Release Notes for Cisco NCS 2000 Series, Release 10.7.x.x

First Published: 2017-09-12

Last Modified: 2018-11-09

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
November 2018	Added the Critical Bug Fixes section for R10.7.0.2.
March 2018	Added the Critical Bug Fixes section for R10.7.0.1.
September 2017	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

Critical Bug Fixes in R10.7.0.2

The following critical issues have been resolved in Release 10.7.0.2:

Caveat ID Number	Description
CSCvj08074	When a SSC is added in a 48 VDC environment, it raises a Extreme Low Voltage Battery (EHIBATVG) alarm that cannot be cleared.
CSCvj11222	The Circuit Diagnostic of CPO R10.7.0.1 does not work with network elements of NCS 2000.
CSCvj13778	If one or more clients continously tries to connect to the SOCKS server, the server msg pipe is filled causing the tProxyS task to be blocked forever.
CSCvj67003	The Circuit Diagnostic of CPO shows blank with the network elements of NCS 2000 in secure mode.
CSCvj33045	When the node is upgraded from R10.6.0.1 to R10.7.0.2, traffic is affected as RAMAN calibration is not completed.

Caveat ID Number	Description
CSCvj37433	CTC does not report the newly created LMPs under the LMP pane.
CSCvj48759	Controllers reboot periodically in a mixed release with WSON circuit that is down.
CSCvj76671	When the node is upgraded from R10.6.0.1 to R10.7.0.2 with ECU-S on NCS 2006, the voltage thresholds are replaced with incorrect values.

Critical Bug Fixes in R10.7.0.1

The following critical issues have been resolved in Release 10.7.0.1:

- The client ports are not listed during WSON OCHCC creation.
- When circuits are restored, the ROADM node that has twenty degree restarts.
- An 'Operation Failed' error message occurs while creating a media channel group containing an OCHNC circuit.
- When the TNC card force reloads, NE discovery takes longer time on CTC after the card switches over.
- When the 24 SMR9 FS card is reset, the traffic is affected on the AD circuits.
- The restoration of OCH Trail causes the node controller to reboot.
- When ONS 15454 M12 and ONS 15454 M6 node controllers with TCC3 card and 40-WSS card are upgraded to R10.7.0.1, the nodes perform roll reboot.
- The MR-MXP card does not recognize the QSFP-40G-LR4 pluggable.
- The SSON circuit restoration does not work on the 20-SMR card due to wrong carrier allocation.
- The Optical Power Failure Low (OPWR-LFAIL) alarm is raised on the SMR-20 card after the restoration or revert of OCHCC WSON circuit.
- The circuit creation fails from CTC NFV view as the source and destination ports are not completely defined.
- The TNC card resets when APC domains are selected and Refresh button is clicked in the **Card View** > **Maintenance** > **APC** > **Refresh**.

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:

New Features in Release 10.7

This section highlights the new features in Release 10.7. For detailed information of each of these features, see the user documentation.

Hardware

Pluggable Port Module Support

The 400G-XP card supports the QSFP-40G-SR4 and the QSFP-100G-SM-SR= pluggable.

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 10.7.

Third Party Certificates on MR-MXP Card

The MR-MXP 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.

A public-private key is generated inside the target system and then the generated public key along with other product or customer specific information (collectively called as a Certificate Signing Request) is then sent to be signed by a CA (customer owned or a third party) after which, the signed certificates are imported or installed via a trusted and secure channel or method into the target system. After the signed certificates are installed, it can be used in conjunction with the private key to authenticate any remote connection before exchanging sensitive information with the same.

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

400G-XP-LC Card Enhancements

- Support for OTU4 traffic- This payload is supported only on the ONS-QSFP28-LR4, QSFP-40G-SR4, and QSFP-100G-SM-SR pluggables. The payload can be provisioned for the OPM_100G slice mode for any trunk configuration.
- Support of 400G-XP-LC cards on Cisco NCS 2002- One 400G-XP-LC card can be installed in the Cisco NCS2002 DC chassis that is powered by NCS2002-DC or NCS2002-DC-E.
- The 400G-XP-LC card is interoperable with NCS55-6X200-DWDM-S card supported on Cisco NCS 5500 Series and NCS4k-4H-OPW-QC2 card supported on Cisco NCS 4000 Series.

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

Y-cable Support for 200G-CK-LC and 10x10G-LC Cards

Y-cable protection is supported when the 200G-CK-LC card is configured in TXP-100G operating mode and the 100G client CPAK ports are provisioned with 100GE payload. This configuration uses the CPAK-100G-LR4 pluggable.

Y-cable protection is supported when the 10x10G-LC card is configured in MXP-10x10G operating mode with 200G-CK-LC card and the 10x10G-LC card is provisioned with 10GE, OC-192/STM-64 payloads. This configuration uses the ONS-SC+-10G-LR and ONS-SC+-10G-SR pluggables.

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.

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

MR-MXP Configuration for 100G and 200G OTU4

2X10GE+2X40GE payload is supported in MXP-100G operating mode which comprises of 200G-CK-LC and MR-MXP cards. This payload is supported only when the sub OpMode in MR-MXP card is OPM_2x40G_2x10G.

OTU4 payload is supported in MXP-CK-100G operating mode which comprises of 200G-CK-LC and MR-MXP cards. This payload is supported only when the sub OpMode in MR-MXP card is OPM_100G.

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

Configuring FIPS and CC

In Configuring Management of FIPS and CC mode, Chrome browser settings and Firefox browser settings have changed.

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

SSON

SSON allows the user to create more than 96 channels in a span. Using SSON, the circuits are placed closer to each other if they are created within the media channel group. SSON circuit is created only if the source and destination nodes have the SSON package.

SSON supports the following types of circuits:

- Media Channel - Establishes a connection between two optical nodes.

- Media Channel Group - Enables the user to reserve a portion of the spectrum along the path, between the source and destination nodes. It is a container that can include one or more media channels.
- Carrier - Optical channel that carries the client payload.

The Bandwidth Occupation graph allows the user to view the spectrum reservation and spectrum availability across the entire C-band.

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

Standardize wavelength identification using GHz

The user can view information about frequency of light in nanometer and bandwidth information in GHz.

For more information, see

TL1 Commands

- DLT-MCH
- DLT-MCHG
- DLT-MCHXC
- ED-MCH
- ED-MCHG
- ENT-MCH
- ENT-MCHG
- OPR-MCH
- OPR-MCHG
- RLS-MCH
- RLS-MCHG
- RTRV-BWP-ETH
- RTRV-CARRIERXC
- RTRV-CKTINFOCARRIER
- RTRV-COS-ETH
- RTRV-CRS-ETH
- RTRV-HOP-MCH
- RTRV-HOP-MCHG
- RTRV-L2-ETH
- RTRV-MCH
- RTRV-MCHFAILUREINFO

- RTRV-MCHG
- RTRV-MCHGFAILUREINFO
- RTRV-MCHGPATH
- RTRV-MCHGXC
- RTRV-MCHPATH
- RTRV-MCHTRAILADIT
- RTRV-MCHXC
- RTRV-NE-APC
- RTRV-NE-WDMANS
- RTRV-PATH-OCH
- RTRV-SLV-WDMANS
- RTRV-SRLG-WDMSIDE
- RTRV-STCN-REP
- RTRV-VLB-REP
- SET-HOP-MCH
- SET-HOP-MCHG

Alarms

The alarm introduced in R10.7 is NO-SHARED-CIPHERS alarm.

For more information, see the Alarm Troubleshooting chapter in the .

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.