



# Release Notes for *Cisco ONS 15310-CL* *Release 7.23*

---



## 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-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 7.23, visit the following URL:

[http://www.cisco.com/en/US/products/hw/optical/ps2006/prod\\_release\\_notes\\_list.html](http://www.cisco.com/en/US/products/hw/optical/ps2006/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://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs>

## Contents

- [Changes to the Release Notes, page 2](#)
- [Caveats, page 2](#)
- [Resolved Caveats for Release 7.2, page 5](#)
- [New Features and Functionality, page 7](#)
- [Related Documentation, page 8](#)



---

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

© 2007 Cisco Systems, Inc. All rights reserved.

[Obtaining Documentation and Submitting a Service Request, page 9](#)

## 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 7.23.

No changes have been added to the release notes for Release 7.23.

## 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.

---

### CSCse36337

When a Server Trail is created on a 1+1 Protection Group, the Node's database gets deleted, and the Node goes for continuous reboot. No workaround available. This issue will be resolved in Release 7.22, 8.0.

### CSCse89357

CTC Network view shows up without any Nodes. The initialization of the network view sometimes would get interrupted with exceptions. Workaround is to relaunch CTC. This issue will be resolved in a future release.

CTC Network view shows up without any Nodes. The initialization of the network view sometimes would get interrupted with exceptions. Workaround is to relaunch CTC. This issue will be resolved in a future release.

## CSCse96077

On an IO port with this issue false TCAs that indicate line or traffic problems are raised every 15 min after the 15 min pm report. There are no alarms with the associated ports. Traffic is not affected. In Release 7.2, during a very short period when the defect is present (less than 1 sec), false TCAs might be raised. This can be reproduced by either removing or then reinserting the card, or by a small burst of defects.

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:

- 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.
- 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 circuit path on the card or any port on the card or the card itself is in a protection group. Note that the protection switch itself might cause a defect burst, which might introduce false TCAs. Before resetting the card, check if any circuit, port, or card is in a protection group. If there is path protection, BLSR, 1+1 or 1:1/1:N protection on the card, lock the protection using a switch command (for example, LOCKOUT/LOCKON) available to users before you reset the card ensuring that no protection switch occurs during soft reset, and that traffic will not be affected. For a card with no protection type, simply soft reset the card and traffic will not be affected.

This issue will be resolved in a future release.

## 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.

## **CSCsh38022**

When IPPM is enabled on a STS circuit, and errors injected, IPPM values do not increment. on CTC. Use TL1 to check the IPPM Values. This will be resolved in a future release.

## **Alarms**

### **CSCse85355,CSCsd52665,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.

## **Common Control Cards**

### **CSCsb62127**

A DCC Link discovered by CTC, can show incorrect bandwidth. When a DCC tunnel is created using two different OC cards, like OC12 and OC48 at its ends, CTC Network view shows incorrect bandwidth. Such a provisioning is a provisioning mistake. No workaround available. This issue will be resolved in a future release.

## CSCsh41379

Create a STS1 circuit on a 310CL node from a DS1 port to anyother port/card. Enable IPPM. try the command "RTRV-STS1::<src>:<ctag>:1;" T11 would return an error message saying STS not provisioned. Simiar is the case with the RTRV-PM-STS1 command. This indicates that we are unable to retrieve STS1 connections provisioned on the DS1 port of 310CI-CTX card. And also unable to retrieve performance monitoring counts for the cross-connects. However the Performance Monitors can be seen through CTC. This is expected to be resolved in a future release.

## 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.

---

## SNMP

### CSCsh46329

On 310CL, create a circuit on DS3, dsx3ValidIntervals is expected to increment by 1 every 15 minutes, but when you check this in simpleTester MIB browser the counter isn't incrementing. Workaround is to check this in CTC. This issue will be fixed in a future release.

## Resolved Caveats for Release 7.2

The following items are resolved in Release 7.2.

## Maintenance and Administration

### CSCsg52340

Automatic Routing of circuits using CTC 7.2 or higher, on nodes older than 7.2 is not possible. A new NE Default introduced in 7.2, causes this problem. Workaround is to toggle the `CIRCUITS_AUTO_ROUTE_DEFAULT_OVERRIDABLE` NE Default. This issue is resolved in Release 7.22, 8.0.

### CSCse92125

Attempt to log-in using CTC. CTC login fails. Workaround is to ensure that the PC is not running a Turkish locale. This issue is fixed in Release 8.0.

### CSCse99104

CTC can incur either repeated failures when you attempt to log in to an NE, and/or a very long time to discover all ENes behind a GNE (could be over 30 minutes on a medium sized network). This issue affects all ONS 15xxx releases from R4.1 to 7.2. This condition is more likely to happen on Windows XP after an upgrade to Service Pack 2, and when the network is made of a medium to large number of GNEs/ENes with SOCKS enabled. This condition can also happen in the case of networks with poor connectivity between CTC and the GNEs.

The solution involves an enhancement to the SOCKS discovery protocol by introducing the concept of designated SOCKS servers. A designated SOCKS server is a NE that runs SOCKS, is LAN connected and has been explicitly marked as a potential SOCKS server by the user. CTC allows the user to enter an unlimited number of designated SOCKS servers. When designated SOCKS servers are defined, the automatic SOCKS server discovery protocol is disabled, resulting in substantial performance improvement during CTC login and ENE discovery.

### CSCse53017

Circuit creation when attempted on ML cards between a 7.2 NE and an older NE, the wizard would die. The source should be on 7.2 NE and destination on the older NE. Workaround is to interchange the source and destination. This issue is resolved in Release 7.22, 8.0.

### CSCse53017

Circuit creation when attempted on ML cards between a 7.2 NE and an older NE, the wizard would die. The source should be on 7.2 NE and destination on the older NE. Workaround is to interchange the source and destination. This issue is resolved in Release 7.22, and 8.0.

### CSCsj04557

Users can now control the local/global domain flag through CTC preference. Previously, the user controlled the local/global flag setting from the login node Network Element (NE) default (`CTC.network.LocalDomainCreationAndViewing`). Any flag changes would be applied immediately in the CTC session.

To change the flag in Release 7.23, from Node view or Network view, open the “Edit” menu and select “Preferences.” In the Preferences dialog, click the checkbox labeled “Domain Settings.” You must restart CTC after changing the flag.

## Common Control Cards

### CSCse01108

When the NE time is changed from CTC (or TL1), the pm bins of the interfaces (OCn/Ds1 on ctx-cl and OCn on 310-MA), which are on the active tcc, does n't get marked as partial. No workaround available. This issue is resolved in Release 7.22 and 8.0.

### CSCse98996

The issue can be reproduced as follow:

- 
- Step 1** On the node Infy12 went to Network view, Edit--->Preferences---->Checked Display events with Node Time Zone
  - Step 2** Changed the time to 11-Mar-2007 01:59:00 PST and let it pass the 02:00:00 am.
  - Step 3** CTC Node view-->Provisioning-->General Tab correctly showed the changed time as 03:00:00 PDT.
  - Step 4** Generated a LOS on a OC3 card. CTC Alarm pane showed the new PDT time.
  - Step 5** Retrieved audit trail. Audit trail showed the correct PDT time.

## 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.

## CTC Cache Installer

The purpose of this cache installer is to allow installing/reinstalling/upgrading CTC core jars into the user's CTC jar cache. The executable: SetupCtc-MMmm00.exe - a self-extracting .zip file - is for this purpose (where MM is the major release and mm is the minor release). To use it, the user runs the SetupCtc .exe. This produces a directory that consists of the CTC core jars and LDCACHE.exe. The user can then, from that installed directory, 'double-click' on LDCACHE.exe to get the CTC core run-time jars copied into the CTC jar cache. LDCACHE.exe can be run at a later time as well to recopy the CTC core jars into the user's CTC jar cache.

# 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 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: [www.cisco.com/go/trademarks](http://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. (1110R)

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.