Release Notes for Cisco NCS 2000 Series, Release 10.6.2

First Published: 2017-04-28

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

Date	Notes
April 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

Important Notes

- **Hard Reset in WSE and AR-XP cards**

  When the software version of the node is changed from Release 10.6.2 to releases prior to 10.6.1, the card undergoes a hard reset. Hence, it is recommended to perform this operation in the maintenance window.
- **CTC Error**

  The text of Error RC15 is incorrect in CTC and will be corrected in a future release.

Supported Firmware Version of MF-6RU and MF10-6RU Shelves

The supported bootrom version is 006 and kernel version is 003.

When the node software is upgraded, the firmware version of the MF-6RU and MF10-6RU shelves are not upgraded automatically. To upgrade the firmware version of the MF-6RU and MF10-6RU shelves, see the "DLP-G792 Performing a Firmware Upgrade on Passive Shelves" task in the .

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 10.6.2

This section highlights the new features in Release 10.6.2. For detailed information of each of these features, see the user documentation.

Hardware

- **Pluggable Port Module Support**

  The MR-MXP card supports the ONS-QSFP-4X10-MLR= pluggable.

  The 400G-XP card supports ONS-QC-16GFC-SW= and ONS-QSFP-4X10-MLR= pluggable.

  Note The maximum transmit launch power (per lane) of the ONS-QC-16GFC-SW= pluggable is +1dBm (the lowest being -7.6dBm).

  For details, see the guide.

- **TCC2 / TCCP2 Card Support**

  The nodes with the TCC2/TCC2P cards in releases prior to R10.6.2 cannot be upgraded to R10.6.2 as the size of the software package exceeds the size of the TCC2/TCC2P flash drive. Hence, R10.6.2 does not have the TCC2/TCC2P software package. If the user wants to continue with the ONS 15454 chassis, it is recommended to use the TCC3 control card. If the user wants to upgrade to a ONS 15454 M6 or NCS 2015 chassis, it is recommended to use the TNCS or TNCS-O control cards.

  ONS 15454 is supported in Flex NCS node as MSM-SSC only to NCS 2006 or NCS 2015 MSM-NC. Only TCC3 controller is supported on the ONS 15454 shelf.

  For more information on TCC2 / TCCP2 card support, see the *Installing the Control Cards* chapter in the *Cisco ONS 15454 DWDM Control Card and Node Configuration Guide, Release 10.x.x.*

Software features

This section lists the software features and enhancements introduced in Release 10.6.2.

- **MR-MXP Enhancements**

  OC192/STM64 and OTU2 client payloads are supported on the MR-MXP card in MXP-200G, MXP-10x10G-100G, MXP-CK-100G, and MXP-100G operating modes. OC192/STM64 and OTU2 client payloads are supported only when the sub OpMode is OPM_10x10G on the MR-MXP card.

  For more information on the MR-MXP enhancements, see the *Provisioning Transponder and Muxponder Cards* chapter in the

- **Node Recovery Enhancements**

  Two enhancements have been introduced to recover the node without traffic loss.

  - Provisioning Database: When provisioning database loss occurs, the following alarms are raised at the node level.

    - The BAD-DB-DETECTED critical alarm is raised when provisioning database loss occurs during reboot of control cards, switchovers, or upgrades. To clear this alarm, restore a previously saved database or use the "Reset NE to Factory Defaults" option in CTC.
    - The NODE-FACTORY-MODE critical alarm is raised when provisioning database loss occurs during system mode conversions, reset to factory defaults, or in new installations. To clear this alarm, restore a previously saved database or use the Rebuild DB option in the Maintenance > Database tabs in CTC.

  - System Database: When system database loss occurs on the active or standby control card, an INVALID SYSDB alarm is raised on the control card. To clear the alarm do any of the following actions:

    - If the alarm is raised only on the active control card, reboot the active card.

    - If the alarm is raised only on the standby control card, reboot the standby card.

    - If the alarm is raised on both the active and standby control cards, contact TAC for support.

  For more information about the node recovery feature, see the *Maintaining the Node* chapter in the

- **400G-XP LC Enhancements**

  - Support for 16G-Fiber Channel payload- This payload is supported only on the ONS-QC-16GFC-SW= pluggable. A new operating mode, OPM_6x16G_FC is introduced to support this payload on ports 1, 2, 3, 4, 5, and 6. This operating mode can be provisioned on any slice, with trunk configuration set to M_100G and M_200G.

  - Support for OTU2 payload- This payload is supported only on the QSFP-4X10G-MLR pluggable. The payload can be provisioned for the OPM_10x10G slice mode for any trunk configuration.

  - Support for trunk PM parameters-Second Order PMD (SOPMD) and Polarization Depended Loss (PDL).

  For more information about the payloads, see the *Provisioning Transponder and Muxponder Cards* chapter in the

- **Optical PM Monitoring on QSFP+**

  The optics PM parameters are enabled on QSFP+ ports of the MR-MXP cards.

- **ROADM Configurations**

  A set of MF-6AD-CFS passive splitter/coupler modules are connected to the SMR-20 EXP-TX/RX ports to obtain a colorless (and gridless) directional A/D stage. The interconnection can be done either with a break-out cable, ONS-MPO-16-LC2=, or with an adapter module, MF-MPO-16LC. The various configurations are colorless terminal ROADM, 2-degrees colorless ROADM and 8-degrees colorless ROADM.

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

- **Multivendor Interoperability**

  The 200G-CK LC can be configured to interoperate with other vendor devices.

- **Duplicate Node Controller**

When a TNC/TNC-E/TSC/TSC-E/TNCS/TNCS-O node controller connects to the same switch where an NCS 2006 or NCS 2015 node controller exists, both the node controllers raise the critical Duplicate Node Controller (DUP-NC) alarm. The subtending shelves of both the node controllers raise the Shelf Communication Failure (SHELF-COMM-FAIL) alarm. Both the node controllers and their subtending shelves shut down their ports on ASIC towards the MSM ports in ECU. However, the traffic is not affected. This feature enables the original node to operate seamlessly in case of such misconfigurations, without the risk of its subtending shelves treating the new node controller as its primary.

For more information on the duplicate node controller, see the *Managing the Shelf* chapter in the

- **Thirty Party Certificates for WSE Card**

  From Release 10.6.2, the WSE card supports the generation of a CSR and installation of Locally Significant Certificates (LSCs) that can be used to authenticate the peer card connection.Third Party Certificates also called Locally Significant Certificates (LSCs) are certificates that are signed by a Certification Authority (CA) other than Cisco Certificate Authority (CA). LSCs allow customers to have their own public key infrastructure (PKI) to provide better security and 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 get signed by a CA (customer owned or a third party). Once signed, the signed certificates are imported or installed (via a trusted and secure channel/method) into the target system. Once installed, the signed certificates in conjunction with the Private Key can be used to authenticate any remote connection/peer before exchanging sensitive information with the same.The Certificate Signing Request (CSR) is exported from the target system and the signed certificates are imported/installed back into the target system.

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

- **OTDR Enhancements**

  - The OTDR scan starts automatically after the LOS alarm is raised and cleared, To perform this, enable the Automatic Scan on LOS Raise and Clear radio button. For more information, see the
  - The default value for the automatic OTDR scan to begin is 3 minutes. For more information, see the *Cisco ONS 15454 Network Configuration Guide, Release 10.x.x*
  - Location [km] in the Reflection table or the Insertion Loss table is enhanced with the Accuracy (km) details.

    For more information, see the *Manage the Node* document.

- **MSM Supported Configurations**

  The following configurations are supported:

  - 40 400G-XP-LC cards provisioned with 10GE payloads. The total number of client interfaces is 1600.
  - 20 400G-XP-LC, 36 200G-CK-LC, and 72 MR-MXP cards provisioned with 10GE payloads. The total number of client interfaces is 1520.
  - 70 400G-XP-LC cards provisioned with 100GE payloads. The total number of client interfaces is 280.
  - 20 400G-XP-LC cards provisioned with 100GE payloads along with 36 200G-CK-LC and 72 MR-MXP cards provisioned with 10GE payloads. The total number of client interfaces is 800.

Recommendations have been provided for optimum system performance.

For more information about this feature, see the *Provisioning Transponder and Muxponder Cards* chapter in the

- **Alarms**

  The alarms introduced in 10.6.2 are:

  - USB-PORTS-DOWN
  - LOCAL-CERT-CHAIN-VERIFICATION-FAILED
  - PEER-CERT-VERIFICATION-FAILED
  - EPROM-SUDI-SN-MISMATCH
  - LOCAL-CERT-EXPIRED
  - INVALID-SYSDB
  - NODE-FACTORY-MODE
  - BAD-DB-DETECTED
  - LOCAL-CERT-ISSUED-FOR-FUTURE-DATE
  - LOCAL-CERT-EXPIRING-WITHIN-30-DAYS
  - LOCAL-SUDI-CERT-VERIFICATION-FAILED
  - LSC-NOT-PRESENT-MIC-IN-USE

  For more information about the alarms , see the *Alarm Troubleshooting* chapter of the

- **TL1 Commands**

  The TL1 commands introduced in 10.6.2 are:

  - RTRV-EQPT-HOLDERTL1

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.