



# Release Notes for Cisco ONS 15310-MA Release 7.2

---

## February 2007

Release notes address closed (maintenance) issues, caveats, and new features for the Cisco ONS 15310-MA. 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 Manual*, and the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide*, and Release 7.2 of the *Cisco ONS SONET TL1 Command Guide*. For the most current version of the Release Notes for Cisco ONS 15310-MA Release 7.2, 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 2](#)

[Caveats, page 2](#)

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

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

[Related Documentation, page 8](#)

[Obtaining Documentation and Submitting a Service Request, page 8](#)



---

**Corporate Headquarters:**

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

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

## Changes to the Release Notes

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

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

## Changes to New Features and Functionality

The following new feature's summary has been revised to better explain secure mode locking behavior:

[IP Addressing with Secure Mode Enabled, page 5](#)

## Changes to Caveats

The following caveat has been added.

[CSCse85355](#)

[CSCsd52665](#)

[CSCsd56328](#)

## Caveats

Review the notes listed below before deploying the ONS 15310-MA. 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.

## CSCsd84638

Sometimes IP connectivity to an ONS 15310-MA is lost and pinging the node fails. Also, as a result, CTC fails to come up. This can occur if both the Ethernet port on the CTXMA card and the Ethernet port on the backplane are accidentally connected to the same network, resulting in loops in the switching network. In normal operation the backport should be used to connect to the network and the frontport should only be used for onsite maintenance. If this issue occurs detach the Ethernet cables from both the frontport and the backport and connect via the backport (or frontport) only, rather than via both at the same time. This issue will not be resolved.

## CSCsc56694

IPPM enabled by CTC for an OCn trunk card is disabled automatically after two hours. This issue will be resolved in Release 8.0.

## 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.

## Common Control Cards

### CSCsc52028

The CTX 2500 card does not accept more than 52 ENE sessions. Figuring 16 ENE sessions per GNE session, the expected ENE logins for 7 GNE sessions is 112, whereas the CTX 2500 accepts only 52. 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-MA, consult the user documentation.

## New Software Features

The following sections describe new software features for Release 7.2.

### IP Addressing with Secure Mode Enabled

This section addresses Release 7.2 secure mode. It also describes how this mode's locked or unlocked options operate in various scenarios with R7.2, or R7.2 in combination with R7.0.

#### Secure Mode

In Release 7.2, you can separate LAN interface access from backplane Ethernet port access by use of the secure mode. Additionally, you can lock this mode so that a node's configuration cannot be altered.

The CTX2500 card defaults to nonsecure, unlocked mode. (Your network's defaults may differ; refer to the NE Defaults documentation to confirm them.) In nonsecure mode, the LAN and backplane Ethernet ports share a single MAC address and IP address. The CTX2500 card allows you to place a node in secure mode to prevent a LAN port user from accessing the network through the backplane port. Secure mode can also be locked, which prevents the mode from being altered.

#### Dual IP Addresses

Changing an ONS 15310-MA node from nonsecure mode to secure mode allows you to provision two Ethernet addresses for the node and causes the active CTX2500 to assign the ports different MAC addresses. In secure mode, one IP address is provisioned for the ONS 15310-MA backplane Ethernet port and the other is provisioned for the CTX2500 LAN port. Both addresses reside on different subnets and packets are not exchanged between these two ports. The dual addresses provide an additional layer of separation between the LAN access port and the ONS 15310-MA network. If secure mode is enabled, the IP addresses provisioned for both ports must follow general IP addressing guidelines and must reside on different subnets from each other and the default router IP address.

In secure mode, the LAN port IP address becomes a private address while the backplane port connects the node to an Operations Support System (OSS) through a central office or private enterprise network. A superuser can configure the node to hide or reveal the backplane's Ethernet IP address in CTC, the routing table, or autonomous message reports.

#### Secure Mode Locking

A superuser can convert a secure node from unlocked to locked mode. Doing so permanently changes the chassis hardware. The procedure for placing a node in secure mode or secure locked mode is similar to the process for an ONS 15454 node. Refer to the "Manage the Node" chapter in the *Cisco ONS 15454 Procedure Guide* for instructions.

When a node is secure and locked, its configuration, Ethernet port status, its secure mode, and the locked status cannot be changed by any network user— including a superuser. To have a secure node's lock removed, contact Cisco Technical Support to arrange a Return Material Authorization (RMA) for the chassis and the CTX2500 card(s). Refer to the Obtaining Technical Assistance section of the *Cisco ONS 15310- CL and ONS 15310-MA Procedure Guide* as needed.

When a node is secure and locked, its configuration, Ethernet port status, its secure mode, and the locked status cannot be changed by any network user— including a superuser. To have a secure node's lock removed, contact Cisco Technical Support to arrange a Return Material Authorization (RMA) for the chassis and the CTX2500 card(s). Refer to the Obtaining Technical Assistance section of the *Cisco ONS 15310- CL and ONS 15310-MA Procedure Guide* as needed.

**Note**

If a CTX2500 card or chassis needs to be unlocked, the locked cards and chassis need to be unlocked together by Cisco Technical Support. RMA the cards and chassis together.

**Mixed Release Shelf Scenarios**

When an active CTX2500 card is converted to locked mode, the standby CTX2500 card and chassis are also changed. The components retain their locked status even if separated.

**Caution**

Enabling secure mode on a CTX2500 card causes it to reboot.

**Note**

A chassis can only be locked by using Release 7.2 software on the active CTX2500 controller card.

**Note**

Software Release 7.0 does not support secure mode locking. This software's behavior in a R7.2 node depends upon where it is used.

Following are some example scenarios using locked or unlocked Release 7.2 and Release 7.0 components:

- If you insert two unlocked R 7.2 CTX2500 cards into a locked chassis, the chassis hardware lock prevails and converts the cards to locked.
- If you remove both CTX2500 cards from a locked chassis and insert both cards into an unlocked R7.2 chassis, the lock follows the active controller card and converts the unlocked chassis to locked.
- If you remove a locked standby CTX2500 from a shelf and insert it as active in an unlocked R7.2 chassis, the locks follows the active controller card and converts the chassis and standby card to locked.
- If you insert a locked CTX2500 as standby into an R7.2 chassis with an unlocked active CTX2500, the active card overwrites the standby card's lock. The chassis remains unlocked.
- If you insert an R7.0 CTX2500 as standby card in a locked chassis (with an active R7.2 card), the active card updates the standby card software version to R7.2. After R7.2 is fully loaded on the standby card, the chassis activates the standby's lock status.

## Node Role Flexibility

In nonsecure mode, a node can be a GNE or ENE. Placing the node into secure mode automatically turns on SOCKS proxy and defaults the node to GNE status. However, the node can be changed back to an ENE. In nonsecure mode, an ENE's SOCKS proxy can be disabled—effectively isolating the node beyond the LAN firewall—but it cannot be disabled in secure mode. To change a node's GNE or ENE status and disable the SOCKS proxy, refer to the “Turn Up a Node” chapter in the *Cisco ONS 15310-CL and ONS 15310-MA Procedure Guide*.



### Note

If the LAN and backplane access ports are disabled in an ENE and the node is isolated from DCC communication (due to user provisioning or network faults), the LAN and backplane ports are automatically reenabled.

## 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.

# Related Documentation

## Release-Specific Documents

- *Release Notes for the Cisco ONS 15310-MA Release 7.0*
- *Release Notes for the Cisco ONS 15310-CL 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 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, transient conditions, and error messages
- *Cisco ONS SONET TLI Command Guide*  
Provides a comprehensive list of TLI commands
- *Cisco ONS SONET TLI Reference Guide*  
Provides general information, procedures, and errors for TLI
- *Cisco ONS 15310-CL and Cisco ONS 15310-MA Ethernet Card Software Feature and Configuration Guide*  
Provides software feature and operation information for Ethernet cards

# 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](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. (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.