



Release Notes for Cisco ONS 15310-CL Release 7.2



Note

The terms "Unidirectional Path Switched Ring" and "UPSR" may appear in Cisco literature. These terms do not refer to using Cisco ONS 15xxx products in a unidirectional path switched ring configuration. Rather, these terms, as well as "Path Protected Mesh Network" and "PPMN," refer generally to Cisco's path protection feature, which may be used in any topological network configuration. Cisco does not recommend using its path protection feature in any particular topological network configuration.

August 2007

Release notes address closed (maintenance) issues, caveats, and new features for the Cisco ONS 15310-CL. For detailed information regarding features, capabilities, hardware, and software introduced with this release, refer to Release 7.0 of the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*, *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Guide*, and *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* and Release 7.2 of the *Cisco ONS SONET TLI Command Guide*. For the most current version of the Release Notes for Cisco ONS 15310-CL Release 7.2, visit the following URL:

http://www.cisco.com/en/US/products/hw/optical/ps2001/prod_release_notes_list.html

Cisco also provides Bug Toolkit, a web resource for tracking defects. To access Bug Toolkit, visit the following URL:

http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

Contents

[Changes to the Release Notes, page 2](#)

[Caveats, page 2](#)

[Resolved Caveats for Release 7.2, page 4](#)

[New Features and Functionality, page 5](#)

[Related Documentation, page 5](#)



Corporate Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2006 Cisco Systems, Inc. All rights reserved.

[Obtaining Documentation and Submitting a Service Request, page 6](#)

[Obtaining Documentation and Submitting a Service Request, page 6](#)

Changes to the Release Notes

This section documents supplemental changes that have been added to the *Release Notes for Cisco ONS 15310-CL Release 7.2* since the production of the Cisco ONS 15310-CL System Software CD for Release 7.2.

The following changes have been added to the release notes for Release 7.2.

Changes to Caveats

The following caveat has been added.

[CSCse85355](#)

[CSCsd52665](#)

[CSCsd56328](#)

Caveats

Review the notes listed below before deploying the ONS 15310-CL. Caveats with tracking numbers are known system limitations that are scheduled to be addressed in a subsequent release. Caveats without tracking numbers are provided to point out procedural or situational considerations when deploying the product.

Maintenance and Administration



Caution

VxWorks is intended for qualified Cisco personnel only. Customer use of VxWorks is not recommended, nor is it supported by Cisco's Technical Assistance Center. Inappropriate use of VxWorks commands can have a negative and service affecting impact on your network. Please consult the troubleshooting guide for your release and platform for appropriate troubleshooting procedures. To exit without logging in, enter a Control-D (hold down the Control and D keys at the same time) at the Username prompt. To exit after logging in, type "logout" at the VxWorks shell prompt.

CSCse96077

In Release 7.2, when either you remove and then reinsert an I/O card, or a small burst of defects occurs for a very short period (less than 1 sec), false TCAs can be triggered that indicate line or traffic problems on an I/O port. Once triggered, the TCAs will be raised every 15 mins, after the 15 min pm report. There are no alarms for the associated ports. Traffic is not affected.

The cards affected are:

ONS 15454 DS1, DS1_E1_56, DS3 (including DS3, DS3N, DS3E, DS3NE), DS3_EC1, DS3XM, DWDM, E1, E1_42, OC3-8, OC12-4, MRC-12, OC192XFP; and ONS 15310-CL and ONS 15310-MA IO ports.

There are two workarounds:

1. Place the affected ports in OOS-DSBLD and then back to IS. This clears the problem for the specific port on the card, but the traffic will be down during the period of OOS-DSBLD.
2. Soft reset the card with problem ports. This clears the problem on all ports on the card. Soft reset might cause a protection switch if any port on that card or the card itself is in a protection group.

You can switch all protected ports away from the card that is to be soft-reset. In this case you can do manual switches away from the ports on that card, or in the case of an equipment switch, away from the equipment to be reset.

You can also perform a soft reset without any pre-action. This might result in protection switches of all active protected ports on that card. In the case of an equipment protection group resetting, the active equipment might incur a protection switch. The switch time will not exceed 60 ms.

For unprotected ports or card equipment, traffic will not be affected.

This issue will be resolved in a future release.

CSCsd52120

Disabling a member circuit other than the first member of a VCAT VCG, does not bring the traffic down. This issue will be resolved in Release 8.0.

CSCeh84908

A CTC client session can disconnect from an ONS node during simultaneous deletion of large numbers of VT level circuits (3000+). Connectivity to the node will recover without any user action. If the condition persists, restart the CTC session to reconnect. This issue is under investigation.

Alarms

CSCse85355

The NE should report alarms or conditions on ingress port not on any internal ports. Alarm detected at the internal ports (TERM) side will be ingress map to the MON side. So the NE raises the STS-MON/VT-MON and STS-TERM/VT-TERM alarms or conditions on the STS-MON/VT-MON ports, irrespective of the actual detection port (MON or TERM). If the user wants the customized severity to be reflected for a specific STS/VT alarms, the alarm profile entities of both STS-MON and STS-TERM, if available, should be changed to the same severity.

CSCsd52665

The NE should report alarms or conditions on ingress port not on any internal ports. Alarm detected at the internal ports (TERM) side will be ingress map to the MON side. So the NE raises the STS-MON/VT-MON and STS-TERM/VT-TERM alarms or conditions on the STS-MON/VT-MON

ports, irrespective of the actual detection port (MON or TERM). If the user wants the customized severity to be reflected for a specific STS/VT alarms, the alarm profile entities of both STS-MON and STS-TERM, if available, should be changed to the same severity.

CSCsd56328

The NE should report alarms or conditions on ingress port not on any internal ports. Alarm detected at the internal ports (TERM) side will be ingress map to the MON side. So the NE raises the STS-MON/VT-MON and STS-TERM/VT-TERM alarms or conditions on the STS-MON/VT-MON ports, irrespective of the actual detection port (MON or TERM). If the user wants the customized severity to be reflected for a specific STS/VT alarms, the alarm profile entities of both STS-MON and STS-TERM, if available, should be changed to the same severity.

Path Protection Functionality

CSCee53579

Traffic hits can occur in an unprotected to path protection topology upgrade in unidirectional routing. If you create an unprotected circuit, then upgrade the unprotected circuit to a path protection circuit using Unprotected to path protection wizard, selecting unidirectional routing in the wizard, the circuit will be upgraded to a path protection circuit. However, during the conversion, traffic hits on the order of 300 ms should be expected. This issue will not be resolved.

TL1



Note

To be compatible with TL1 and DNS, all nodes must have valid names. Node names should contain alphanumeric characters or hyphens, but no special characters or spaces.

Resolved Caveats for Release 7.2

The following items are resolved in Release 7.2.

There are no new resolved items in Release 7.2.

Common Control Cards

CSCsf13376

CRC threshold configuration and detection feature is broken for release 7.2. Excessive CRC errors does not cause CRC trigger action to take effect in this release 7.2. No workaround available. This issue is resolved in Release 8.0.

New Features and Functionality

This section highlights new features and functionality for Release 7.2. For complete documentation of each of the features of the ONS 15310-CL, consult the user documentation.

New Software Features and Functionality

Network Circuit Automatic Routing Overridable NE Default

The Network Circuit Automatic Routing Overridable NE default makes it possible to set by default whether or not a user creating circuits can change (override) the automatic circuit routing setting (also provisionable as a default).

The new NE default supporting this feature is:

```
CTC.circuits.RouteAutomaticallyDefaultOverridable
```

This default works in combination with the existing circuit routing default:

```
CTC.circuits.RouteAutomatically
```

The overridable option enables network administrators to manage how circuits are created on a network-wide basis. For example, if the Automatic Circuit Routing default is set to FALSE (the check box is unchecked by default), then setting the Network Circuit Automatic Routing Overridable default to FALSE ensures that manual circuit routing is enforced for all users creating circuits (the default is not overridable by the user). When the Network Circuit Automatic Routing Overridable default is set to TRUE (the factory configured setting) users can click in the Automatic Routing check box to change the automatic routing setting if they wish.

When the Route Automatically check box is not selectable during circuit creation, the following automatic routing sub-options will also be unavailable:

- Using Required Nodes/Spans
- Review Route Before Creation

Like the Automatic Circuit Routing default, the Network Circuit Automatic Routing Overridable default applies to all nodes in the network. The Route Automatically check box is either overridable or not depending on how the default is set for the node you are logged into through CTC. To ensure correct behavior after setting the default, propagate the chosen default setting to all nodes through which users might log into the network to perform provisioning. For more information on NE defaults and their provisioning consult the user documentation.

TL1

Related Documentation

Release-Specific Documents

- *Release Notes for the Cisco ONS 15310-CL, Release 7.0*
- *Release Notes for the Cisco ONS 15310-MA, Release 7.2*

- *Release Notes for the Cisco ONS 15454 SDH, Release 7.2*
- *Release Notes for the Cisco ONS 15327, Release 7.2*
- *Release Notes for the Cisco ONS 15600, Release 7.2*
- *Release Notes for the Cisco ONS 15454, Release 7.2*

Platform-Specific Documents

- *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*
Provides installation, turn up, test, and maintenance procedures
- *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*
Provides technical reference information for SONET/SDH cards, nodes, and networks
- *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide*
Provides a list of SONET alarms and troubleshooting procedures, general troubleshooting information, and hardware replacement procedures
- *Cisco ONS SONET TL1 Command Guide*
Provides a comprehensive list of TL1 commands

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. 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. (1005R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2006 Cisco Systems, Inc. All rights reserved.