



# Release Notes for Cisco ONS 15310-CL Release 6.2.2

---



## 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 6.0 of the *Cisco ONS 15310-CL Procedure Guide*, *Cisco ONS 15310-CL Reference Guide*, *Cisco ONS SONET TL1 Command Guide*, and *Cisco ONS 15310-CL Troubleshooting Guide*. For the most current version of the Release Notes for Cisco ONS 15310-CL Release 6.2.2, visit the following URL:

[http://www.cisco.com/en/US/products/hw/optical/ps2001/prod\\_release\\_notes\\_list.html](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](http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl)

## Contents

[Changes to the Release Notes, page 3](#)

[Caveats, page 3](#)

[Resolved Caveats for Release 6.2.2, page 4](#)

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

[Related Documentation, page 6](#)

[Obtaining Documentation, page 6](#)



---

### Corporate Headquarters:

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

Copyright © 2007 Cisco Systems, Inc. All rights reserved.

[Documentation Feedback, page 7](#)

[Cisco Product Security Overview, page 7](#)

[Obtaining Technical Assistance, page 8](#)

[Obtaining Additional Publications and Information, page 10](#)

# Changes to the Release Notes

This section documents supplemental changes that have been added to the *Release Notes for Cisco ONS 15310-CL Release 6.2.2* since the production of the Cisco ONS 15310-CL System Software CD for Release 6.2.2.

No changes have been added to the release notes for Release 6.2.2.

## Caveats

Review the notes listed below before deploying the ONS 15310-CL. Caveats with DDTS tracking numbers are known system limitations that are scheduled to be addressed in a subsequent release. Caveats without DDTS 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.

---

### 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.

## Data I/O Cards

### CSCsb40206

In Asymmetric configuration, with autonegotiation enabled and flow control selected, an ML-series card might fail to synchronize with, or to recognize the asymmetric flow control. This issue is under investigation.

## Path Protection Functionality

### CSCee53579

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

## Bridge and Roll

### CSCei37364

When a rollTo leg is not receiving a good signal, and because of this the rollPending alarm is not cleared, there is no alarm indicating the reason that the RollPending alarm fails to clear. This issue is resolved in Release 7.0.

## 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 6.2.2

The following items are resolved in Release 6.2.x.

## Maintenance and Administration

### CSCsd67191

Rarely, in a large network with many host routes the Proxy ARP server might run out of ring buffer storage, resulting in a subsequent failure of the driver to receive new packets. This can lead to DCC failure and loss of all connections. This issue is resolved in Releases 6.2 and 8.

### CSCeg81602

A 100 second outage on DS1 traffic that is physically looped back, and in IS-AINS state, can occur during a span switch. With a loopback on the DS1 traffic a span switch will induce errors that raise a signal degrade (SD) on the DS1. The system then injects AIS due to the SD to keep from transitioning to IS from IS-AINS. To prevent this issue avoid using a physical loopback. This issue is resolved Release 6.0.

## Data I/O Cards

### CSCeh26707

Loss of Ethernet signal on one of the front ports takes longer than expected to be propagated to the remote port. Link integrity operates slower than expected for Ethernet failures (though it works as expected for SONET failures). To see this, any condition that causes an Ethernet loss of signal (removal of a front port Ethernet cable, for example) will invoke the Ethernet integrity function. This issue is resolved in Release 6.0.

### CSCeh28342

On ML-series in the ONS 15310-CL, when policing is enabled, the configured policed rate is not forwarded. This can occur when policing at a rate lower than 1 Mbps. The workaround is to set the policed rate higher than 1 Mbps, or to raise the configured policed rate until the desired rate is forwarded. This issue is resolved in Release 6.0.

## Path Protection Functionality

### CSCec15064

A path protected /SNCP circuit with a defect signal present (for example, AIS-P or AIS-V) on the protect path will produce RDI-P or RDI-V upstream of the detection point, but these signals will not be detected or indicated. This issue is resolved in Release 6.0.

## TL1 Functionality

### CSCsb69386

If a TL1 tunnel is open on an ONS 153xx NE, sometimes when the NE reboots the nodes behind the tunnel will become permanently grayed out. This issue can occur when the tunnel far end is either rebooting or is already servicing other TL1 tunnels with several NEs behind the tunnel. To work around this issue, restart CTC at a later time, when the far end NE has less active TL1 tunnels. This issue is resolved in Release 6.2.

## New Features and Functionality

This section highlights new features and functionality for Release 6.2.x. For complete documentation of each of the features of the ONS 15310-CL, consult the user documentation.

There are no new features for Release 6.2.x.

# Related Documentation

## Release-Specific Documents

- *Release Notes for the Cisco ONS 15310-CL, Release 6.2*
- *Release Notes for the Cisco ONS 15454 SDH, Release 6.2.2*
- *Release Notes for the Cisco ONS 15327, Release 6.2.2*
- *Release Notes for the Cisco ONS 15600, Release 6.2.2*
- *Release Notes for the Cisco ONS 15454, Release 6.2.2*
- *Upgrading Cisco ONS 15310-CL to Release 6.2*

## Platform-Specific Documents

- *Cisco ONS 15310-CL Procedure Guide*  
Provides installation, turn up, test, and maintenance procedures
- *Cisco ONS 15310-CL Reference Manual*  
Provides technical reference information for SONET/SDH cards, nodes, and networks
- *Cisco ONS 15310-CL 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

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

## Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

## Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

Cisco Marketplace:

<http://www.cisco.com/go/marketplace/>

## Ordering Documentation

You can find instructions for ordering documentation at this URL:

[http://www.cisco.com/univercd/cc/td/doc/es\\_inpk/pdi.htm](http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm)

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:  
<http://www.cisco.com/en/US/partner/ordering/>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

## Documentation Feedback

You can send comments about technical documentation to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems  
Attn: Customer Document Ordering  
170 West Tasman Drive  
San Jose, CA 95134-9883

We appreciate your comments.

## Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.

- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

[http://www.cisco.com/en/US/products/products\\_psirt\\_rss\\_feed.html](http://www.cisco.com/en/US/products/products_psirt_rss_feed.html)

## Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—[security-alert@cisco.com](mailto:security-alert@cisco.com)
- Nonemergencies—[psirt@cisco.com](mailto:psirt@cisco.com)



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

<http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on>

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

## Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

## Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>



#### Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

## Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

## Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

**Severity 1 (S1)**—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

**Severity 2 (S2)**—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

**Severity 3 (S3)**—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

## Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

<http://www.cisco.com/ipj>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>

---

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

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0711R)

Copyright © 2007, Cisco Systems, Inc.  
All rights reserved.