Release Notes for Cisco ONS 15454, ONS 15454 M2, and ONS 15454 M6 DWDM, Release 10.0.2.x

First Published: 2014-09-26

Last Modified: 2014-11-28

Text Part Number: OL-32786-02

This Release Notes document contains information about new features and enhancements, in the platforms. For the latest version of the Release Notes for , visit this URL:

For detailed information regarding features, capabilities, hardware, and software introduced in this release, see the guides listed in the "Additional References" section.

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

This chapter includes these topics:

Revision History

Date	Notes
November 2014	Revised the part number and added the Critical Bug Fixes in Release 10.0.2.1, on page 2 section.
September 2014	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 10.0.2.1

The following critical issues have been resolved in Release 10.0.2.1:

- CTC becomes slow and does not allow access to the node during the node upgrade from 9.6.0.5 to 10.0.2.
- The network element loses connectivity with CTC after the node is upgraded from 9.6.0.5 to 10.0.2. The control card is also reset and the EQPT-FAIL alarm is raised on the control card.
- The USB-WRITE-FAIL alarm is raised on the node controller when a bulk performance monitoring parameter query is run on a large multi-shelf configuration.
- The TNC card might reset during the node upgrade from 9.6.0.5 to 10.0.2.

Critical Bug Fixes in Release 10.0.2

The following critical issues have been resolved in Release 10.0.2:

- While tuning the RAMAN-COP card, the power level of the Raman pump does not change.
- When an OTUk-LOF alarm is raised at the trunk port of a 100G-LC-C or 100G-CK-C card, traffic loss occurs.
- The OSC on the TNCE card goes down on a node that has an active TNC card and standby TNCE card.

New Features for Release 10.0.2

This section highlights new features for Release 10.0.2. For detailed documentation of each of these features, see the user documentation.

Software

These software enhancements have been introduced in Release 10.0.2.

VTXP Enhancements

- The user can provision an OCH CC circuit using the DWDM network functional view between the MSTP transponder client interface and the CRS-1 router PLIM interface (10G and 100G ethernet controller). OCH trail circuits are created between the router and MSTP interfaces as a result of an OCH CC circuit creation between the two interfaces.

CTC Enhancements

- CTC displays the circuit constraints of the circuit in the graphical view of the Circuit Maintenance perspective of the DWDM network functional view. The user can also modify the circuit constraints of the circuit being edited in this view. These modified circuit constraints are applied to the circuit only after an automatic circuit restoration or a manual reroute.
- CTC displays the link direction in the circuit map for Link Management Protocol (LMP) links between the router PLIM interface and the OCH ports on the MTSP node. This is also applicable to the internal patchcords between the trunk interface and the OCH ports of the MSTP node.
- The Change drop port admin state field is set to the OOS,DSBLD state by default in the circuit deletion confirmation dialog box in CTC.
- CTC allows tuning of the router PLIM interface by specifying the channel ID, frequency or the wavelength.
- CTC displays the ethernet statistics that are retrieved from the ethernet controllers on the router. The information is displayed in a tabular format.

WSON Enhancements

- The user can configure optical validation threshold values for the protected GMPLS circuits.

Non-continuous Loopback Support on 100G Cards

The loopback and drop facility is supported on the 100G-LC-C, 10x10G-LC, CFP-LC, and 100G-CK-C cards as follows:

1. Trunk facility loopback (drop) and client facility loopback (drop) is supported on:

    - 100G-LC-C cards configured in the TXP mode (with CXP client pluggable) for OTU4 and 100GE client payloads.

    - 100G-CK-LC configured in the TXP mode (with CPAK client pluggable) for OTU4 and 100GE client payloads.

2. Backplane facility loopback (drop) is supported on:

    - 100G-LC-C and CFP-LC configured in the TXP mode (with CFP client pluggable) for OTU4 and 100GE client payloads.

    - 100G-CK-C and CFP-LC configured in the TXP mode (with CFP client pluggable) for OTU4 and 100GE client payloads.

New ROADM Configurations

Four new A/D ROADM configurations are supported for 48 channel 100 GHz systems.

Documentation Updates

In the Cisco Network Configuration Guide, the GMPLS view is called as the Circuit Creation view and the NFV view is called as the Circuit Maintenance view.

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.

Additional References

Related Documents

Use this document in conjunction with the other release-specific documentation listed in the table below:

Technical Assistance

Link	Description
http://www.cisco.com/support	The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.

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.