Release Notes for Cisco NCS 2000 Series, Release 11.0

First Published: 2019-03-08

Last Modified: 2023-06-12

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 platforms.

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.
March 2019	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

Documentation Roadmap

Use the documentation roadmap to quickly access publications of Cisco NCS 2000 Series, Release 11.0. https://www.cisco.com/c/en/us/td/docs/optical/15000r10_0/ncs/doc_roadmap/b-ncsroadmap10xx.html

JRE Compatibility

The table displays the JRE compatibility with software releases.

Supported Pluggables

The document at the following URL lists the GBIC, SFP, SFP+, QSFP, XFP, CXP, CFP, and CPAK modules that are supported on the Cisco platforms:

Important Notes

Changes in CTC

In the Circuits tab of the network view, node view, shelf view, card view, or the NFV view, circuits are no longer selected automatically in the right circuit pane when you select one or more circuits in the left circuit pane. You need to manually select the circuits in the right pane.

Upgrade Limitation

During a software upgrade from Release 10.7.0.2 to Release 11.00 some of the subtending shelves may not upgrade. To overcome this issue, perform a soft reset of the control cards of the impacted shelves.

New Features in Release 11.0

This section highlights the new features in Release 11.0. For detailed information of each of these features, see the user documentation.

Hardware

TNCS-2 and TNCS-2O Cards

The cards work in redundant mode with another TNCS-2, TNCS-2O, TNCS, TNCSO, or TNCE cards. The TNCS-2 and the TNCS-2O cards can replace the TNCS-2, TNCS-2O, TNCS, TNCSO, or TNCE cards in any chassis. The TNCS-2O has an optical module that performs Optical Time Domain Reflectometry functions with the internal module or daughter card on two of the OSC ports.

For more information, see the Installing the Control Cards chapter in the .

TNCS-O Card Support

For more information, see the Installing the Control Cards chapter in the .

Support for SM Pluggable

The ONS-SI-100-LX-10= and ONS-SE-100-LX-10= pluggables are supported on NCS 2015-ECU for MSM.

The Carrier Loss (CARLOSS) alarm is not raised on the ONS-SI-100-LX-10= and ONS-SE-100-LX-10= pluggables.

For more information, see the .

Pluggable Port Module Support

The supported pluggables are QSFP-40G-SR-BD and QSFP-40/100G-SR-BD. The 400G-XP card supports QSFP-40G-SR-BD and QSFP-40/100G-SR-BD; the MR-MXP card supports QSFP-40G-SR-BD.

Note Power monitoring is not supported on Version 1 and Version 2 for the QSFP-40G-SR-BD pluggable. Power monitoring support is available from Version 3 onwards.

For more information, see the .

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 11.0.

Support for Regenerator Constraints

Based on the optical validation, the control plane sets the best path between the source and the destination. If a path with a regenerator is not available, the control plane uses the regenerator present in the network while setting up the path. For using a regenerator, the optical path needs to be validated. If the optical validation fails, then, the regenerator cannot be used, and the circuit creation fails. If validation is not supported, path constraints and regenerator constraints can be added to path request (main, protected or restored paths). The user can include a regen location on a service path of interest.

For more information, see the Node Reference chapter in the .

OTDR Support for TNCS-2O Cards

A TNCS-2O card has an optical module that provides Optical Time Domain Reflectometer (OTDR) measurement, ORL measurement, and standard Optical Service Channel (OSC) capability on two ports. These capabilities are available on up to four ports for each shelf; a shelf can have two TNCS-2O cards. About reflection reports, it is now possible to start a scan in auto mode requesting for new and legacy reflection loss reports.

For more information, see the Turning Up a Node and Manage the Node chapter in the .

400G-XP-LC Enhancements

- The OTNXC operating mode on the 400G-XP-LC card supports encryption.
- The new payloads supported for the MXP operating mode are FC-10G, FC-8G, and 40GE.
- The OPM_2x40G_2x10G slice mode can be configured in the MXP operating mode for 40GE payloads.
- LLDP support—The source MAC address of 10GE, 100GE, or 40GE ports can be retrieved after an LLDP packet is received on the client port. LLDP filtering is enabled or disabled on the 10GE, 100GE, or 40GE ports using the Provisioning > Line > Ethernet tab in CTC.
- Third Party Certificates - The 400G-XP-LC card supports the generation of a Certificate Signing Request (CSR) and the installation of Locally Significant Certificates (LSCs) that can be used to authenticate the

peer card connection. Third party certificates also referred to as Locally Significant Certificates (LSCs) are certificates that are signed by a Certification Authority (CA) other than Cisco Certificate Authority. LSCs allow customers to have their own Public Key Infrastructure (PKI) to provide better security, to have control of their own CA, and to define policies, restrictions, and usages on the generated certificates.

For more information, see the Provisioning Transponder and Muxponder Cards chapter in the .

ANS APC Skipping

The upgraded NE update XML file imported on the CTC for the respective NCS 2000 node will import the new ANS parameters and settings for the new degree or modules. The existing ANS parameters or module settings are not impacted. This prevents unintended changes to the APC corrections to the existing degree and its associations.

For more information, see the Node Reference chapter in the .

8QAM Support on non-SSON Networks

The 8QAM mode offers a better Signal to Noise ration (SNR) performance and is also required for non-SSON networks where MSTP modules such as 80-WXC-C, 40-SMR1-C, and 40-SMR2-C are installed. In 8QAM mode, the two carriers must follow the same path and the distance in the frequency of the two carriers must be minimized to avoid a large skew between them. In SSON networks, this is already managed by the control plane, because the two carriers are part of the same media channel. In non-SSON networks, this is not automatically managed by the control plane and the user must manage these constraints.

NCS 1004 Alien Wavelength Support

The following trunk modes are added to NCS 1004 alien wavelength to support the different configuration of payloads and modulation provided by NCS 1004.

- 200G
- 300G 3bps
- 300G 3.4375bps
- 400G
- 500G
- 600G

For 300G payloads, information related to bit per symbol is also added that can be configured using the NCS 1004 CLI. This configuration implies a different signal spectrum width that must be taken into account when a new media channel is created.

For more information, see the Creating Optical Channel Circuits and Provisionable Patchcords chapter in .

TLS Version Support

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

TL1 Commands

The TL1 commands introduced in R11.0 are:

- ENT-OTDRLOSSREFLSCAN
- RTRV-NEDFLT-ALSPARAM
- RTRV-NEDFLT-OPTSTH
- RTRV-OTDRRXORLPARAMS
- RTRV-OTDRSCANPOINTSHEADER
- RTRV-OTDRSCANPOINTSLIST
- RTRV-OTDRSCANSTATUSDIR
- RTRV-PATH-OCH
- RTRV-RGNCONSTRAINT-CPS
- RTRV-RGNCONSTRAINT-MCH
- RTRV-RGNCONSTRAINT-UNICFG
- SET-NEDFLT-ALSPARAM
- SET-NEDFLT-BERLEVEL
- SET-NEDFLT-DWDMCONFIG
- SET-NEDFLT-ETHERPARAM
- SET-NEDFLT-FECMODE
- SET-NEDFLT-NEGEN
- SET-NEDFLT-OPTSTH
- SET-NEDFLT-OTNLINE
- SET-NEDFLT-OTNPPR
- SET-NEDFLT-OTNTH
- SET-NEDFLT-PMTH
- SET-NEDFLT-PROTECTION
- SET-NEDFLT-SNMPMIB
- SET-NEDFLT-SOAKTIME
- SET-NEDFLT-SOFTWARE
- SET-NEDFLT-SYNCCONF
- SET-NEDFLT-WSON
- SET-OTDRRXORLPARAMS
- SET-RGNCONSTRAINT-CPS
- SET-RGNCONSTRAINT-MCH
- SET-RGNCONSTRAINT-UNICFG

Alarms

The alarm introduced in Release 11.0 is FPGA-UPGRAGE-FAILED.

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

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

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)

© 2023 Cisco Systems, Inc. All rights reserved.