Release Notes for Cisco NCS 2000 Series, Release 10.9.x.x

First Published: 2018-08-23

Last Modified: 2023-06-26

Cisco NCS 2000 Series Release Notes

Note Explore the Content Hub, the all new portal that offers an enhanced product documentation experience.

- Use faceted search to locate content that is most relevant to you.
- Create customized PDFs for ready reference.
- Benefit from context-based recommendations.

Get started with the Content Hub at content.cisco.com to craft a personalized documentation experience.

Do provide feedback about your experience with the Content Hub.

This Release Notes document contains information about new features and enhancements, in the Cisco NCS 2000 Series platforms.

For the latest version of the Release Notes for Cisco NCS 2000 Series, visit this URL:

http://www.cisco.com/c/en/us/support/optical-networking/network-convergence-system-2000-series/products-release-notes-list.html

Cisco also provides Bug Search Tool, a web resource for tracking defects. To access Bug Search Tool, visit the following URL: https://tools.cisco.com/bugsearch.

Revision History

Table 1: Revision History

Date	Notes
June 2023	Updated with **TLS Version Support** section.
January 2021	Added the Critical Bug Fixes in Release 10.9.0.2, on page 2 section.
August 2020	Added the Critical Bug Fixes in Release 10.9.0.1 section.
August 2018	This is the first release of this publication.

Software and Hardware Requirements

Before you begin to install the software, you must check whether your system meets the following minimum software and hardware requirements:

- Hardware—Intel Core i5, i7, or faster processor. A minimum of 4 GB RAM, 100 GB hard disk with 250 MB of available hard drive space.
- One of the following operating systems:
  - Windows 7, Windows Server 2008, or later
  - Apple Mac OS X
  - UNIX workstation with Solaris Version 9 or 10 on an UltraSPARC-III or faster processor, with a minimum of 1 GB RAM and a minimum of 250 MB of available hard drive space.
  - Ubuntu 12.10
- Java Runtime Environment—JRE 1.8 and later.
- Java version 8.0
- Browser:
  - Internet Explorer
  - Mozilla Firefox
  - Safari
  - Google Chrome

Critical Bug Fixes in Release 10.9.0.2

The following critical issues have been resolved in Release 10.9.0.2:

- When more than 16 SMR modules are cascaded, power instability occurs.
- When the node type is changed from METRO-DWDM to NON-DWDM, the node automatically resets.
- CTC version is changed.

Critical Bug Fixes in Release 10.9.0.1

The following critical issues have been resolved in Release 10.9.0.1:

- In a mixed flex and legacy setup, when a circuit is created and added/dropped on a legacy node, PMI is incorrectly raised on the legacy line Rx if LOS-P alarm is present for that specific channel.
- The attribute name in CERENT-ENTITY-MIB (entityx.mib) is incorrect.
- CTC launcher version is incorrect.

The following known issues are present in R10.9.0.1:

- When NE Defaults are exported and imported without any change in R10.9.0.1, CTC throws an error message that NODE.powerMonitor.EHBATVG -57.7 is not a valid value.
- PWR-CON-LMT alarm is raised during upgrade or revert operation from R10.8 to R10.9.0.1 and the other way round.

JRE Compatibility

The JRE Compatibility table displays the JRE compatibility with NCS 2000 software releases.

New Features in Release 10.9

This section highlights the new features in Release 10.9. For detailed information of each of these features, see the user documentation.

Software Features

Note Before you dive into this release's features, we invite you to content.cisco.com to experience the features of the Cisco Content Hub. Here, you can, among other things:

- Create customized books to house information that's relevant only to you.
- Collaborate on notes and share articles by experts.
- Benefit from context-based recommendations.
- Use faceted search to close in on relevant content.

And, if you are already experiencing the Content Hub, we'd like to hear from you!

Click the **Feedback** icon on the page and let your thoughts flow!

This section lists the software features and enhancements introduced in Release 10.9.

400G-XP-LC Enhancements

- The cross-connect circuit bandwidth supported are ODU2, ODU2e, and ODU4.
- The OPM_10x10G and OPM-100G slice modes are supported for OTN cross-connect circuits.
- The new payloads supported for the OTNXC operating mode are OC192/STM64, OTU2, OTU2e, OTU4, and 100GE.
- The new payloads supported for the MXP operating mode are OC192/STM64 and OTU2e.
- The ODU4 internal ports on the 400G-XP-LC card support configuration of Pseudo Random Binary Sequence (PRBS) with all operating modes.

- The 2x150G 8QAM modulation format is configurable on the 400G-XP MXP trunk ports. It can be done by selecting M_150G as the Trunk Operating mode. The M_150G mode is not available for cross-connection and regeneration configurations. The enhancement is supported with the NCS2K-S pkg.
- The Trunk GCC0 configuration is supported on the 400G-XP-LC card. The supported GCC0 rate on the 400G-XP-LC card is 1200K. The card supports provision of one GCC0 channel for each of the trunk ports. In case of OTU4C3 (8QAM) payload, only one GCC0 channel is configurable on the second trunk port.
- The 400G-XP-LC card provides encryption capability on the OTU4 ports. This card provides confidentiality of the data, which is sent over a fiber optic communication channel, using Next Generation Cryptography. The MXP operating mode supports the encryption feature.

For more information, see the Provisioning Transponder and Muxponder Cards chapter in the *Cisco NCS 2000 Series Line Card Configuration Guide, Release 10.x.x*.

Media Channel Group Restoration

In case of a fiber cut in a path, the media channels in a media channel group (MCHG) are restored using another available path. This helps reduce the network outage time. The user has an option to shrink the media channel group after restoration to the minimum size. This is required to maintain all media channels in the same group. All the media channels inside a MCHG inherit the restoration settings of the MCHG. The feature is supported with the NCS2K-S pkg.

For more information, see the Provisioning Transponder and Muxponder Cards chapter in the *Cisco NCS 2000 Series Line Card Configuration Guide, Release 10.x.x*.

Remote TXP Shelf Node

This feature remotize the transponder present in the different nodes of the optical network. The transponder node containing a set of transponders is physically connected to the ROADM node using the external PPC. The transponder node and the ROADM nodes must be on the same IP routing domain to have a control plane running on the entire network. The feature is supported with the NCS2K-F pkg.

For more information, see the Creating Optical Channel Circuits and Prvisionable Patchcords chapter in the *Cisco NCS 2000 Series Network Configuration Guide, Release 10.x.x*.

OTDR Functionality for OPT-RAMP-C and OPT-RAMP-CE Cards

For OPT-RAMP-C and OPT-RAMP-CE cards, the direction of OSC propagation is opposite to the direction of C-band signal unlike other amplifier cards. Hence, OTDR functionality is reversed when used with OPT-RAMP-C and OPT-RAMP-CE cards. For example, when OTDR scan is started for LINE-RX direction, the scan is performed in LINE-TX direction.

TLS Version Support

The supported version of Transport Layer Security (TLS) protocol is 1.2.

Known Issue

The TNC card resets when alarm suppression is enabled over USB.

Cisco Bug Search Tool

Use the Bug Search Tool (BST) to view the list of outstanding and resolved bugs in a release.

BST, the online successor to Bug Toolkit, is designed to improve the effectiveness in network risk management and device troubleshooting. The tool allows partners and customers to search for software bugs based on product, release, and keyword, and aggregates key data such as bug details, product, and version. The tool has provision to filter bugs based on credentials to provide external and internal bug views for the search input.

The BST is available at Bug Search. To search for a specific bug, go to https://tools.cisco.com/bugsearch/bug/*bugid*. For more information on BST, see Bug Search Help.

Search Bugs in BST

Follow the instructions below to search bugs specific to a software release in BST.

Procedure

Step 1 Go to https://tools.cisco.com/bugsearch/.

You will be prompted to log into Cisco.com. After successful login, the Bug Toolkit page opens.

Step 2 To search for release specific bugs, enter the following parameters in the page:

a) Search For — Enter **ONS 15454** in the text box.
b) Releases — Enter the appropriate release number.
c) Show Bugs — Select **Affecting or Fixed in these Releases**.

Step 3 Press **Enter**.

Note:

- By default, the search results include bugs with all severity levels and statuses. After you perform a search, you can filter your search results to meet your search requirements.
- An initial set of 25 search results is shown in the bottom pane. Drag the scroll bar to display the next set of 25 results. Pagination of search results is not supported.

Short Description