8:4491:2000::/64 eq 30000
RP/0/RP0/CPU0:ios(config-ipv6-acl)# permit tcp 2001:DB8:4491:2000::/64
2001:DB8:4491:2000::/64 eq 30010
```

3. Apply the ACL to the management interface.

   After creating the ACL, apply it to the appropriate management interface to control bidirectional span loss calculation and OTDR autoscan traffic between nodes. Apply the ACL in both ingress and egress directions.

   This example applies the IPv4 ACL to **MgmtEth0/RP0/CPU0/0**.

```
RP/0/RP0/CPU0:ios# configure terminal
RP/0/RP0/CPU0:ios(config)# interface MgmtEth0/RP0/CPU0/0
RP/0/RP0/CPU0:ios(config-if)# ipv4 access-group span-loss-otdr-acl ingress
RP/0/RP0/CPU0:ios(config-if)# ipv4 access-group span-loss-otdr-acl egress
RP/0/RP0/CPU0:ios(config-if)# commit
RP/0/RP0/CPU0:ios(config-if)# end
```

   This example applies the IPv6 ACL to **MgmtEth0/RP0/CPU0/0**.

```
RP/0/RP0/CPU0:ios# configure terminal
RP/0/RP0/CPU0:ios(config)# interface MgmtEth0/RP0/CPU0/0
RP/0/RP0/CPU0:ios(config-if)# ipv6 access-group span-loss-otdr-acl-v6 ingress
RP/0/RP0/CPU0:ios(config-if)# ipv6 access-group span-loss-otdr-acl-v6 egress
```

```
RP/0/RP0/CPU0:ios(config-if)# commit
RP/0/RP0/CPU0:ios(config-if)# end
```

The management interface permits span loss calculation and OTDR autoscan traffic only through the configured IPv4 and IPv6 ACL rules.

Configure OTDR in expert mode

Use this procedure to configure expert mode OTDR scan parameters when automatic adjustment is not used for the selected port and direction.

Configure expert mode when you must control capture length, offset, resolution, sensitivity, measurement time, pulse width, span length, and relative thresholds.

Expert mode does not run a training phase and does not automatically adjust scan parameters.

Procedure

1. Enter configuration mode.

   Example

   ```
   configure
   ```

2. Use the **hw-module** command to enter OTDR expert mode configuration for the slot, port, and direction.

   hw-module location 0/RP0/CPU0 slot *slot-number* **otdr port** *port-number* **direction** *direction* **mode-expert**

   Example

   ```
   hw-module location 0/RP0/CPU0 slot 2 otdr port 1 direction tx mode-expert
   ```

3. Configure the expert mode scan parameters.

   For parameter descriptions, ranges, and defaults, see OTDR expert-mode parameters.

   Example

   ```
   pulse-width 10
   span-length 1
   measure-time 180
   capture-length 1
   capture-offset 0
   fiber-resolution 4
   loss-sensitivity 4
   reflection-sensitivity -300
   loss-relative-threshold 20
   reflection-relative-threshold 20
   ```

4. Commit the configuration and exit configuration mode.

Example

```
commit
end
```

OTDR expert mode is configured for the selected port and direction.

OTDR expert mode parameters

This topic lists parameter descriptions, valid ranges, and default values for OTDR expert mode configuration, including capture, resolution, sensitivity, and span settings.

Use these values when configuring OTDR expert mode.

Table 25: OTDR expert mode parameters

Parameter	Description	Range	Default
capture-length (km)	Distance of the measurement endpoint.	1 to 150	100
capture-offset (km)	Start point of the measurement.	0 to 150	0
fiber-resolution (m)	Distance between measurement steps.	0 to 100	25
loss-sensitivity (in 0.1 dB)	Limit under which the loss is not considered a real loss.	4 to 50	6
measure-time (sec)	Time required to perform the complete optical scan.	1 to 360	180
pulse-width (ns)	Pulse duration during the measurement.	8 to 100,000	1000
reflection-sensitivity (in 0.1 dB)	Limit under which the reflection is not considered a real reflection.	-400 to -140	-300
span-length (km)	Length of span.	1 to 150	100
loss-relative-threshold (in 0.1 dB)	Threshold to compare the OTDR loss value plus the relative loss threshold with the baseline value.	1 to 300	2
reflection-relative-threshold (in 0.1 dB)	Threshold to compare the OTDR reflection value plus the relative reflection threshold with the baseline value.	1 to 300	2

> **Note**
>
> From Release 7.5.1, the plus sign labels in positive range values are removed in the Cisco NCS 1001 CLI help description.

Start OTDR measurement in expert mode

Use this procedure to start an OTDR expert mode scan for a selected slot, port, and direction after expert mode parameters are configured.

Start expert measurement after OTDR parameters are configured in expert mode.

The scan continues in the background after the command starts the action.

Procedure

Start the OTDR expert mode scan.

hw-module slot *slot-number* **otdr port** *port-number* **direction** *direction* **scan expert**

Example

```
hw-module slot 3 otdr port 1 direction tx scan expert
```

The system displays the message "Otdr action will continue in the background."

What to do next

To see the measurement status, use the **show hw-module slot** *slot-number* **otdr status** command.

Display the OTDR measurement list

Use this procedure to display available OTDR measurements, identify the SOR file for each scan, and inspect detailed output for a selected measurement position.

Review the list to identify available OTDR measurements prior to retrieving a specific scan output by position number.

The command lists saved OTDR measurements along with the SOR filename associated with each measurement.

Procedure

1. Use the **show hw-module** command to display the list of OTDR measurements.

   show hw-module slot *slot-number* **otdr scan**

   Example

```
show hw-module slot 3 otdr scan

  # | otdr# | Rx/Tx | Mode | Date/Time       | SOR filename
----+-------+-------+------+-----------------+--------------------------------------
```

```
  0 |   1   |  Tx   | AUTO | 20180504-092810 |
ncs1001_slot3_otdr1_TX.20180504-092810.sor
  1 |   1   |  Tx   | AUTO | 20180504-114239 |
ncs1001_slot3_otdr1_TX.20180504-114239.sor
```

Example
Table 26: OTDR measurement list fields

Field	Description
#	Number of OTDR measurements
otdr#	Port where the OTDR measurement was performed
Rx/Tx	Direction of OTDR measurement
Mode	Type of scan, automatic or expert
Date/Time	Date and time of OTDR measurement
SOR filename	Name of the file that contains measurement data

2. Use the **show hw-module** command to display scan data for a measurement position.

   show hw-module slot *slot-number* **otdr scan** *position-number*

   Example

```
show hw-module slot 3 otdr scan 0

Measurement on: 20180504-151351
OTDR device number: 1
Scan direction: Tx
Scan mode: Auto
Directory location: /harddisk:/otdr
File name: ncs1001_slot3_otdr1_TX.20180504-151351.sor
Total ORL: 29.86 dB
Distance (estimate): 38.996 km
Total number of event detected: 3

Event# | TYPE         | LOCATION(km) | ACCURACY(m) | MAGNITUDE(dB) |
TH-CROSSING
-------+--------------+--------------+-------------+---------------+------------

   0   | LOSS         |    0.000     |    5.62     |    -1.09      | NO
   1   | LOSS         |   23.840     |  114.06     |    -0.44      | NO
   2   | END OF FIBER |   38.996     |  249.00     |               | NO
```

Example
Table 27: OTDR scan detail fields

Field	Description
OTDR device number	Port number
Scan direction	Direction of scan

Field	Description
Scan mode	Mode of scan, automatic or expert
Directory location	Location where the SOR file is stored
File name	Name of the SOR file
Total ORL	Optical return loss in dB
Distance (estimate)	Distance in km
Total number of event detected	Events detected during the OTDR measurement
Event#	Event number
TYPE	Event type, such as LOSS or END OF FIBER
LOCATION(km)	Location of the event in the span
ACCURACY(m)	Accuracy of the event location in the span
MAGNITUDE(dB)	Loss magnitude of the event
TH-CROSSING	loss-abs-threshold value

The command output shows the stored OTDR measurements for the selected scan details.

Stop OTDR measurement

Use this procedure to stop an OTDR measurement that is running in automatic or expert mode and verify that the scan is stopped.

Stop an OTDR measurement when the current scan must be canceled.

The same **abort** command applies to automatic and expert modes.

Procedure

1. Stop the OTDR scan for the selected slot and port.

   hw-module slot *slot-number* **otdr port** *port-number* **scan abort**

   Example

   ```
   hw-module slot 3 otdr port 1 scan abort
   ```

2. Use the **show hw-module** command to display OTDR status to verify the abort state.

   Example

   ```
   show hw-module slot 3 otdr status

   Port | Rx/Tx | Date/Time      | Training | OTDR Measurement | Next scan (min)
   ```

```
-----+-------+-----------------+----------+------------------+----------------

  1  |  Tx   | 20190927-102727 | ABORTED  | UNKNOWN          | 0
```

Example

```
show hw-module slot 3 otdr status

Port | Rx/Tx | Date/Time       | Training | OTDR Measurement
-----+-------+-----------------+----------+-----------------
  1  |  Tx   | 20180503-181159 | UNKNOWN  | ABORTED
```

The selected OTDR measurement is stopped.

Display OTDR photodiode power levels

Use this procedure to display photodiode power values and the logical ports associated with the OTDR module physical ports during controller verification.

Display OTS controller summaries when you must view OTDR photodiode power levels and logical port associations.

Procedure

Use the **show controllers ots** command to display the OTDR OTS controller summary.

show controllers ots *rack/slot/instance/port* **summary**

Example

```
RP/0/RP0/CPU0:IOS#show controllers ots 0/2/0/* summary
Tue Jan 23 13:49:41.604 CET

Port       Type  Status  TX Power  TX Total Power  RX Power  RX Total Power
Ots0_2_0_0 Com   N/A     -40.00    Unavailable     -40.00    Unavailable
Ots0_2_0_1 Com   N/A       0.60    Unavailable     -16.60    Unavailable
Ots0_2_0_2 Osc   N/A     -17.60    Unavailable       1.30    Unavailable
Ots0_2_0_3 Com   N/A     -40.00    Unavailable     -40.00    Unavailable
Ots0_2_0_4 Com   N/A       0.20    Unavailable     -22.20    Unavailable
Ots0_2_0_5 Osc   N/A     -23.60    Unavailable       1.30    Unavailable
```

The output displays photodiode power values and logical ports for the OTDR module.

What to do next

> **Note**
>
> Parameters such as Status, RX Total Power, TX Total Power, RX Attenuation, TX Attenuation, Amplifier Gain, and Amplifier Tilt values on the corresponding OTS controller are not available for the OTDR card.

OTDR machine learning events

This topic provides reference details for OTDR machine learning feature history and event classifications shown in scan output when machine learning is enabled.

Use this reference to identify the OTDR machine learning feature changes and the event types that can appear in scan output.

Table 28: Feature history

Feature name	Release information	Description
OTDR machine learning model	Cisco IOS XR Release 7.3.2	The OTDR machine learning model is updated to Version 4 to improve event recognition performance.

Table 29: Feature history

Feature name	Release	Description
OTDR machine learning	Cisco IOS XR Release 7.3.1	Machine learning can be enabled on the OTDR card. If enabled, the OTDR measurement provides additional event information about the fiber.

When the machine learning parameter is set to one, the scan output can display these event types:

Table 30: Machine learning event types

Event	Description
FIBER TERMINATED	The fiber is correctly plugged in to the far-end node.
OPEN CONNECTOR	The fiber is not correctly plugged in to the far-end node.
FACE PLATE	The beginning of the fiber.
PASS THROUGH	The connection between two fibers.

Enable machine learning on the OTDR card

Use this procedure to enable machine learning on an OTDR card so scan output can include additional fiber-event classifications for the selected direction.

Enable ML for the selected OTDR slot, port, and direction in configuration mode.

When ML is enabled, OTDR scan output includes additional event classifications for the fiber span.

Procedure

Use the **hw-module location** command to enable ML on the selected OTDR card, port, and direction.

hw-module location *location* **slot** *slot-number* **otdr port** *port-number* **direction** *direction* **ml-enabled 1**

Example

```
hw-module location 0/RP0/CPU0 slot 1 otdr port 1 direction tx ml-enabled 1
```

Machine learning is enabled for the selected OTDR card, port, and direction.

View scan output with machine learning enabled

Use this procedure to view OTDR scan output after machine learning is enabled and interpret the ML event classification for the fiber span.

View scan output by position number after ML is enabled on the OTDR card.

The ML graph analysis section in the command output shows additional event classifications.

Procedure

1. Use the **show hw-module** command to display the scan output for position 0.

   Example

```
RP/0/RP0/CPU0:156-ML#show hw-module slot 1 otdr scan 0
Measurement on: 20200916-171424
OTDR device number: 1
Scan direction: Tx
Scan mode: Auto
Directory location: /harddisk:/otdr
File name: 156-ML_ncs1001_slot1_otdr1_TX.20200916-171424.sor
Total ORL: 31.37 dB
Distance (estimate): 61.275 km
High Reflection Location: 0.00 km
Total number of event detected: 2

ML graph analysis:
Total number of event detected: 3
Event# | TYPE           | LOCATION(km)
-------+----------------+-------------
   A   | FACE PLATE     | 0.001
   B   | PASS THROUGH   | 11.876
   C   | OPEN CONNECTOR | 61.285
```

   The **OPEN CONNECTOR** event type in the output indicates that the fiber span is not connected to a far-end node.

2. Use the **show hw-module** command to display the scan output for another measurement position.

Example

```
RP/0/RP0/CPU0:156-ML#show hw-module slot 1 otdr scan 6
Measurement on: 20200917-140822
OTDR device number: 1
Scan direction: Tx
Scan mode: Auto
Directory location: /harddisk:/otdr
File name: 156-ML_ncs1001_slot1_otdr1_TX.20200917-140822.sor
Total ORL: 31.29 dB
Distance (estimate): 61.279 km
High Reflection Location: 0.00 km
Total number of event detected: 1

ML graph analysis:
Total number of event detected: 3
Event# | TYPE             | LOCATION(km)
-------+------------------+-------------
   A   | FACE PLATE       | 0.001
   B   | PASS THROUGH     | 11.876
   C   | FIBER TERMINATED | 61.622
```

The **FIBER TERMINATED** event type in the output indicates that the fiber span is properly connected to a far-end node.

5 Configure Performance Monitoring

Topics:

Explains how to set optical controller thresholds, collect performance data at supported intervals, and view current or historical counters for troubleshooting.

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 the current and historical PM counters for the various controllers in several intervals.

PM for optical parameters include laser bias current, transmit and receive optical power, mean polarization mode dispersion, accumulated chromatic dispersion, and received optical signal-to-noise ratio (OSNR). These parameters simplify troubleshooting operations and enhance data that can be collected directly from the equipment.

Performance monitoring parameters

This topic explains how performance monitoring parameters help service providers collect controller data, set thresholds, and identify optical performance issues earlier.

Performance monitoring (PM) parameters are optical controller measurements and thresholds that service providers use to gather, store, report, and troubleshoot controller performance data.

Optical performance monitoring parameters

PM for optical parameters includes measurements that support controller troubleshooting and equipment-level data collection.

- Laser bias current
- Optical power transmitted (OPT)
- Optical power received (OPR)
- Mean polarization mode dispersion
- Accumulated chromatic dispersion
- Received optical signal-to-noise ratio (OSNR)

Configure performance monitoring parameters

Use this procedure to set report and threshold parameters for optical transport section controller performance monitoring intervals on Cisco NCS 1001 and commit the configuration.

Configure performance monitoring parameters to control how the device reports optical transport section (OTS) controller data and threshold crossing alerts.

The configuration applies to OTS controller PM intervals such as 30 seconds, 15 minutes, and 24 hours.

Procedure

1. Enter global configuration mode.

   Example

   ```
   configure
   ```

2. Use the **controller** *controller-type* command to configure the PM parameters for the OTS controllers.

   controller *controller-type Rack/Slot/Instance/Port* **pm 15-min 24-hour 30-sec ots report threshold opr opt** *value*

   Example

   This example enables the maximum threshold crossing alert (TCA) for optical power received (OPR) on OTS controller 0/1/0/0 in 24-hour intervals.

   ```
   configure
   controller ots 0/1/0/0 pm 24-hour ots report opr max-tca enable
   commit
   ```

Example

This example sets the maximum TCA for OPR on OTS controller 0/1/0/0 in 24-hour intervals.

```
configure
controller ots 0/1/0/0 pm 24-hour ots threshold opr max 4000
commit
```

3. Commit the configuration.

Example

```
commit
```

The performance monitoring parameters for the OTS controllers are configured.

What to do next

For details about PM collection intervals, see Performance monitoring collection intervals.

Performance monitoring collection intervals

This topic provides the sampling intervals and jitter values that the performance monitoring collector uses when it gathers controller data from equipment.

Use these values to understand how often the PM collector gathers controller data.

Table 31: PM collection intervals

PM interval	Samples	Jitter provision
30 seconds	30 samples	6 seconds
15 minutes	32 samples	45 seconds
24 hours	1 sample	45 seconds

The jitter provision compensates for computation delays that occur when the data provider PM engine collects data.

View performance monitoring parameters

Use this procedure to display current or historical optical transport section controller performance monitoring counters for supported intervals, including 10 second flex-bin buckets.

Check current and historical optical controller counters using PM parameters.

Table 32: Feature History

Feature Name	Release Information	Feature Description
10sec PM buckets	Cisco IOS XR Release 7.3.1	Performance monitoring parameters for the OTS and OTS OCH controllers in 10-second intervals are available. This new bucket for performance monitoring allows you to gather, store, and report performance data with higher granularity. Commands modified: ▪ controller ots ▪ show controllers

Procedure

Use the **show controllers** command to display the current or historical PM parameters.

show controllers *controller-type Rack/Slot/Instance/Port* **pm current history 15-min 24-hour 30-sec flex-bin optics** *lane-number* **bucket** *bucket-number*

The **flex-bin** option corresponds to a 10-second bucket.

Specify the **bucket** option when you use **pm history**.

Example

This example displays current PM parameters of the Optics controller in 15-minute intervals.

```
RP/0/RP0/CPU0:ios# show controllers ots 0/1/0/0 pm current 15-min optics 1
Thu Mar 16 15:07:21.093 CET

Optics in the current interval [15:00:00 - 15:07:21 Thu Mar 16 2017]

Optics current bucket type : Valid
MIN AVG MAX Threshold TCA Threshold TCA
(min) (enable) (max) (enable)
LBC[% ] : 0.2 4.5 18.6 0.0 NO 0.0 NO
OPT[dBm] : -40.00 -0.40 8.00 -50.00 NO 10.00 NO
OPR[dBm] : -17.52 -17.01 -16.90 -50.00 NO 10.00 NO

Last clearing of "show controllers OPTICS" counters never
```

The command output displays the selected current or historical PM counters.

What to do next

For details about bucket ranges and bucket behavior, see Performance monitoring bucket values.

Performance monitoring bucket values

This topic provides bucket values for performance monitoring time intervals and explains how to verify interval timestamps in command output during review.

Use bucket values to select historical PM intervals and confirm that command output matches the expected time interval.

This table lists bucket values for each performance monitoring time interval.

Table 33: Bucket values for each PM interval

PM time interval	Bucket value
15 minutes	1 to 32
24 hours	no value
30 seconds	1 to 30
flex-bin (10 seconds)	1

Bucket interval verification

The **show controllers** command might occasionally return the previous bucket. Verify the timestamp and interval in the command output during the review of historical PM data.

This example shows a query that returned the earlier 30-second bucket.

```
RP/0/RP0/CPU0:ios# show controllers optics 0/1/0/4 pm history 30-sec optics 1
 bucket 5
Mon May 29 15:02:05.697 CEST

Optics in interval 1 [15:01:00 - 15:01:30 Mon May 29 2017]

Optics history bucket type : Valid
              MIN       AVG       MAX
LBC[% ]     : 335.3     341.3     352.3
OPT[dBm]    : 1.90      2.01      2.10
OPR[dBm]    : -12.20    -12.16    -12.10

Last clearing of "show controllers OPTICS" counters never
```

6 USB Automount

Topics:

Explains how to access a USB device as the disk2: file system, mount it when needed, copy files, and unmount it safely before removal.

USB automount

This topic explains how USB automount lets you read from and write to files on supported Cisco NCS 1000 devices without manually mounting a USB device.

USB automount is a file system feature that mounts a supported USB device automatically so that you can access the device as the `disk2:` file system.

USB automount behavior

USB automount behavior depends on the device and the virtual machine where the USB device is used.

Table 34: USB automount behavior by device

Device	Behavior
Cisco NCS 1002	When you insert a USB device, the device is automatically mounted in sysadmin-vm with read and write permissions and remains unmounted in Cisco IOS XR by default. Automatic mounting in sysadmin-vm is supported only when the USB file system is FAT or FAT32.
Cisco NCS 1001	The USB device is automatically mounted in both sysadmin-vm and Cisco IOS XR.

Mount the USB device in sysadmin-vm

Use this procedure to mount the USB device in sysadmin-vm when the device is unmounted and you need to access files through the disk2: file system.

Mount the USB device to restore file access from sysadmin-vm before you read from or write to the device.

The USB device is usually mounted automatically. Use this procedure only when you must mount the device again after an unmount operation.

Procedure

Mount the USB device in sysadmin-vm.

Use the **usb device operation mount** command.

Example

```
sysadmin-vm:0_RP0#usb device operation mount
Fri Jul 13 09:26:00.821 UTC success usb mounted
```

The USB device is mounted in sysadmin-vm.

You can access the USB device as the `disk2:` file system.

Mount the USB device in Cisco IOS XR

Use this procedure to mount the USB device in Cisco IOS XR when the device is unmounted and you need to access files through disk2:.

Mount the USB device to restore file access from Cisco IOS XR before you read from or write to the device.

Use this procedure only when you must mount the USB device again after an unmount operation.

Procedure

Mount the USB device in Cisco IOS XR.

Use the **unmount disk2: undo** command.

Example

```
RP/0/RP0/CPU0:ios#unmount disk2: undo
Fri Jul 13 14:56:34.326 IST
disk2: mounted successfully.
```

The USB device is mounted in Cisco IOS XR.

You can access the USB device as the `disk2:` file system.

Copy files to the USB device

Use this procedure to copy a file to the mounted USB device from sysadmin-vm and confirm that the file is available in the disk2: file system.

Copy files to the USB device when you must save logs, archives, or other files outside the device storage.

Before you begin

Mount the USB device before you copy files to it.

Procedure

1. Copy the file to the USB device.

   Use the **scp** command and set the destination to `/disk2\:`.

   Example

   ```
   [sysadmin-vm:0_RP0:~/showtech]$scp
   showtech-envmon-admin-2018-Jul-04.171400.IST.tgz /disk2\:
   ```

2. Change to the USB device directory.

   Use the **cd /disk2\:** command.

   Example

   ```
   [sysadmin-vm:0_RP0:~/showtech]$cd /disk2\:
   ```

3. List the directory contents.

   Use the **ls -lrt** command.

Example

```
[sysadmin-vm:0_RP0:/disk2:]$ls -lrt
total 122424
drwxr-xr-x 2 root root      8192 Jul 12  2017 System Volume Information
drwxr-xr-x 2 root root      8192 Jun 11 16:16 boot
drwxr-xr-x 3 root root      8192 Jun 11 16:17 EFI
-rwxr-xr-x 1 root root 125306880 Jul 10 13:50 calvVarLog.tar
-rwxr-xr-x 1 root root     23023 Jul 13 05:23
showtech-envmon-admin-2018-Jul-04.171400.IST.tgz
```

The copied file appears in the USB device directory.

Unmount the USB device from sysadmin-vm

Use this procedure to unmount the USB device from sysadmin-vm before you remove the device from a Cisco NCS 1000 device.

Unmount the USB device from sysadmin-vm to complete file system operations before you remove the device.

Procedure

Unmount the USB device from sysadmin-vm.

Use the **usb device operation unmount** command.

Example

```
sysadmin-vm:0_RP0#usb device operation unmount
Fri Jul 13 09:25:24.531 UTC success usb unmounted
```

The USB device is unmounted from sysadmin-vm.

Unmount the USB device from Cisco IOS XR

Use this procedure to unmount the USB device from Cisco IOS XR before you remove the device from a Cisco NCS 1000 device.

Unmount the USB device from Cisco IOS XR to complete file system operations before you remove the device.

Procedure

Unmount the USB device from Cisco IOS XR.

Use the **unmount disk2:** command.

Example

```
RP/0/RP0/CPU0:ios#unmount disk2:
Fri Jul 13 14:56:46.393 IST
disk2: unmounted successfully.
```

The USB device is unmounted from Cisco IOS XR.

7 Fault Profiles

Topics:

Defines custom fault profiles to adjust default severity levels for data path alarms across system, slot, and port levels. This functionality provides granular control over fault reporting, allowing administrators to prioritize and manage system alerts according to specific network infrastructure needs.

Table 35: Feature History

Feature Name	Release Information	Feature Description
Fault Profiles	Cisco IOS XR Release 7.3.1	This feature allows you to create a fault profile for faults on the system or on the line card. Each fault profile can contain one or more faults with user-defined severities. Commands added: ▪ fault-profile ▪ fault-profile apply

Fault profiles

This topic explains how fault profiles change default fault severities for system, node, slot, and port scopes so that generated faults use the severity values that match your operational requirements.

A fault profile is a user-defined fault configuration that

- contains one or more fault identifiers with assigned severities,
- overrides the default severity for matching faults when the profile is applied, and
- uses precedence from the most specific scope to the least specific scope.

The default fault list captures all the fault types generated by the system and the default severity for each fault type. When no fault profile is defined or applied, the system uses the default severity value.

Fault profile precedence starts at the most specific scope. Port-level profiles have the highest precedence, and system-level profiles have the lowest precedence.

Severity levels

Fault profiles support these severity levels:

- Critical
- Major
- Minor
- Non-Faulted
- Non-Reported

Fault profile actions

You can use fault profiles to

- create or delete a fault profile,
- add alarms to a fault profile,
- remove alarms from a fault profile, and
- change the severity of an alarm in an existing fault profile.

Fault profile limitations

This topic explains the limits for fault profile support, profile count, and profile assignment. Use this information to plan alarm severity changes before you configure a profile.

Use these limitations to decide whether fault profiles apply to your alarm management design.

Supported scope and profile limits

These limitations apply to fault profiles:

- Fault profiling is available only for data path alarms. Supported alarms include Ethernet, generic framing procedure (GFP), optics, optical transport section (OTS), SDH, SONET, G.709, and Common Public Radio Interface (CPRI).
- You can create a maximum of 61 profiles.
- You can apply only one fault profile at each node level or port level.

Configure a fault profile

Use this procedure to create a fault profile, assign one or more alarm severities, and apply the profile at the port, slot, or node level.

Use a fault profile when a fault requires a severity that differs from the default system profile.

The **fault-profile** command creates the profile, and the **fault-profile apply** command attaches the profile to the required scope.

The *severity-level* value for **sas** and **nsas** can be **CRITICAL**, **MAJOR**, **MINOR**, **NONFAULTED**, or **NONREPORTED**.

For each *fault-type*, the node supports a list of *fault-name* values that correspond to alarms that the node can raise. For example, **HW_OTS** supports **OTS_AS_MT**, **OTS_APC_RUNNING**, **OTS_SWITCH_TO_PROTECT**, **OTS_APC_CONFIG_MISMATCH**, **OTS_APC_DISABLED**, **OTS_AUTO_POW_RED**, **OTS_AUTO_LASER_SHUT**, **OTS_AMPLI_GAIN_HIGH**, **OTS_AMPLI_GAIN_LOW**, **OTS_RX_LOC**, **OTS_RX_LOS_P**, **OTS_RX_POWER_FAIL_LOW**, and **OTS_TX_POWER_FAIL_LOW**.

Before you begin

Identify the fault type, fault tag, severity values, and target scope for the profile.

Procedure

1. Enter global configuration mode.

   configure terminal

2. Use the **fault-profile** command to create a fault profile with a unique name.

   fault-profile *fault-profile-name*

3. Use the **fault identifier** command to add the fault identifier and severity values to the fault profile.

   fault identifier subsystem XR fault-type HW_GFP HW_ETHERNET HW_SDH_CONTROLLER HW_SONET HW_OPTICS HW_G709 HW_CPRI HW_OTS fault-tag *fault-name* **sas** *severity-level* **nsas** *severity-level*

4. Commit the profile configuration.

   commit

5. Apply the fault profile at the required scope.

   fault-profile *fault-profile-name* **apply rack** *0* **slot ALL LC1 LC2 LC3 port** *port-id*

6. Commit the applied profile.

   commit

7. Exit configuration mode.

   exit

The fault profile changes the severity for matching faults at the scope where the profile is applied.

Port or slot-level profile

This example creates a fault profile and applies it at the port or slot level.

```
RP/0/RP0/CPU0:ios#configure terminal
RP/0/RP0/CPU0:ios(config)#fault-profile FpSystem fault-identifier subsystem
XR
fault-type HW_OTS fault-tag OTS_SWITCH_TO_PROTECT sas NONFAULTED nsas NONFAULTED
RP/0/RP0/CPU0:ios(config)#commit
RP/0/RP0/CPU0:ios(config)#fault-profile FpSystem apply rack 0 slot LC2 port 1
RP/0/RP0/CPU0:ios(config)#commit
RP/0/RP0/CPU0:ios(config)#exit
```

Node-level profile

This example creates a fault profile and applies it at the node level.

```
RP/0/RP0/CPU0:ios#configure terminal
RP/0/RP0/CPU0:ios(config)#fault-profile FpNode fault-identifier subsystem XR
fault-type HW_OTS fault-tag OTS_RX_LOS_P sas CRITICAL nsas CRITICAL
RP/0/RP0/CPU0:ios(config)#commit
RP/0/RP0/CPU0:ios(config)#fault-profile FpNode apply rack 0 slot ALL
RP/0/RP0/CPU0:ios(config)#commit
RP/0/RP0/CPU0:ios(config)#exit
```

8 Configure AAA

Topics:

Table 36: Feature History

Feature Name	Release Information	Feature Description
OC support for AAA user	Cisco IOS XR Release 7.3.2	This feature allows all authorized users on XR VM to access administration data on the router through NETCONF or gRPC interface, similar to accessing the CLI. This functionality works by internally mapping the task group of the user on XR VM to a predefined group on System Admin VM. Therefore, the NETCONF and gRPC users can access the administrative information on the router even if their user profiles do not exist on System Admin VM. Command added: • **aaa authorization (System Admin-VM)**

AAA services

This section explains how authentication, authorization, and accounting services verify users, control task permissions, and record user or system activity on the router.

Authentication, authorization, and accounting (AAA) is a security service framework that

- verifies the identity of a user or principal,
- verifies that an authenticated user or principal has permission to perform a specific task, and
- logs sessions and records user-generated or system-generated actions for audit trails.

AAA is part of the software base package and is available by default.

Login authentication command

To configure AAA authentication at login, use the **aaa authentication login** command in global configuration mode.

Admin access for NETCONF and gRPC clients

This section explains how authorized users on the XR virtual machine access administration data through NETCONF or gRPC without matching user profiles on the System Admin VM.

Admin access for NETCONF and gRPC clients is a system capability that

- maps the task group of an authorized user on the XR virtual machine to a predefined group on the System Admin VM,
- allows NETCONF and gRPC users to access administration information on the router, and
- is enabled by default from Cisco IOS XR Software Release 7.3.2.

NETCONF is an XML-based protocol that uses Secure Shell transport to configure a network. gRPC is an open-source remote procedure call framework.

Administration access before Release 7.3.2

Before Cisco IOS XR Software Release 7.3.2, users who used NETCONF, gRPC, or another configuration interface other than the command-line interface (CLI) to access administration information had to belong to user groups configured on the System Admin VM. Otherwise, the router denied access through the client interface with an UNAUTHORIZED access error message.

By default, the XR VM synchronizes only the first configured user to the System Admin VM. If you delete this first user in the XR VM, the system synchronizes the next user in the **root-lr** group to the System Admin VM only when there are no other users configured in the System Admin VM. Subsequent users are not automatically synchronized to the System Admin VM

Administration access from Release 7.3.2

From Cisco IOS XR Software Release 7.3.2, the system internally maps users who are authorized on the XR VM to the System Admin VM based on the task table of the user on the XR VM. With this feature, NETCONF and gRPC users can access administration information on the router even when their user profiles do not exist on the System Admin VM.

User profile mapping from XR VM to System Admin VM

This section explains how predefined System Admin VM groups, command rules, and data rules support admin CLI access and NETCONF or gRPC access to administration data.

User profile mapping is an AAA behavior that

- uses predefined groups, command rules, and data rules in the System Admin VM,
- allows users from different System Admin VM groups to access permitted command and data scopes, and
- supports administration data access for NETCONF and gRPC applications based on those groups and rules.

The system creates the predefined groups, command rules, and data rules when the internal AAA process starts or when you create the first user.

Predefined group access

The predefined groups provide these access levels:

- **root-system**: Has the highest privilege in the System Admin VM.
- **admin-r**: Has read and execute access to all data.
- **aaa-r**: Has access only to AAA data.

With the admin access feature, NETCONF and gRPC applications can access administration data that is determined by these rules and groups.

Predefined AAA configuration example

Use the **show running-configuration aaa** command to view the AAA configuration.

```
aaa authentication groups group aaa-r gid 100 users %%__system_user__%%
!
aaa authentication groups group admin-r gid 100 users %%__system_user__%%
!
aaa authentication groups group root-system gid 100 users "%%__system_user__%%
 "
!
aaa authorization cmdrules cmdrule 1 context * command * group root-system ops
 rx action accept
!
aaa authorization cmdrules cmdrule 2 context * command "show running-config
aaa" group aaa-r ops rx action accept
!
aaa authorization cmdrules cmdrule 3 context * command "show tech-support aaa"
 group aaa-r ops rx action accept
!
aaa authorization cmdrules cmdrule 4 context * command "show aaa" group aaa-r
 ops rx action accept
!
aaa authorization cmdrules cmdrule 5 context * command show group admin-r ops
 rx action accept
!
aaa authorization datarules datarule 1 namespace * context * keypath * group
root-system ops rwx action accept
!
aaa authorization datarules datarule 2 namespace * context * keypath /aaa group
 aaa-r ops r action accept
!
aaa authorization datarules datarule 3 namespace * context * keypath /aaa group
 admin-r ops rwx action reject
!
aaa authorization datarules datarule 4 namespace * context * keypath / group
admin-r ops r action accept
```

Allow read access to administration data for NETCONF and gRPC clients

Use this procedure to create a command rule that allows users in the admin-r group to read administration data through NETCONF or gRPC GET operations.

Create a command rule when users in the **admin-r** group must read administration data through NETCONF or gRPC clients.

NETCONF and gRPC users access administration data on the router through GET operations as defined by each protocol. Configure a command rule if the client context requires read access.

Before you begin

Ensure that the user group exists and that you can access the System Admin configuration mode.

Procedure

1. Enter the system admin configuration mode.

   Example

   ```
   admin
   configure
   ```

2. Use the **aaa authorization cmdrules cmdrule 6** command to create command rule 6.

   Example

   ```
   aaa authorization cmdrules cmdrule 6
   ```

3. Use the **context netconf** command to set the client context for the command rule.

   Example

   ```
   context netconf
   ```

   This example uses the NETCONF context. Use the context that matches the client type requiring read access.

4. Use the **command get** command to allow the GET operation.

   Example

   ```
   command get
   ```

5. Use the **group admin-r** command to apply the command rule to the **admin-r** group.

   Example

   ```
   group admin-r
   ```

6. Use the **ops rx** command to set the operation permissions to read and execute.

Example

```
ops rx
```

7. Use the **action accept** command to accept requests that match the command rule.

Example

```
action accept
```

8. Commit the configuration.

Example

```
commit
```

The command rule allows users in the **admin-r** group to read administration data for the configured client context.

The running configuration includes this command rule:

```
aaa authorization cmdrules cmdrule 6
context netconf
command get
group admin-r
ops rx
action accept
!
```

What to do next

Use the **show running-configuration aaa** command to verify the command rule.

9 Host Services and Applications

Topics:

This section explains the functions and prerequisites of host services and applications in Cisco IOS XR software.

A host service or application is a router feature that

- checks network connectivity and the route a packet follows to reach a destination,
- maps a host name to an IP address or an IP address to a host name, and
- transfers files between routers and UNIX workstations.

Prerequisites

Install the relevant optional RPM package before using host services or applications.

HTTP clients

This section explains how HTTP clients transfer files and data over a network and support configurable parameters for secure and flexible operation.

A HTTP client is a network utility that

- transfers files and data from HTTP servers to devices over a network using the HTTP protocol,
- enables configuration of connection, security, and transport parameters via **http client** command, and
- and supports advanced features such as SSL/TLS options, source interface selection, and protocol versioning.

Configurable parameters for HTTP clients

HTTP client is available by default. You can configure http client settings or view and modify the existing settings. To configure the settings, use the **http client** command in XR configuration mode.

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#http client ?
connection          Configure HTTP Client connection
response            How long HTTP Client waits for a response from the server

                    for a request message before giving up
secure-verify-host  Verify that if server certificate is for the server it is
 known as
secure-verify-peer  Verify authenticity of the peer's certificate
source-interface    Specify interface for source address
ssl                 SSL configuration to be used for HTTPS requests
tcp-window-scale    Set tcp window-scale factor for High Latency links
version             HTTP Version to be used in HTTP requests
vrf                 Name of vrf
```

Table 37: Commands used to configure HTTP client settings

Parameters	Description
connection	Configure HTTP Client connection by using either retry or timeout options.
response	How long HTTP Client waits for a response from the server for a request message before giving up.
secure-verify-host	Verify host in peer's certificate. To disable verifying this, you can use the command **http client secure-verify-host disable**
secure-verify-peer	Verify authenticity of the peer's certificate.
source-interface	Specifies the interface for source address for all outgoing HTTP connections. You can enter either an ipv4 or ipv6 address or both.
ssl version	SSL version (configuration) to be used for HTTPS requests.
tcp-window-scale scale	Set tcp window-scale factor for high latency links.

Parameters	Description
version version	HTTP version to be used in HTTP requests. • 1.0 - HTTP1.0 will be used for all HTTP requests. • 1.1 - HTTP1.1 will be used for all HTTP requests. • default libcurl - will use HTTP version automatically.
vrf name	Name of vrf.

This example shows how to set the tcp window-scale to 8.

```
RP/0/RP0/CPU0:ios(config)#http client tcp-window-scale 8
```

This example shows how to set the HTTP version to 1.0.

```
RP/0/RP0/CPU0:ios(config)#http client version 1.0
```

Note

HTTP client uses libcurl version 7.30

TCP

This section explains how TCP enables reliable, connection-oriented data transfer across networks.

A Transmission Control Protocol (TCP) is a transport layer protocol that

- establishes reliable, connection-oriented communication between devices,
- manages sequencing and acknowledgment of data packets to ensure correct delivery, and
- multiplexes multiple application data streams over a single network connection.

TCP dump file converter

This section explains how TCP dump file converters make network packet traces readable for troubleshooting.

A TCP dump file converter is a network analysis tool that

- converts IOS XR binary dump files into user-friendly formats, such as PCAP or text,
- enables easier viewing and analysis of packet traces during incidents like Non-Stop Routing (NSR) disablement or session flaps, and
- assists network engineers in identifying and resolving issues by making critical packet information accessible.

Additional reference information

When NSR is disabled or a session flap occurs on the system, the TCP process running on an NCS system automatically stores the latest 200 packet traces in binary format within a temporary folder. These traces include details about configured routing protocols and overall network traffic.

Methods to convert and view binary packet trace files

There are two primary methods to convert and view binary packet trace files:

- You can use the **show tcp dump-file <binary filename>** command to view each binary file in text format manually. For more information, see View binary files in text format manually on page 137.

  This process is time-consuming because you must view each file individually, one after the other.

- You can convert all stored packet traces in binary files into PCAP, text, or both using the **tcp dump-file convert** command. For more information, see Convert binary files to readable format using TCP dump file converter on page 138.

  This active approach greatly improves the efficiency and ease of packet analysis during network troubleshooting.

Limitations and restrictions for TCP dump file converter

Understand the limitations and restrictions you must consider when using the TCP dump file converter to manage session data and file viewing.

These limitations and restrictions apply to the TCP dump file converter:

- The system stores only the most recent 200 message exchanges. These occur right before session termination, when NSR is disabled, or during a session flap.
- You can view only one binary file in text format using the **show tcp dump-file <binary filename>** command.
- TCP dump files are generated by default for BGP, MSDP, MPLS LDP, and SSH.

View binary files in text format manually

Use this task to view packet trace binary files in text format without using the TCP dump file converter.

This task enables manual examination of packet trace binary files by displaying their contents in text format, which supports troubleshooting without conversion tools.

This task is useful when you need to check packet traces directly on the device and do not have access to TCP dump file conversion utilities.

Follow these steps to view packet trace binary files in text format:

Procedure

1. Use the **show tcp dump-file list all** command to view the list of packet traces in binary files stored in the tcpdump folder.

   Example

   ```
   RP/0/RP0/CPU0:ios# show tcp dump-file list all
   total 1176
   -rw-r--r-- 1 root root 5927 Nov 22 12:42 31_0_0_126.179.20966.cl.1700656933
   -rw-r--r-- 1 root root 5892 Nov 22 12:42 31_0_0_127.179.35234.cl.1700656933
   -rw-r--r-- 1 root root 6148 Nov 22 12:42 31_0_0_149.179.54939.cl.1700656933
   -rw-r--r-- 1 root root 5894 Nov 22 12:42 31_0_0_155.179.18134.cl.1700656933
   -rw-r--r-- 1 root root 6063 Nov 22 12:42 31_0_0_156.179.25445.cl.1700656933
   -rw-r--r-- 1 root root 5860 Nov 22 12:42 31_0_0_161.179.30859.cl.1700656933
   -rw-r--r-- 1 root root 5832 Nov 22 12:42 31_0_0_173.179.36935.cl.1700656933
   -rw-r--r-- 1 root root 5906 Nov 22 12:42 31_0_0_190.179.25642.cl.1700656933
   ```

2. Use the **show tcp dump-file <binary filename>** command to view each packet trace binary file in text format.

Example

```
RP/0/RP0/CPU0:ios# show tcp dump-file 10_106_0_73.179.34849.cl.1707424077
location 0/RP0/CPU0
Filename: 10_106_0_73.179.34849.cl.1707424077

================================================================
Connection state is CLOSED, I/O status: 0, socket status: 103
PCB 0x00007f86bc05e3b8, SO 0x7f86bc05e648, TCPCB 0x7f86bc0c3718, vrfid
0x60000000,
Pak Prio: Medium, TOS: 192, TTL: 1, Hash index: 1593
Local host: 10.106.0.72, Local port: 179 (Local App PID: 11354)
Foreign host: 10.106.0.73, Foreign port: 34849
(Local App PID/instance/SPL_APP_ID: 11354/1/0)

Current send queue size in bytes: 0 (max 0)
Current receive queue size in bytes: 0 (max 0)  mis-ordered: 0 bytes
Current receive queue size in packets: 0 (max 0)

Timer          Starts    Wakeups         Next(msec)
Retrans        103448          8               0
SendWnd             0          0               0
TimeWait            1          0               0
AckHold        106815     106545               0
KeepAlive           1          0               0
PmtuAger            0          0               0
GiveUp              0          0               0
Throttle            0          0               0
FirstSyn            0          0               0

   iss: 161240548   snduna: 163206936   sndnxt: 163206936
sndmax: 163206936   sndwnd: 63104       sndcwnd: 18120
   irs: 3691232436  rcvnxt: 3693473072  rcvwnd: 26099   rcvadv: 3693499171
```

This sample displays only a portion of the actual output. The full output provides additional packet trace details.

You can examine the text details of packet trace binary files directly using the command-line interface without converting them to other formats.

Convert binary files to readable format using TCP dump file converter

Use this task to convert TCP dump packet traces in binary files into PCAP and text formats for easier analysis.

This task enables you to convert TCP dump packet trace files into readable formats (PCAP and text) for analysis and review.

You may need to analyze network packet traces captured in binary format, which are not readable as-is. Converting them to PCAP or text allows you to use analysis tools or view them manually in the CLI.

Follow these steps to convert TCP dump packet traces to PCAP and text formats:

Procedure

---

1. Use the **tcp dump-file convert all-formats all** command to convert the dump packet traces in binary files into PCAP and text formats.

Example

```
RP/0/RP0/CPU0:ios# tcp dump-file convert all-formats all
ascii file is saved at :
/harddisk:/decoded_dumpfiles/text_tcpdump_peer_all_node0_RP0_CPU0_2024_3_19_10_8_53.462070.txt
pcap file is saved at :
/harddisk:/decoded_dumpfiles/pcap_tcpdump_peer_all_node0_RP0_CPU0_2024_3_19_10_8_40.154838.pcap
[OK]
```

By default, the system stores the converted files in the decoded_dumpfiles folder on the hard disk.

Using the **location node-id** and **file <file path>** keywords, you can save the converted TCP dump file to your desired location.

For example, **tcp dump-file convert all-formats all location** *0/RP0/CPU0* **file** */harddisk:/demo2*.

```
RP/0/RP0/CPU0:ios# tcp dump-file convert all-formats all location 0/RP0/CPU0
 file /harddisk:/demo2
ascii file is saved at : /harddisk:/demo2.txt
pcap file is saved at : /harddisk:/demo2.pcap
[OK]
```

2. Use the **run cat <text file path>** command to view the converted text file in the CLI.

Example

```
RP/0/RP0/CPU0:ios# run cat
/harddisk:/decoded_dumpfiles/text_tcpdump_peer_all_node0_RP0_CPU0_2024_3_19_10_8_53.462070.txt
Filename: 2024_3_19_10_8_53.462070

================================================================
Connection state is CLOSED, I/O status: 0, socket status: 103
PCB 0x0000000000f47a80, SO 0xf476d0, TCPCB 0xf6a370, vrfid 0x60000000,
Pak Prio: Medium, TOS: 192, TTL: 255, Hash index: 563
Local host: 14:11:11::1, Local port: 47743 (Local App PID: 19579)
Foreign host: 14:11:11::2, Foreign port: 179
(Local App PID/instance/SPL_APP_ID: 19579/1/0)

Current send queue size in bytes: 0 (max 0)
Current receive queue size in bytes: 0 (max 0)  mis-ordered: 0 bytes
Current receive queue size in packets: 0 (max 0)

Timer          Starts    Wakeups         Next(msec)
Retrans            70          2                0
SendWnd             0          0                0
TimeWait            2          0                0
AckHold            66         61                0
KeepAlive           1          0                0
PmtuAger            0          0                0
GiveUp              0          0                0
Throttle            0          0                0
FirstSyn            1          1                0

   iss: 3113104891  snduna: 3113106213  sndnxt: 3113106213
sndmax: 3113106213  sndwnd: 31523       sndcwnd: 2832
   irs: 4250126727  rcvnxt: 4250128049  rcvwnd: 31448   rcvadv: 4250159497
```

This sample displays only a portion of the actual output. The full output provides additional details.

3. Use the **scp** command to copy the converted packet traces from the system to your local computer and view the converted PCAP file.

The system converts TCP dump packet traces into readable PCAP and text formats. The files are stored at your specified location and are accessible for further analysis from the CLI or on your local machine.

10 NCS 1001 Application Hosting

Topics:

Explains Docker container application hosting and restrictions, architecture and resource controls, TPA bring-up methods, App Manager Docker options, third-party RPM workflows, supported commands, use cases, and third-party Python script deployment.

Application hosting

This section explains application hosting on IOS XR and how Docker support lets third-party applications run on NCS 1001 devices to extend router capabilities.

Application Hosting is the infra IOS-XR that allows you to

- run third-party applications on the NCS 1001 devices, and
- use third-party applications to extend device capabilities to complement IOS-XR features.

The Docker daemon is packaged with IOS-XR software on the base Linux OS. This provides native support for running applications inside docker containers on IOS-XR. Docker is the preferred way to run TPAs on IOS-XR.

App Manager

The App Manager is the infra on IOS-XR tasked with the responsibility of managing the life cycle of all container apps (third part and Cisco internal) and process scripts. App Manager runs natively on the host as an IOS-XR process. App Manager leverages the functionalities of docker, systemd and RPM for managing the lifecycle of third-party applications.

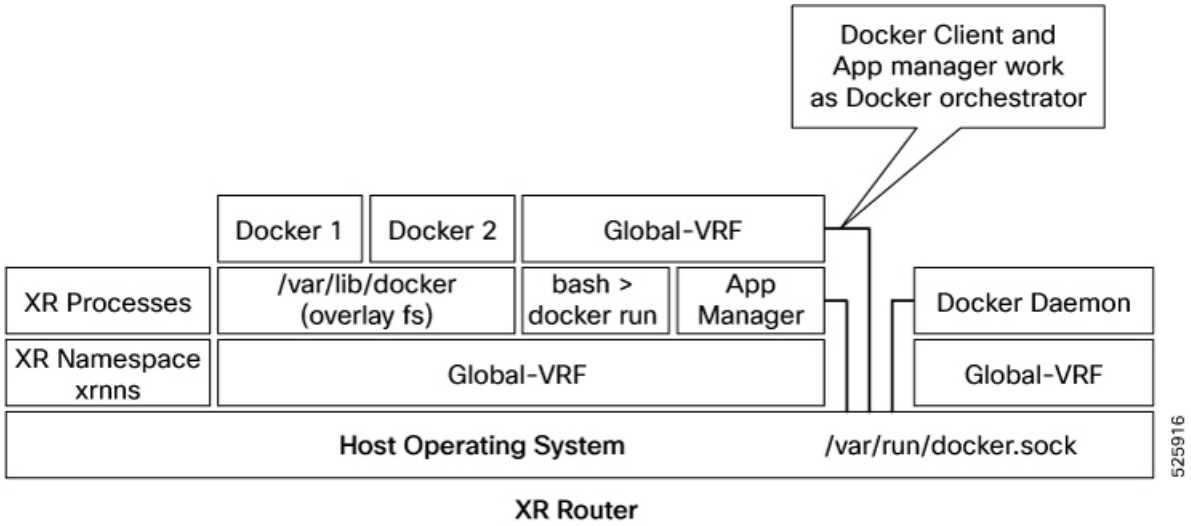
Restriction in docker container application hosting

MPLS packets are not supported on Linux interfaces.

Docker container application hosting architecture

This section describes the docker container application hosting architecture.

Figure 19: Docker on IOS XR



The App manager internally uses docker client, which interacts with TPAs (docker 1 and docker 2) by using the docker commands. The docker client sends the docker commands to **docker daemon**, which, then, executes the commands. The docker daemon uses the **docker.sock** Unix socket to communicate with the dockers.

When the **docker run** command is executed, a docker container is created and started from the docker image. Docker containers can be either in **global-vrf** namespace.

The docker utilizes overlayfs under the **/var/lib/docker** folder for managing the directories.

To host an application in docker containers, see Hosting an Application in Docker Containers.

Guidelines and limitations

- For docker run options --mount and --volume, use the host paths.
  - "/var/run/netns"
  - "/var/lib/docker"
  - "/misc/disk1"
  - "/disk0"
  - "/misc/config/grpc"
  - "/etc"
  - "/dev/net/tun"
  - "/var/xr/config/grpc"
  - "/opt/owner"
- The maximum allowed size for shm-size option is 64 Mb.

TP application resource configuration

IOS XR is equipped with inherent safeguards to prevent third party applications from interfering with its role as a Network OS.

- Although IOS XR does not impose a limit on the number of TPAs that can run concurrently, it does impose constraints on the resources allocated to the Docker daemon, based on these parameters:
  - CPU: By default, ¼ of the CPU per core available in the platform.

    You can hard limit the default CPU usage in the range between 25-75% of the total system CPU using the appmgr resources containers limit cpu value command. This configuration restricts the TPAs from using more CPU than the set hard limit value irrespective of the CPU usage by other XR processes.

    This example provides the CPU hard limit configuration.

    ```
    RP/0/RSP0/CPU0:ios(config)#appmgr resources containers limit cpu ?
      <25-75>  In Percentage
    RP/0/RSP0/CPU0:ios(config)#appmgr resources containers limit cpu 25
    ```

  - RAM: By default, 1 GB of memory is available.

    You can hard limit the default memory usage in the range between 1-25% of the overall system memory using the appmgr resources containers limit memory value command. This configuration restricts the TPAs from using more memory than the set hard limit value.

    This example provides the memory hard limit configuration.

    ```
    RP/0/RSP0/CPU0:ios(config)#appmgr resources containers limit memory ?
      <1-25>  In Percentage
    RP/0/RSP0/CPU0:ios(config)#appmgr resources containers limit memory 20
    ```

  - Disk space is restricted by the partition size, which varies by platform and can be checked by executing "run df -h" and examining the size of the `/misc/app_host` or `/var/lib/docker` mounts.
- All traffic to and from the application is monitored by the XR control protection, LPTS.
- Signed Applications are supported on IOS XR. Users have the option to sign their own applications by onboarding an Owner Certificate (OC) through Ownership Voucher-based workflows as described in RFC 8366. Once an Owner

Certificate is onboarded, users can sign applications with GPG keys based on the Owner Certificate, which can then be authenticated during the application installation process on the router.

This table shows the various functions performed by appmgr.

Package manager	Lifecyle manager	Monitoring and debugging

• Handles installation of docker images packaged as RPMs.
• Syncs the required state to standby to restart apps in cases of switchover, etc
	• Handles application start, stop, and kill operations.
	• Handles automatic application reload on:
	  • Router reboot
	  • Container crash
	  • Switchover
		• Logging, stats, application health check.
		• Forwards docker deamon logs to XR syslog.
		• Allows to execute into docker shell of running application.

TP App Bring-up

This section provides the information, how to bring-up the TP container app. This can be done by these four ways.

- App Config
- UM Model
- Native Yang Model
- gNOI Containerz

Bring up TPAs using application configuration

Follow these steps to configure the docker run time options.

Procedure

1. Configure the docker run time option.

   Use **--pids-limit** to limit the number of process IDs using appmgr.

   #### Example

   This example shows the configuration of the docker run time option **--pids-limit** to limit the number of process IDs using appmgr.

   ```
   RP/0/RP0/CPU0:ios#appmgr application alpine_app activate type docker source
   alpine docker-run-opts "-it –pids-limit 90" docker-run-cmd "sh"
   ```

   The number of process IDs is limited to 90.

2. Verify the docker run time option configuration.

   Use the **show running-config appmgr** command to verify the run time option.

Example

This example shows how to verify the docker run time option configuration.

```
RP/0/RP0/CPU0:ios#show running-config appmgr
Thu Mar 23 08:22:47.014 UTC
appmgr
 application alpine_app
  activate type docker source alpine docker-run-opts "-it –pids-limit 90"
docker-run-cmd "sh"
 !
!
```

Bring up TPAs using UM model

Follow these steps to configure the docker run time options.

Procedure

Configure the docker run time option.

Use **--pids-limit** to limit the number of process IDs using Netconf.

Example

This example shows the configuration of the docker run time option **--pids-limit** to limit the number of process IDs using Netconf.

```
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="101">
  <edit-config>
    <target>
      <candidate/>
    </target>
    <config>
      <appmgr xmlns=http://cisco.com/ns/yang/Cisco-IOS-XR-um-appmgr-cfg>

        <applications>
          <application>
            <application-name>alpine_app</application-name>
            <activate>
              <type>docker</type>
                  <source-name>alpine</source-name>
                  <docker-run-cmd>/bin/sh</docker-run-cmd>
                  <docker-run-opts>-it --pids-limit=90</docker-run-opts>
            </activate>
          </application>
        </applications>
      </appmgr>
    </config>
  </edit-config>
```

The number of process IDs is limited to 90.

Bring up TPAs using native model

This example shows the configuration of the docker run time option --**pids-limit** to limit the number of process IDs using Native YANG model.

```
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="101">
  <edit-config>
    <target>
      <candidate/>
    </target>
    <config>
      <appmgr xmlns=http://cisco.com/ns/yang/Cisco-IOS-XR-appmgr-cfg>

        <applications>
          <application>
            <application-name>alpine_app</application-name>
            <activate>
              <type>docker</type>
               <source-name>alpine</source-name>
               <docker-run-cmd>/bin/sh</docker-run-cmd>
               <docker-run-opts>-it --pids-limit=90</docker-run-opts>
            </activate>
          </application>
        </applications>
      </appmgr>
    </config>
  </edit-config>
```

Bringup TPAs using gNOI Containerz

The Containerz - gNOI Container Service on NCS 1001 device is a workflow to onboard and manage third-party applications using gNOI RPCs.

For more information, see gNOI Containerz.

Docker run options using application manager

With this feature, runtime options for docker containerized applications on IOS-XR can be configured during launch using the **appmgr activate** " command. AppMgr, which oversees docker containerized applications, ensures that these runtime options can effectively override default configurations, covering aspects like CPU, security, and health checks during the container launch.

This feature introduces multiple runtime options that allow users to customize different parameters of docker containers. The configuration of these runtime options is flexible, as users can use either command or Netconf for the configuration process. Regardless of the chosen method, runtime options must be added to **docker-run-opts** as needed.

Table 38:

Docker run option	Description
--cpus	Number of CPUs
--cpuset-cpus	CPUs in which to allow execution (0-3, 0,1)
--cap-drop	Drop Linux capabilities
--user, -u	Sets the username or UID
--group-add	Add additional groups to run
--health-cmd	Run to check health

Docker run option	Description
--health-interval	Time between running the check
--health-retries	Consecutive failures needed to report unhealthy
--health-start-period	Start period for the container to initialize before starting health-retries countdown
--health-timeout	Maximum time to allow one check to run
--no-healthcheck	Disable any container-specified HEALTHCHECK
--add-host	Add a custom host-to-IP mapping (host:ip)
--dns	Set custom DNS servers
--dns-opt	Set DNS options
--dns-search	Set custom DNS search domains
--domainname	Container NIS domain name
--oom-score-adj	Tune host's OOM preferences (-1000 to 1000)
--shm-size	Option to set the size of /dev/shm
--init	Run an init inside the container that forwards signals and reaps processes
--label, -l	Set meta data on a container
--label-file	Read in a line delimited file of labels
--pids-limit	Tune container pids limit (set -1 for unlimited)
--work-dir	Working directory inside the container
--ulimit	Ulimit options
--read-only	Mount the container's root filesystem as read only
--volumes-from	Mount volumes from the specified container(s)
--stop-signal	Signal to stop the container
--stop-timeout	Timeout (in seconds) to stop a container
--cap-addNET_RAW	Enable NET_RAW capabilities
--publish	Publish a container's port(s) to the host
--entrypoint	Overwrite the default ENTRYPOINT of the image
--expose	Expose a port or a range of ports
--link	Add link to another container
--env	Set environment variables
--env-file	Read in a file of environment variables
--network	Connect a container to a network

Docker run option	Description
--hostname	Container host name
--interactive	Keep STDIN open even if not attached
--tty	Allocate a pseudo-TTY
--publish-all	Publish all exposed ports to random ports
--volume	Bind mount a volume
--mount	Attach a filesystem mount to the container
--restart	Restart policy to apply when a container exits
--cap-add	Add Linux capabilities
--log-driver	Logging driver for the container
--log-opt	Log driver options
--detach	Run container in background and print container ID
--memory	Memory limit
--memory-reservation	Memory soft limit
--cpu-shares	CPU shares (relative weight)
--sysctl	Sysctl options

Third party RPMs installation using App Manager install UI

This section explains how App Manager install UI supports runtime installation of third-party RPMs while the router continues operating and prepares readers for the related installation workflow.

This section describes how to install third party RPMs using App Manager install UI at runtime while the router is running.

Limitation and guidelines for third party RPMs

These are the limitations and guidelines for the TP RPMs.

- RPM must not have “scriptlets”. Scriptlets allow packages to run code on installation and removal.
- RPM must not be already installed via XR Install UI.
- RPM must not be already installed via App manager UI.
- TP RPMs must install files only to the `/var/lib/docker/appmgr/` filesystem location.
- RPM Signature verification is not enforced by App Manager Install UI. It supports unsigned TP RPMs.

Install third party RPMs using App Manager install UI

Use this task to install third party RPMs using App Manager install UI.

Procedure

1. Create an RPM containing the application (in the form of a docker container image).
2. Use App manager RPM build tool to generate TP RPMs. See https://github.com/ios-xr/xr-appmgr-build/blob/main/README.md.
3. Install the TP RPM using the App Manager Install UI command.

Example

```
RP/0/RP0/CPU0:ios# appmgr package install rpm
/harddisk\:/alpine-0.1.0-XR_7.3.1.x86_64.rpm
```

Uninstall third party RPMs using App Manager install UI

Use this task to uninstall third party RPMs using App Manager install UI.

Uninstallation of TP RPM can be performed using two ways.

> **Attention**
>
> App manager uninstall CLI uninstalls the TP RPM at runtime while NCS 1001 is running.

Procedure

1. Uninstall using source name.

Example

```
RP/0/RP0/CPU0:ios# appmgr package uninstall source alpine
```

2. Uninstall using package name.

Example

```
RP/0/RP0/CPU0:ios# appmgr package uninstall package
alpine-0.1.0-XR_7.3.1.x86_64
```

Supported commands on application manager

This section provides details about Application Manager operations and IOS XR commands used to manage running containers, including start, stop, kill, and exec actions.

Action commands

App Manager action commands are used to start, stop, kill and exec shell commands inside running container.

Table 39: Action commands

Command name	Commands	Purpose
Application start	**appmgr application start name** *<name>*	Starts a stopped container or application.
Application stop	**appmgr application stop name** *<name>*	Stops a stopped running container or application.
Application kill	**appmgr application kill name** *<name>*	Kills a running container or application.
Application copy	**appmgr application copy** *<storage-path>*	Copy data between host and container.
Appliction exec	**appmgr application exec** *<name>* **docker-exec-cmd** *<cmd>*	Executes command inside TP container application (docker only).

Examples

Here are examples for the app manager action commands. For more information on the commands, see *Command Reference Guide for NCS 1001*.

Action CLI (Start): This starts a stopped container

```
RP/0/RP0/CPU0:ios# appmgr application start name alpine_app
```

Action CLI (Stop): This stops a running container

```
RP/0/RP0/CPU0:ios# appmgr application stop name alpine_app
```

Action CLI (Kill): This forcefully kills a running container

```
RP/0/RP0/CPU0:ios# appmgr application kill name alpine_app
```

Action CLI (Copy): Copy data between host and container

```
RP/0/RP0/CPU0:ios# appmgr application copy harddisk:/data.txt alpine_app:/
```

Action CLI (Exec): Execute command inside TP container app

```
RP/0/RP0/CPU0:ios# appmgr application exec name txt alpine_app docker-exec-cmd
 "ls -ltr"
```

Show commands

App Manager show commands shows the application or container info.

Table 40: show commands

Command name	Commands	Purpose
Source table modification	**show appmgr source-table**	Lists all third-party applications onboarded via (XR Infra / Appmgr CLI / Containerz).

Command name	Commands	Purpose
Application table modification	**show appmgr application-table**	Lists all third-party applications managed via (Config / Containerz) workflow in a tabular view.
Application source name	**show appmgr source name** *<name>*	Shows the source name.
Application package install	**show appmgr packages installed**	Lists all the application manager RPM packages installed.
Appliction exec	**show appmgr application name** *<name>* **info detail summary**	Shows application information at desired verbosity.
Application logs	**show appmgr application name** *<name>* **logs**	Shows application logs.
Application stats	**show appmgr application name** *name* **stats**	Shows application statistics.
Application process script table	**show appmgr process-script-table**	Shows summary status of all registered process-scripts.

Examples

This section shows the example outputs for the show appmgr commands. For more information on the show appmgr commands, see the *Command Reference guide for the NCS 1001*.

The example output shows the onboarded TP applications.

```
RP/0/RP0/CPU0:ios# show appmgr source-table
Sno Name               File                                Installed By

--- ----------------- -------------------- ----------------------------------
1   alpine                 alpine.tar.gz               containerz

2   hello-world        hello-world.tar.gz       app_manager
3   bonnet               bonnet.tar.gz              xr_install
```

The example output shows the Workflow column that specifies how to manage the TP applications.

```
RP/0/RP0/CPU0:ios#show appmgr application-table
Name          Type    Config State  Status                 Workflow
------------- ------ ------------ -------------
---------------------------------
alp-cz-app    Docker  Activated    Up 2 minutes     containerz
bnt-cfg-app  Docker  Activated    Up 1 minutes     config
```

The example output shows the details of the *swan* application. The `Status` value under `Vrf Relay: <name>` indicates the running status of the relay agent. If it reports an `Exited` state or a `Restarting` state, use the relay agent logs for troubleshooting.

```
RP/0/RP0/CPU0:ios#show appmgr application name swan info detail
Mon Nov 23 21:22:47.240 UTC
Application: swan
  Type: Docker
  Source: swanagent
  Config State: Activated
```

```
  Docker Information:
    Container ID:
cd27988cd5b066d6272085e5e3ff675c94a64cb4ad06f90c2d89453a8ec4af34
    Container name: swan
    Labels:
    Image: swanagent:latest
    Command: "./agentxr"
    Created at: 2020-11-23 21:22:39 +0000 UTC
    Running for: 8 seconds ago
    Status: Up Less than a second
    Size: 0B (virtual 82.9MB)
    Ports:
   Mounts: /var/opt/cisco/iosxr/appmgr/config/docker/swanagent,/var/run/netns

    Networks: host
    LocalVolumes: 0
    Vrf Relays:
      Vrf Relay: vrf_relay.swan.70ec1f59336271ab
        Source VRF: vrf-mgmt
        Source Port: 8000
        Destination VRF: vrf-default
        Destination Port: 10000
        IP Address Range: 172.16.0.0/12
        Status: Up 10 seconds
      Vrf Relay: vrf_relay.swan.5c7373d41d0ec84f
        Source VRF: vrf-mgmt
        Source Port: 8001
        Destination VRF: vrf-default
        Destination Port: 10001
        IP Address Range: 172.16.0.0/12
        Status: Up 11 seconds
```

Top use cases for application hosting

This section provides details about common application hosting use cases, including network performance measurement, server management automation, and hosted tools that extend router operations.

Some of the top use cases for application hosting are:

- **Measure network performance**: An application can be hosted to measure the bandwidth, throughput and latency of the network and monitor the performance. An example of such an application is the iPerf tool.
- **Automate server management**: An application can be hosted to automate the server functions like upgrading software, allocation of resources, creating user accounts, and so on. Examples of such an application are the Chef and Puppet configuration management tools.

Manually deploy and activate third party script

Use this procedure to automatically deploy and activate third-party Python scripts through App Manager, including scheduler status checks and script execution for router automation.

NCS 1001 provides CLI commands to perform configurations and operations on the optical devices. If you want to automate the NCS 1001 node operations, you can run third party scripts through App manager. See Automatically deploy and activate third party script on page 161.

Follow these steps to deploy and activate third party script manually.

Procedure

1. Use the **show script status** command to check the list of the OPS scripts that are in-built in XR.

   Example

   This command lists the status of *xr_script_scheduler* script. *Ready* status in the output means that the script checksum is verified and is ready to run.

```
RP/0/RP0/CPU0:ios#show script status
Tue Oct 24 18:03:09.220 UTC
=============================================================================================

 Name                              | Type    | Status            | Last Action |
 Action Time
---------------------------------------------------------------------------------------------

 show_interfaces_counters_ecn.py | exec    | Ready             | NEW         |
 Tue Oct 24 07:10:36 2025
 xr_data_collector.py            | exec    | Ready             | NEW         |
 Tue Oct 24 07:10:36 2025
 xr_script_scheduler.py          | process| Ready             | NEW         |
 Tue Oct 24 07:10:36 2025
=============================================================================================
RP/0/RP0/CPU0:ios#
```

2. Use the appmgr to run the XR scheduler script.

   XR scheduler script contains the necessary

   Example

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#appmgr
RP/0/RP0/CPU0:ios(config-appmgr)#process-script xr_script_scheduler
RP/0/RP0/CPU0:ios(config-process-script)#executable xr_script_scheduler.py
RP/0/RP0/CPU0:ios(config-process-script)#commit
```

3. Check for available process scripts in app manager.

   Example
   This output highlights the *xr_script_scheduler.py* process script that is not activated.

```
RP/0/RP0/CPU0:ios#show appmgr process-script-table
Wed Oct 22 09:45:02.795 UTC
Name                Executable           Activated  Status    Restart Policy
    Config Pending
------------------- -------------------- ----------- ---------
----------------- -----------------
xr_script_scheduler  xr_script_scheduler.py     No     Not Started   Always
                 No
```

4. Activate the available process script.

   You can start executing a process script only after it is activated.

Example

```
RP/0/RP0/CPU0:ios#appmgr process-script activate name xr_script_scheduler
Wed Oct 22 09:45:41.035 UTC
```

(Optional) Verify the status of the process script. This example shows the process script *xr_script_scheduler* is *Activated*.

```
RP/0/RP0/CPU0:ios#show appmgr process-script-table
Wed Oct 22 09:45:47.275 UTC
Name                Executable           Activated  Status    Restart Policy
    Config Pending
------------------- -------------------- ----------- ---------
---------------- ----------------
xr_script_scheduler  xr_script_scheduler.py     Yes     Not Started   Always
                  No
```

5. Use the **appmgr process-script start** command to start the available process script.

Example

xr_script_scheduler is the only available process script.

This command starts the process script *xr_script_scheduler*.

```
RP/0/RP0/CPU0:ios#appmgr process-script start name xr_script_scheduler
Wed Oct 22 09:46:08.273 UTC
```

(Optional) Verify the status of the process script after activation. This example shows the process script *xr_script_scheduler* is *Activated* and *Started*.

```
RP/0/RP0/CPU0:ios#show appmgr process-script-table
Wed Oct 22 09:46:24.679 UTC
Name                Executable           Activated  Status    Restart Policy
    Config Pending
------------------- -------------------- ----------- ---------
---------------- ----------------
xr_script_scheduler  xr_script_scheduler.py       Yes     Started   Always
                No
```

6. Verify the scheduler script is running.
   a) Run the **show script execution** command to verify the functioning of the debug and monitoring scripts.

Example

This command displays a list of OPS scripts currently running.

```
RP/0/RP0/CPU0:ios# show script execution
Tue Oct 24 19:41:15.882 UTC
=============================================================================================================

 Req. ID   | Name (type)                                  | Start
         | Duration   | Return | Status
-------------------------------------------------------------------------------------------------------------

 1698176223| xr_script_scheduler.py (process)         | Tue Oct 24 19:37:02
 2025 | 253.32s    | None   | Started
=============================================================================================================
RP/0/RP0/CPU0:ios#
```

b) Use the **show script execution details** command to verify if the scheduler script is running.

Example

This command displays a list of OPS scripts currently running. If the scheduler script is correctly configured and activated, the scheduler script execution detail appears in the output.

```
RP/0/RP0/CPU0:ios#show script execution details
Tue Oct 25 18:01:56.590 UTC
==============================================================================================

 Req. ID   | Name (type)                                    | Start
         | Duration   | Return | Status
----------------------------------------------------------------------------------------------

 1698170509| xr_script_scheduler.py (process)         | Tue Oct 25 18:01:49
 2023 | 7.68s       | None   | Started
----------------------------------------------------------------------------------------------

 Execution Details:
 ------------------
 Script Name  : xr_script_scheduler.py
 Version      : 25.3.1.14Iv1.0.0
 Log location :
/harddisk:/mirror/script-mgmt/logs/xr_script_scheduler.py_process_xr_script_scheduler

 Arguments    :
 Run Options  : Logging level - INFO, Max. Runtime - 0s, Mode - Background

 Events:
 -------
 1.   Event        : New
      Time         : Tue Oct 25 18:01:49 2025
      Time Elapsed : 0.00s Seconds
      Description  : Started by Appmgr
 2.   Event        : Started
      Time         : Tue Oct 25 18:01:49 2025
      Time Elapsed : 0.11s Seconds
      Description  : Script execution started. PID (15985)
==============================================================================================
RP/0/RP0/CPU0:ios#
```

7. Copy the third party RPM files to the NCS 1001 node.

a) Use any of the file transfer mechanisms to copy third-party RPM.

Example

This example shows copying the RPM to the harddisk of the NCS 1001 node using **scp**.

```
RP/0/RP0/CPU0:ios#scp
user@171.xx.xxx.xxx:/users/user/rpm-factory/RPMS/x86_64/nms-1.1-25.3.1.x86_64.rpm
 /harddisk:
Tue Oct 24 18:02:42.400 UTC
<snip>
Password:
nms-1.1-24.1.1.x86_64.rpm                                                    100%
9664   881.5KB/s   00:00
RP/0/RP0/CPU0:ios#
```

b) (Optional) Verify the RPM files using **dir <filepath>**.

Example

```
RP/0/RP0/CPU0:ios#dir harddisk:/nms-1.1-24.1.1.x86_64.rpm
Wed Oct  24 19:53:54.041 UTC
```

8. Install the third party RPM files to use the required debug and monitoring python scripts.

   The third party RPM files have the customized scripts to be executed. The third-party RPM contains two types of files:

   - One or more python scripts–For more information on developing python scripts, see IOS XR Programmability with Python and xr-python-scripts.
   - Run parameter JSON file–*xr_script_scheduler.json* has instruction for the scheduler script.

   Example

   This is an example *xr_script_scheduler.json* file. Customize this file as per your requirements.

```
[
    {
        "name": "__template_entry__.py",
       "description": ["**This is a template entry for documentation purpose.
 This entry will be ignored**",
                        "name : Name of the python script to be executed",
                        "       [string][mandatory]",
                        "description:  Description of the script",
                        "              [string or list of strings][optional:
 default empty string]",
                       "cmd_line_parameters: Script command line parameters"
 ,
                        "                     [list of strings][optional:
default Null][Example: ",
                        "env_variables: Enviromental variables to be set in
script run shell",
                        "               [list of key value pairs][optional:
default Null][Example: [['INT_NAME': 'hu0/1/0/1']]",
                      "run_policy: Script restart policy when script exits",

                        "            [string: one of
always/once/stop][optional: default 'always']",
                        "            always: restart the script every time
it exits",
                        "            once:  do not restart the script if it
exits",
                        "            stop:  stop an existing script run "
                        ],
        "cmd_line_parameters": [],
        "env_variables": [],
        "run_policy": "always"
    },
    {
        "name": "monitor_int_rx_cntr.py",
        "description": "Monitoring mgmt interface for Rx threshold of 100 ",

       "cmd_line_parameters": ["MgmtEth0/RP0/CPU0/0", "200", "-log", "debug"],

       "env_variables": [["INT_NAME", "FourHundredGigE0/9/0/0"], ["INT_NAME2",
 "FourHundredGigE0/10/0/0"]],
        "run_policy": "always"
    },
    {
```

```
        "name": "monitor_int_rx_cntr.py",
        "description": "Monitoring Fo0/0/0/0 interface for Rx threshold of
1000000 ",
        "cmd_line_parameters": ["FourHundredGigE0/0/0/0", "1000000"],
        "run_policy": "once"
    },
    {
        "name": "monitor_int_rx_cntr2.py",
        "description": "Monitoring Fo0/0/0/1 interface for Rx threshold of
5000000 ",
        "cmd_line_parameters": ["FourHundredGigE0/0/0/1", "5000000"],
        "run_policy": "always"
    },
    {
        "name": "monitor_int_rx_cntr2.py",
        "description": "Monitoring Fo0/0/0/2 interface for Rx threshold of
5000000 ",
        "cmd_line_parameters": ["FourHundredGigE0/0/0/2", "8000000"],
        "run_policy": "stop"
    }
]
```

Example

Use the **appmgr package install rpm <full RPM file path>** command to install the third-party RPMs.

```
RP/0/RP0/CPU0:ios#appmgr package install rpm
/harddisk:/nms-1.1-25.3.1.x86_64.rpm
Tue Oct 24 18:03:26.685 UTC
RP/0/RP0/CPU0:ios#
RP/0/RP0/CPU0:ios#show appmgr packages installed
Tue Oct 24 19:42:07.967 UTC
Sno Package
--- ------------------------------------------------------------
1   nms-1.1-25.3.1.x86_64
RP/0/RP0/CPU0:ios#
```

After the scripts and the run parameters file become ready, build the RPM and configure the RPM to install files at `<default exr appmgr rpm install path>/ops-script-repo/exec/<rpm name>/`. RPM build tool for TPA is available at RPM Build Tool.

> **Note**
>
> Install the scripts in directories named after the RPM for smoother execution.

9. Use the **show script status** command to verify that the scripts and the run parameter files contained in the RPM are all installed successfully and added to the script management repository.

Example

This output shows the status that two scripts (monitor_int_xr_cntr.py and monitor_int_rx_cntr2.py) and a run parameter file (xr_script_scheduler.json) file were installed in the third-party RPM named “nms”.

```
RP/0/RP0/CPU0:ios#show script status
```

```
Tue Oct 24 19:41:10.696 UTC
=============================================================================================

 Name                              | Type    | Status            | Last Action |
 Action Time
---------------------------------------------------------------------------------------------

 nms/monitor_int_rx_cntr.py        | exec    | Ready             | NEW         |
 Tue Oct 24 19:38:41 2023
 nms/monitor_int_rx_cntr2.py       | exec    | Ready             | NEW         |
 Tue Oct 24 19:38:41 2023
 nms/xr_script_scheduler.json      | exec    | Ready             | NEW         |
 Tue Oct 24 19:38:41 2023
 show_interfaces_counters_ecn.py | exec    | Ready             | NEW         |
 Tue Oct 24 19:33:52 2023
 xr_data_collector.py              | exec    | Ready             | NEW         |
 Tue Oct 24 19:33:52 2023
 xr_script_scheduler.py            | process| Ready             | NEW         |
 Tue Oct 24 19:33:52 2023
=============================================================================================
RP/0/RP0/CPU0:ios#
```

After the scripts are installed, the scheduler script starts reading the run parameter JSON file and executes the required debug and monitoring scripts.

The logs generated by the scripts are available in the directory `/harddisk\:/mirror/script-mgmt/logs/`.

10. Verify that the debug and monitoring scripts are running.

Example

Use the **show script execution** command to verify that the scripts are running.

```
RP/0/RP0/CPU0:ios#show script execution
Tue Oct 24 19:41:15.882 UTC
=============================================================================================

 Req. ID    | Name (type)                                  | Start
      | Duration    | Return | Status
---------------------------------------------------------------------------------------------

 1698176223| xr_script_scheduler.py (process)             | Tue Oct 24 19:37:02
 2023 | 253.32s     | None   | Started
 1698176224| nms/monitor_int_rx_cntr.py (exec)            | Tue Oct 24 19:38:43
 2023 | 152.46s     | None   | Started
 1698176225| nms/monitor_int_rx_cntr.py (exec)            | Tue Oct 24 19:38:44
 2023 | 152.03s     | None   | Started
 1698176226| nms/monitor_int_rx_cntr2.py (exec)           | Tue Oct 24 19:38:44
 2023 | 151.63s     | None   | Started
=============================================================================================
RP/0/RP0/CPU0:ios#
```

(Optional) Use the **show script execution name***script-name***detail [output][error]**

11. Verify all the active packages are installed.

Example

```
RP/0/RP0/CPU0:ios#show install active summary
Fri Nov 14 12:52:39.322 IST
Label : 25.3.1.31I-iso
```

```
    Active Packages: 2
        ncs1001-xr-25.4.1.31I version=25.4.1.31I [Boot image]
        ncs1001-cosm-1.0.0.0-r253131I
```

12. (Optional) Use the **appmgr process-script stop** command to stop the process script.

Example
This command stops the execution of the process script *xr_script_scheduler*.

```
RP/0/RP0/CPU0:ios#appmgr process-script stop name xr_script_scheduler
Wed Oct 22 09:46:35.110 UTC
```

(Optional) Verify the status of the process script after stopping it. This example shows the process script *xr_script_scheduler* is *Activated* and *Stopped*.

```
RP/0/RP0/CPU0:ios#show appmgr process-script-table
Wed Oct 22 09:46:41.245 UT
Name                Executable           Activated  Status    Restart Policy
    Config Pending
------------------- -------------------- ---------- --------
--------------- ----------------
xr_script_scheduler  xr_script_scheduler.py       Yes     Stopped   Always
                No
```

Automated deployment of third party Python scripts

This section explains how automated deployment runs third-party Python scripts on the router by using App Manager to activate **xr_script_scheduler.py** and execute scripts delivered in third-party RPMs.

Efficient network automation is pivotal in handling extensive cloud-computing networks. The Cisco IOS XR infrastructure plays a crucial role by enabling automation through the initiation of API calls and execution of scripts. Traditionally, an external controller is used for this purpose, utilizing interfaces like NETCONF, SNMP, and SSH to communicate with NCS 1001.

This feature streamlines the operational structure by executing automation scripts directly on the router, thus eliminating the need for an external controller. It allows scripts to leverage Python libraries and access underlying router information. This approach not only accelerates the execution of various types of scripts but also enhances reliability by removing dependencies on the speed and network reachability of an external controller.

The third party script is automatically executed by the xr_script_scheduler.py script upon the installation of third-party RPMs. App manager configuration is required to activate the xr_script_scheduler.py script and run the third party scripts after installation.

> **Note**
>
> If you use the **autorun** configuration, the **xr_script_scheduler.py** script activates automatically.

Automatically deploy and activate third party script

NCS 1001 provides CLI commands to perform configurations and operations on the optical devices. If you want to automate the NCS 1001 node operations, you can run third party scripts through App manager.

Follow these steps to deploy and activate third party script.

Procedure

1. Use the **show script status** command to check the list of the OPS scripts that are in-built in XR.

   Example

   This command lists the status of *xr_script_scheduler* script. *Ready* status in the output means that the script checksum is verified and is ready to run.

```
RP/0/RP0/CPU0:ios#show script status
Tue Oct 24 18:03:09.220 UTC
=============================================================================================

 Name                              | Type    | Status            | Last Action |
 Action Time
---------------------------------------------------------------------------------------------

 show_interfaces_counters_ecn.py | exec    | Ready             | NEW         |
 Tue Oct 24 07:10:36 2025
 xr_data_collector.py            | exec    | Ready             | NEW         |
 Tue Oct 24 07:10:36 2025
 xr_script_scheduler.py          | process| Ready             | NEW         |
 Tue Oct 24 07:10:36 2025
=============================================================================================
RP/0/RP0/CPU0:ios#
```

2. Use the appmgr to automatically run the XR scheduler script.

   Activate the scheduler script automatically using the "autorun" option with the configuration.

   Example

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#appmgr
RP/0/RP0/CPU0:ios(config-appmgr)#process-script xr_script_scheduler
RP/0/RP0/CPU0:ios(config-process-script)#executable xr_script_scheduler.py
RP/0/RP0/CPU0:ios(config-process-script)#autorun
RP/0/RP0/CPU0:ios(config-process-script)#commit
```

   The 'autorun' configuration has been added to enable automatic activation of the process script. If you prefer manual activation/deactivation using CLI, skip the 'autorun' configuration line. See Manually deploy and activate third party script on page 153.

3. Verify the scheduler script is running.

a) Run the **show script execution** command to verify the functioning of the debug and monitoring scripts.

Example

This command displays a list of OPS scripts currently running.

```
RP/0/RP0/CPU0:ios# show script execution
Tue Oct 24 19:41:15.882 UTC
==========================================================================================

 Req. ID   | Name (type)                                    | Start
         | Duration   | Return | Status
------------------------------------------------------------------------------------------

 1698176223| xr_script_scheduler.py (process)         | Tue Oct 24 19:37:02
 2025 | 253.32s    | None   | Started

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

b) Use the **show script execution details** command to verify if the scheduler script is running.

Example

This command displays a list of OPS scripts currently running. If the scheduler script is correctly configured and activated, the scheduler script execution detail appears in the output.

```
RP/0/RP0/CPU0:ios#show script execution details
Tue Oct 25 18:01:56.590 UTC
==========================================================================================

 Req. ID   | Name (type)                                    | Start
         | Duration   | Return | Status
------------------------------------------------------------------------------------------

 1698170509| xr_script_scheduler.py (process)         | Tue Oct 25 18:01:49
 2023 | 7.68s      | None   | Started
------------------------------------------------------------------------------------------

 Execution Details:
 ------------------
 Script Name  : xr_script_scheduler.py
 Version      : 25.3.1.14Iv1.0.0
 Log location :
/harddisk:/mirror/script-mgmt/logs/xr_script_scheduler.py_process_xr_script_scheduler

 Arguments    :
 Run Options  : Logging level - INFO, Max. Runtime - 0s, Mode - Background

 Events:
 -------
 1.   Event        : New
      Time         : Tue Oct 25 18:01:49 2025
      Time Elapsed : 0.00s Seconds
      Description  : Started by Appmgr
 2.   Event        : Started
      Time         : Tue Oct 25 18:01:49 2025
      Time Elapsed : 0.11s Seconds
      Description  : Script execution started. PID (15985)
==========================================================================================
RP/0/RP0/CPU0:ios#
```

4. Copy the third party RPM files to the NCS 1001 node.
   a) Use any of the file transfer mechanisms to copy third-party RPM.

      Example

      This example shows copying the RPM to the harddisk of the NCS 1001 node using **scp**.

```
RP/0/RP0/CPU0:ios#scp
user@171.xx.xxx.xxx:/users/user/rpm-factory/RPMS/x86_64/nms-1.1-25.3.1.x86_64.rpm
 /harddisk:
Tue Oct 24 18:02:42.400 UTC
<snip>
Password:
nms-1.1-24.1.1.x86_64.rpm                                                  100%
9664   881.5KB/s   00:00
RP/0/RP0/CPU0:ios#
```

   b) (Optional) Verify the RPM files using **dir** <**filepath**>.

      Example

```
RP/0/RP0/CPU0:ios#dir harddisk:/nms-1.1-24.1.1.x86_64.rpm
Wed Oct  24 19:53:54.041 UTC
```

5. Install the third party RPM files to use the required debug and monitoring python scripts.

   The third party RPM files have the customized scripts to be executed. The third-party RPM contains two types of files:

   - One or more python scripts–For more information on developing python scripts, see IOS XR Programmability with Python and xr-python-scripts.
   - Run parameter JSON file–*xr_script_scheduler.json* has instruction for the scheduler script.

   Example

   This is an example *xr_script_scheduler.json* file. Customize this file as per your requirements.

```
[
    {
        "name": "__template_entry__.py",
       "description": ["**This is a template entry for documentation purpose.
 This entry will be ignored**",
                        "name : Name of the python script to be executed",
                        "       [string][mandatory]",
                        "description:  Description of the script",
                        "              [string or list of strings][optional:
 default empty string]",
                       "cmd_line_parameters: Script command line parameters"
 ,
                        "                     [list of strings][optional:
default Null][Example: ",
                        "env_variables: Enviromental variables to be set in
script run shell",
                        "                [list of key value pairs][optional:
default Null][Example: [['INT_NAME': 'hu0/1/0/1']]",
                      "run_policy: Script restart policy when script exits",

                        "            [string: one of
always/once/stop][optional: default 'always']",
                        "            always: restart the script every time
```

```
it exits",
                        "            once:  do not restart the script if it
exits",
                        "             stop:  stop an existing script run "
                        ],
        "cmd_line_parameters": [],
        "env_variables": [],
        "run_policy": "always"
    },
    {
        "name": "monitor_int_rx_cntr.py",
        "description": "Monitoring mgmt interface for Rx threshold of 100 ",

       "cmd_line_parameters": ["MgmtEth0/RP0/CPU0/0", "200", "-log", "debug"],

       "env_variables": [["INT_NAME", "FourHundredGigE0/9/0/0"], ["INT_NAME2",
 "FourHundredGigE0/10/0/0"]],
        "run_policy": "always"
    },
    {
        "name": "monitor_int_rx_cntr.py",
        "description": "Monitoring Fo0/0/0/0 interface for Rx threshold of
1000000 ",
        "cmd_line_parameters": ["FourHundredGigE0/0/0/0", "1000000"],
        "run_policy": "once"
    },
    {
        "name": "monitor_int_rx_cntr2.py",
        "description": "Monitoring Fo0/0/0/1 interface for Rx threshold of
5000000 ",
        "cmd_line_parameters": ["FourHundredGigE0/0/0/1", "5000000"],
        "run_policy": "always"
    },
    {
        "name": "monitor_int_rx_cntr2.py",
        "description": "Monitoring Fo0/0/0/2 interface for Rx threshold of
5000000 ",
        "cmd_line_parameters": ["FourHundredGigE0/0/0/2", "8000000"],
        "run_policy": "stop"
    }
]
```

Example

Use the **appmgr package install rpm <full RPM file path>** command to install the third-party RPMs.

```
RP/0/RP0/CPU0:ios#appmgr package install rpm
/harddisk:/nms-1.1-25.3.1.x86_64.rpm
Tue Oct 24 18:03:26.685 UTC
RP/0/RP0/CPU0:ios#
RP/0/RP0/CPU0:ios#show appmgr packages installed
Tue Oct 24 19:42:07.967 UTC
Sno Package
--- ------------------------------------------------------------
1   nms-1.1-25.3.1.x86_64
RP/0/RP0/CPU0:ios#
```

After the scripts and the run parameters file become ready, build the RPM and configure the RPM to install files at `<default exr appmgr rpm install path>/ops-script-repo/exec/<rpm name>/`. RPM build tool for TPA is available at RPM Build Tool.

> **Note**
>
> Install the scripts in directories named after the RPM for smoother execution.

6. Use the **show script status** command to verify that the scripts and the run parameter files contained in the RPM are all installed successfully and added to the script management repository.

   Example

   This output shows the status that two scripts (monitor_int_xr_cntr.py and monitor_int_rx_cntr2.py) and a run parameter file (xr_script_scheduler.json) file were installed in the third-party RPM named “nms”.

```
RP/0/RP0/CPU0:ios#show script status

Tue Oct 24 19:41:10.696 UTC
=============================================================================================

 Name                              | Type    | Status            | Last Action |
 Action Time
---------------------------------------------------------------------------------------------

 nms/monitor_int_rx_cntr.py        | exec    | Ready             | NEW         |
 Tue Oct 24 19:38:41 2023
 nms/monitor_int_rx_cntr2.py       | exec    | Ready             | NEW         |
 Tue Oct 24 19:38:41 2023
 nms/xr_script_scheduler.json      | exec    | Ready             | NEW         |
 Tue Oct 24 19:38:41 2023
 show_interfaces_counters_ecn.py | exec    | Ready             | NEW         |
 Tue Oct 24 19:33:52 2023
 xr_data_collector.py              | exec    | Ready             | NEW         |
 Tue Oct 24 19:33:52 2023
 xr_script_scheduler.py            | process| Ready             | NEW         |
 Tue Oct 24 19:33:52 2023
=============================================================================================
RP/0/RP0/CPU0:ios#
```

   After the scripts are installed, the scheduler script starts reading the run parameter JSON file and executes the required debug and monitoring scripts.

   The logs generated by the scripts are available in the directory `/harddisk\:/mirror/script-mgmt/logs/`.

7. Verify that the debug and monitoring scripts are running.

   Example

   Use the **show script execution** command to verify that the scripts are running.

```
RP/0/RP0/CPU0:ios#show script execution
Tue Oct 24 19:41:15.882 UTC
=============================================================================================

 Req. ID    | Name (type)                                  | Start
      | Duration    | Return | Status
---------------------------------------------------------------------------------------------

 1698176223| xr_script_scheduler.py (process)            | Tue Oct 24 19:37:02
```

```
 2023 | 253.32s    | None   | Started
 1698176224| nms/monitor_int_rx_cntr.py (exec)         | Tue Oct 24 19:38:43
 2023 | 152.46s    | None   | Started
 1698176225| nms/monitor_int_rx_cntr.py (exec)         | Tue Oct 24 19:38:44
 2023 | 152.03s    | None   | Started
 1698176226| nms/monitor_int_rx_cntr2.py (exec)        | Tue Oct 24 19:38:44
 2023 | 151.63s    | None   | Started
==========================================================================================================
RP/0/RP0/CPU0:ios#
```

(Optional) Use the **show script execution name** *script-name* **detail [output] [error]**

A SNMP MIBs

Topics:

Explains SNMP MIB support for Cisco NCS 1001, how to enable optical OTS trap notifications, and where to find related SNMP documentation resources.

SNMP MIBs are management information modules that

- define objects that network management systems can query on Cisco NCS 1001,
- enable platform and system monitoring functions, and
- provide trap definitions for alarms reported through SNMP.

For details about supported Management Information Bases (MIBs) and related documentation, see SNMP MIBs supported on NCS 1001.

SNMP MIBs supported on NCS 1001

This section provides details about supported SNMP MIBs on NCS 1001 and links to tools and documentation for MIB definitions, SNMP configuration, and SNMP best practices.

Use this reference to identify the supported MIBs and locate documentation for SNMP object definitions and configuration guidance.

Supported SNMP MIBs

These MIBs are supported on NCS 1001:

- CISCO-OPTICAL-OTS-MIB
- CISCO-CONFIG-MAN-MIB
- CISCO-FLASH-MIB
- CISCO-ENTITY-REDUNDANCY-MIB
- CISCO-SYSTEM-MIB
- CISCO-ENTITY-ASSET-MIB
- EVENT-MIB
- DISMAN-EXPRESSION-MIB
- CISCO-FTP-CLIENT-MIB
- NOTIFICATION-LOG-MIB
- CISCO-RF-MIB
- CISCO-TCP-MIB
- UDP-MIB
- CISCO-OTN-IF-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-OPTICAL-MIB
- CISCO-ENTITY-SENSOR-MIB

> **Note**
>
> CISCO-OPTICAL-OTS-MIB contains the SNMP traps for all the specific NCS 1001 alarms that are not related to other platforms. These alarms are reported through SNMP traps with appropriate severity and hardware port notification. Other MIBs such as CISCO-OPTICAL-MIB contains the SNMP traps for alarms that can also be raised on other platforms, for example, NCS 1002.

SNMP MIB documentation resources

This table maps each SNMP task to its documentation resource.

Table 41: SNMP MIB documentation resources

Task	Resource
Determine the MIB definitions	For details about MIB definitions, see SNMP Object Navigator.
Configure SNMP	For details about SNMP configuration, see Configure SNMP.
Understand SNMP best practices	For details about the recommended order of SNMP query, maximum cache hit, and SNMP retry and timeout recommendations, see SNMP Best Practices.

Configure SNMP traps

Use this procedure to enable optical OTS SNMP trap notifications on Cisco NCS 1001 and commit the configuration so that platform-specific alarms are reported through SNMP.

Enable SNMP traps for optical OTS alarms when Cisco NCS 1001 specific alarms must be reported to an SNMP management system.

CISCO-OPTICAL-OTS-MIB contains SNMP traps for Cisco NCS 1001 specific alarms that are not related to other platforms.

Procedure

1. Enter the configuration mode.

   Example

   ```
   configure
   ```

2. Use the **snmp-server traps optical-ots** command to enable optical OTS SNMP traps.

   Example

   ```
   snmp-server traps optical-ots
   ```

3. Commit the configuration.

Optical OTS SNMP traps are enabled, and the committed configuration reports relevant Cisco NCS 1001 alarms through SNMP.

What to do next

Verify that the SNMP management system receives trap notifications for the expected alarm conditions.