



Release Notes for Cisco ONS 15327 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 15327 SONET. For detailed information regarding features, capabilities, hardware, and software introduced with this release, refer to Release 7.2 of the *Cisco ONS 15327 Procedure Guide*, *Cisco ONS 15327 Reference Manual*, and *Cisco ONS 15327 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 15327 Release 7.23, visit the following URL:

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.x, page 7](#)

[New Features and Functionality, page 9](#)

[Related Documentation, page 10](#)

[Obtaining Documentation and Submitting a Service Request, page 10](#)



Americas Headquarters:

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

© 2007 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 15327 Release 7.2* since the production of the Cisco ONS 15327 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 15327. 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.



Note

In releases prior to 4.6 you could independently set proxy server gateway settings; however, with Release 4.6.x and forward, this is no longer the case. To retain the integrity of existing network configurations, settings made in a pre-4.6 release are not changed on an upgrade to Release 7.0.x. Current settings are displayed in CTC (whether they were inherited from an upgrade, or they were set using the current GUI).

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.

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.

CSCed24448

After a static route is provisioned to 0.0.0.0 and then deleted, the default route disappears. If this occurs, reprovision the default gateway. This issue will not be resolved.

CSCee65731

An ONS 15327 that does not have an SNTP server reference resets the time to Jan. 1, 1970 during a software activation. A routine common control switchover does not cause the node to lose the time setting. To avoid this issue provision a SNTP server reference. This issue cannot be resolved.

CSCdy10030

CVs are not positively adjusted after exiting a UAS state. When a transition has been made from counting UAS, at least 10 seconds of non-SES must be counted to exit UAS. When this event occurs, Telcordia GR-253 specifies that CVs that occurred during this time be counted, but they are not. There are no plans to resolve this issue at this time.

CSCdy49608

A node connection might fail during bulk circuit creation, causing the circuit creation to also fail. For example, this has been seen while creating 224 VT 1.5 protected circuits, on a path protection consisting of eight ONS 15327 nodes. If you experience a bulk circuit creation failure of this type, cancel the circuit creation batch, then delete any incomplete circuits. Restart the batch from the last successful circuit. This issue will not be resolved.

CSCdx35561

CTC is unable to communicate with an ONS 15327 that is connected via an Ethernet craft port. CTC does, however, communicate over an SDCC link with an ONS 15327 that is Ethernet connected, yielding a slow connection. This situation occurs when multiple ONS 15327s are on a single Ethernet segment and the nodes have different values for any of the following features:

- Enable OSPF on the LAN
- Enable Firewall
- Craft Access Only

When any of these features are enabled, the proxy ARP service on the node is also disabled. The ONS 15327 proxy ARP service assumes that all nodes are participating in the service.

This situation can also occur immediately after the aforementioned features are enabled. Other hosts on the Ethernet segment (for example, the subnet router) may retain incorrect ARP settings for the ONS 15327s.

To avoid this issue, all nodes on the same Ethernet segment must have the same values for Enable OSPF on the LAN, Enable Firewall, and Craft Access Only. If any of these values have changed recently, it may be necessary to allow connected hosts (such as the subnet router) to expire their ARP entries.

You can avoid waiting for the ARP entries to expire on their own by removing the SDCC links from the affected ONS 15327 nodes. This will disconnect them for the purposes of the proxy ARP service and the nodes should become directly accessible over the Ethernet. Network settings on the nodes can then be provisioned as desired, after which the SDCC can be restored.

This issue will not be resolved.

CSCdy11012

When the topology host is connected to multiple OSPF areas, but CTC is launched on a node that is connected to fewer areas, the topology host appears in CTC, and all nodes appear in the network view, but some nodes remain disconnected. This can occur when the CTC host does not have routing information to connect to the disconnected nodes. (This can happen, for example, if automatic host detection was used to connect the CTC workstation to the initial node.)

CTC will be able to contact the topology host to learn about all the nodes in all the OSPF areas, but will be unable to contact any nodes that are not in the OSPF areas used by the launch node. Therefore, some nodes will remain disconnected in the CTC network view.

To work around this issue, if no firewall enabled, then the network configuration of the CTC host can be changed to allow CTC to see all nodes in the network. The launch node must be on its own subnet to prevent network partitioning, and craft access must not be enabled. The CTC host must be provisioned with an address on the same subnet as the initial node (but this address must not conflict with any other node in the network), and with the default gateway of the initial node. CTC will now be able to contact all nodes in the network.

If a firewall is enabled on any node in the network, then CTC will be unable to contact nodes outside of the initial OSPF areas. This issue will not be resolved.

CSCdy37198

On Cisco ONS 15327 platforms equipped with XTC cross-connect cards, Ethernet traffic may be lost during a BLSR protection switch, with no accompanying alarm or condition raised. Possible affected circuits will be between Ethernet cards (E100T-4) built over Protection Channel Access (PCA) bandwidth on BLSR spans. When BLSR issues the switch, the PCA bandwidth is preempted. Since there is no longer a connection between the ends of the Ethernet circuit, traffic is lost. Further, in nodes equipped with XTC cards, the E100T-4 cards do not raise an alarm or condition in CTC. This issue will not be resolved.

CSCds23552

You cannot delete the standby XTC once it is removed. If you have two XTC cards and then decide to operate with only one, you will get a standing minor alarm. The alarm cannot be removed by CTC. The XTC is a combo card, combining the functionality of the ONS 15454 TCC2, cross connect, DS1 and DS3 cards, with a protection group automatically provisioned. On the ONS 15454, similar behavior occurs for the TCC2 card. The cross connect card for the ONS 15454 can only be deleted if there are no circuits provisioned. DS1 and DS3 cards can only be deleted if they are not in a protection group. User-defined alarm profiles from Release 5.0.x allow you to mask the improper removal alarm from the standby XTC slot without masking any other items if desired, thus avoiding this issue. This issue will not be resolved.

Data IO Cards

CSCdy41135

When using a G1000-2 card, TIM-P can be mistakenly raised on a PCA circuit after a protection switch. This occurs when path trace is enabled on a PCA circuit that is no longer in use after a protection switch. To work around this issue, either disable path trace or use alarm profiling to filter out the unwanted alarm. This issue will not be resolved.

CSCdy13035

Excessive Ethernet traffic loss (greater than 60 ms) might occur when the active XTC is removed from the chassis while using the G1000-2 card. On rare occasions, permanent loss of traffic can occur. Do not remove the active XTC from the chassis to force a protection switch. Instead, perform a soft reset of the active XTC through the network management interface. Once the XTC is in standby mode, it can be removed from the chassis without inducing excessive traffic loss.

This issue impacts only cards with Version number 800-18490-01 and is resolved by a newer version of the G1000-2 cards. Cards with Version number 800-18490-02, rev A0 or later incorporate improved hardware PLL circuitry on the G1000-2 line card to allow an active XTC removal without causing excessive traffic loss. The caveat herein is for the previous hardware version.

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.

CSCsh17401

15327-XTC-28-3 card will not boot when installed in standby slot of existing node. Software load on standby XTC-28-3 card is several versions older than version on active XTC-28-3. Problem has been observed on RMA'd cards delivered with 3.3 or 3.4 software being installed in standby slots on nodes running 4.1.x or higher software.

Workaround: Install problem card in stand alone or lab node and manually download software to the card and activate. Then install card into production node.

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.

CSCeb37707

With a VT Path Protection circuit, if you inject signals with a thru-mode test set into one path of the circuit in a particular order, you may not see the appropriate alarms. This can occur when you first inject LOP-P, then clear, then inject LOP-V. This issue will not be resolved.

BLSR Functionality

CSCsc14824

A low memory alarm might be raised when interconnecting two BLSRs on a single ONS 15327 node. When interconnecting one BLSR or using Path Protection, 1:1, or 1:0 protection the low memory alarm will not be seen. To clear a low memory alarm perform an XTC side switch.

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.x

The following items are resolved in Release 7.2.x

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 CIRCUIITS_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.

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

CSCsg20452

15327 DCC failure Adjacent nodes see SDCC/LDCC Termination failures. These failures cause loss of visibility of the 15327 on CTC. The Multi-Channel communication controller(MCC) which is used for DCC Communication sees an interrupt called GUN(Global Under Run). When this happens DCC Communication to the node is completely broken. Workaround is to reset the XTC card, to resume DCC communication and restore visibility. This issue is resolved in 7.22

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.
-

The problem is not observed on this load.

Path Protection

CSCsh77496

If Path Protection/SNCP circuits are created while path defects are present on Path Protection/SNCP trunks, then sometimes Path Protection/SNCP circuits may not switch and traffic outage is observed.

Workaround: Avoid creating Path Protection circuits when faults are present on either of the Path Protection trunks ports. This issue is resolved in 6.03, 7.05 and 7.2.3.

New Features and Functionality

This section highlights new features and functionality for Release 7.2. For detailed documentation of each of these features, consult the user documentation.

New Software Features

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 15327, Release 7.0
- Release Notes for the Cisco ONS 15454 SDH, Release 7.2
- Release Notes for the Cisco ONS 15454, Release 7.2
- Release Notes for the Cisco ONS 15600, Release 7.2
- Release Notes for the Cisco ONS 15310-CL, Release 7.2
- Cisco ONS 15327 Software Upgrade Guide, Release 7.2

Platform-Specific Documents

- *Cisco ONS 15327 Procedure Guide*
Provides installation, turn up, test, and maintenance procedures
- *Cisco ONS 15327 Reference Manual*
Provides technical reference information for SONET/SDH cards, nodes, and networks
- *Cisco ONS 15327 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. 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.

© 2007 Cisco Systems, Inc. All rights reserved.