



# Release Notes for *Cisco ONS 15327* *Release 7.0.7*

---

**OL-15530-01**  
**June 27, 2008**



**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.

---

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 7.0 of the *Cisco ONS 15327 Procedure Guide*, *Cisco ONS 15327 Reference Manual*, *Cisco ONS SONET TLI Command Guide*, and *Cisco ONS 15327 Troubleshooting Guide*. For the most current version of the Release Notes for Cisco ONS 15327 Release 7.07, 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://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 7.0.x, page 6](#)
- [New Features and Functionality, page 9](#)
- [Related Documentation, page 15](#)



---

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

© 2007 Cisco Systems, Inc. All rights reserved.

- [Obtaining Documentation, page 16](#)
- [Documentation Feedback, page 17](#)
- [Cisco Product Security Overview, page 17](#)
- [Obtaining Technical Assistance, page 18](#)
- [Obtaining Additional Publications and Information, page 19](#)

## Changes to the Release Notes

This section documents supplemental changes that have been added to the *Release Notes for Cisco ONS 15327 Release 7.07* since the production of the Cisco ONS 15327 System Software CD for Release 7.07.

Date	Notes
02/26/2008	Added CSCsm27602 under the Data IO Cards subsection in the Caveats section.

## 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).

### 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.

## Common Control Cards

### CSCsh17401

15327-XTC-28-3 card does 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 is to install problem card in stand alone or lab node and manually download software to the card and activate. Then install card into production node. This issue will be resolved in a future release.

## 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.

### CSCsm27602

On the G1000/G1K port the transition from IS state to OSS-DSBLD state and back to IS state may cause a loss of traffic.

This issue occurs when G1000/G1K port has auto-negotiation disabled and is over-subscribed (that is, the port is receiving ethernet traffic at a rate more than the SONET circuit capacity).

The work around to solve this issue is to change the port to OSS-MT state and apply a facility loopback. This enables the traffic to recover. Then change the port back to IS state. This enables the traffic to come up.

This issue is to be resolved in release 8.5.1.

## 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.

## Performance Monitoring

### CSCdt10886

The far-end STS PM counts do not accumulate on an OC-48 linear 1+1 circuit even though the near-end STS PM counts on the other end are increasing. To see this issue, connect two nodes with an OC-12 or OC-48 linear 1+1 protected span. Place a piece of test equipment in the middle of the span and inject B3 errors. The near-end STS PM counts accumulate, but the far-end STS PM counts do not accumulate. To work around this issue, Use the near-end STS PM count from the adjacent node to see the far-end STS PM count for the current node. This issue will be resolved in a future release.

## 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 7.0.x

The following items are resolved in Release 7.0.x.

## Maintenance & Administration

### CSCsl04416

When a node is upgraded from 4.14 release to 7.05 release, the Back Plane (BP) LAN connection goes to down state. If slot 7 has the active TCC on the 4.14 release and we try to activate to 7.05 release, there is a high probability that the BP LAN stays in down state.

The workaround is to make TCC in slot 11 active, before the activation to 7.05 release.

The problem is solved by protecting the critical area of the LAN port during the activation process. This issue is resolved in release 7.0.7.



**Note** If the upgrade from release 4.14 to 7.05 causes the Back Plane LAN to go down, the only way to bring it back up is to:

1. Reset the active TCC
2. Issue the vxWork command to re-enable the BP LAN

### CSCsg22891

This allows you to change AISVONAI and AISONLOF flag through CTC and TL1 for DS1, DS1N and XTC cards. 1) In the XTC-28 card view, Provisioning->DS1->Line pane. 2) Tried enabling "Send AIS-V on Defects" checkbox. The checkbox is editable from the CTC. 3) Tried to uncheck "send AIS-V on defects" checkbox from CTC. Unchecking of this checkbox is allowed. 4) Tried to enable "Send AIS-V on Defects" from TL1 using ED-T1. From TL1, enabling of "Send AIS-V on Defects" checkbox is allowed. 5) Tried to check the "Send AIS-V on Defects" checkbox from TL1, unchecking of "Send AIS-V on Defects" checkbox is allowed. With reference to CSCsf99327, the defaults values for AISVONAI and AISONLOF should be editable from both CTC and TL1.

## Common Control Cards

### CSCsi97098

Standby TCC resets after connecting to the database through FTP. Standby TCC resets and sometimes a DBOSYNC alarm is raised for 30 seconds after it comes up.

This condition happens when the FTP connection between the active and standby TCC faces an interruption and the standby TCC decides to reset itself.

This issue is resolved by allowing the standby TCC to reinitialize its FTP connection to the active TCC before rebooting. This issue is resolved in release 7.0.7.

## Data IO Cards

### CSCsI53199

For any SONET/SDH defect the G1K-4 card soaks the defect for a fixed duration of time (200 ms). The G1K-4 card initiates link integrity after this duration and brings down the front port. The end devices re-converge after the link comes up.

Certain network configurations results in SONET/SDH disruptions of durations more than 200 ms. Such disruptions necessitates that the link integrity be initiated at an interval greater than 200 ms.

This issue is resolved in release 7.0.7 by allowing the timer duration to be configured with the following settings:

- 200 ms
- 1000 ms
- 5000 ms
- Disable Link Integrity

The user can select an option from the CTC on a per port basis.

## Electrical IO Cards

### CSCsd59042

When upgrading the software from Release 6.x.x to Release 7.x.x, the DS3 and EC1-12 cards fail to load if the node name begins with the letters FL. Changing the node name resolves this issue.

## Alarms

### CSCsi23824

The Signal Fail-Path (SF-P) and Signal Degrade-Path (SD) alarms are not reported on the following cards.

- OC192XFP: 15454-10G-RX, 15454E-10G-RX, 15454-10G-S1, 15454E-10G-I1
- MRC-12: 15454-MRC-I-12, 15454E-MRC-I-12
- MRC25G-12: 15454E-MRC-2.5G12
- MRC25G-4: 15454-MRC-2.5G4
- ADM-10G: 15454-ADM-10G
- RAN-SVC - 15454-RAN-SVC, 15454E-RAN-SVC

In case Path Protection circuits are created on the affected cards, these circuits may not switch if the SF-P and SD-P conditions exist on the path.

This issue is resolved in release 7.0.7.

## 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.

## 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 while 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 7.0.x. For detailed documentation of each of these features, consult the user documentation.

## New Software Features

The following feature has been added for Release 7.0.2.

### Daylight Savings Time Support

With Release 7.0.2 CTC and TL1 display daylight savings time (DST) in keeping with the new DST rules applicable from 2007 forward. As described in the change in energy policy for the United States of America (USA), the DST start date will be the 2nd Sunday of March and the DST end date will be 1st Sunday of November.

The following features were added for Release 7.0.

### BLSR STS and VT Squelching

Release 7.0.x supports BLSR STS squelching for the ONS 15454, ONS 15327, and ONS 15600, and VT squelching for the ONS 15454, and ONS 15327, with limited VT squelching support (see below) provided by the ONS 15600.

Release 7.0.x nodes display STS and VT squelch tables depending on the type of circuits created. For example, if a fiber cut occurs, the BLSR squelch tables show STSs or VTs that will be squelched for every isolated node. Squelching replaces traffic by inserting the appropriate alarm indication signal path (AIS-P) and prevents traffic misconnections. For an STS with a VT-access check mark, the AIS-P will be removed after 100 ms.

## BLSR STS Squelch Tables in CTC

BLSR STS squelch tables show STSs that will be squelched for every isolated node. BLSR STS numbers, East and West source and destination information, and East and West incoming, or outgoing VT traffic indications are displayed in the BLSR Squelch Table window. BLSR squelching is performed on STSs that carry STS circuits only. Squelch table entries will not appear for STSs carrying VT circuits or Ethernet circuits to, or from E-Series Ethernet cards provisioned in a multicard Ethergroup. These squelch tables contain entries with adjacent node IDs displayed, instead of source or destination node IDs.

## BLSR VT Squelch Tables in CTC

BLSR VT squelch tables only appear on the node dropping VTs from a BLSR and are used to perform VT-level squelching when a node is isolated. VT squelching is supported on the ONS 15454 and the ONS 15327 platforms. The ONS 15600 platform does not support VT squelching; however, when an ONS 15454 and an ONS 15600 are in the same network, the ONS 15600 node allows the ONS 15454 node to carry VT circuits in a VT tunnel. The ONS 15600 performs 100-ms STS-level squelching for each VT-access STS at the switching node in case of a node failure.

When using a VT circuit on a VT tunnel (VTT), or on a VT aggregation point (VAP), the VTT or VAP allows multiple VT circuits to be passed through on a single STS without consuming VT matrix resources on the cross-connect card.

In case of a source and destination node failure of a VTT, the switching node performs 100-ms STS-level squelching for the VTT STS. The node dropping VT traffic performs VT-level squelching. VT traffic on the VTT that is not coming from the failed node is protected.

An STS grooming node (VAP source) does not carry VT circuits through a VTT. The STS grooming node performs STS-level squelching for each STS timeslot at the switching node in case the VT-grooming (VAP destination) node fails. The node dropping VT traffic performs VT-level squelching for each VT timeslot in case the STS-grooming end node fails. No VT traffic on the VAP is protected during a failure of the STS-grooming node or the VT-grooming node.

The VT squelch table provides BLSR VT group number and channel indications, and East and West source information. To view the VT squelch table, double-click the VT with a check mark in the BLSR STS squelch table window. The check mark appears on every VT-access STS; however, the VT-squelch table appears only by double-clicking the check mark on the node dropping the VT. The intermediate node of the VT does not maintain the VT-squelch table.

## “Ring is Squelching STS Traffic” Condition

Release 7.0.x supports an informational Ring is Squelching STS Traffic (STS-SQUELCH-L) condition that can be raised on an OC-N facility. The STS-SQUELCH-L condition indicates that traffic is squelched due to node failure (traffic outage). If the node failure scenario includes the source or destination node, then switching the nodes will squelch all the STSs that originate from or are destined to the failure node. The condition resolves when the node is no longer failing.

## “Ring is Squelching VT Traffic” Condition

Release 7.0.x supports an informational Ring is Squelching VT Traffic (VT-SQUELCH-L) condition that can be raised on an OC-N facility. The VT-SQUELCH-L condition indicates that traffic is squelched due to node failure (traffic outage). If the node failure scenario includes the source node, the node dropping VT will squelch VT traffic. The condition resolves when the node failure is recovered.

## BLSR STS and VT Squelching

Release 7.0.x supports BLSR STS squelching for the ONS 15454, ONS 15327, and ONS 15600, and VT squelching for the ONS 15454, and ONS 15327, with limited VT squelching support (see below) provided by the ONS 15600. STS-level squelching is supported in previous releases. With VT-level squelching added in Release 7.0.x the STS squelch table now displays VT-access status for each STS (every entry) in the table. There is a check box in both the east and west sides for each entry of STS squelch table, and a check mark in this box indicates that the STS is VT-access.

Release 7.0.x nodes display STS and VT squelch tables depending on the type of circuits created. For example, if a fiber cut occurs, the BLSR squelch tables show STSs or VTs that will be squelched for every isolated node. Squelching replaces traffic by inserting the appropriate alarm indication signal path (AIS-P) and prevents traffic misconnections. For an STS with a VT-access check mark, the AIS-P will be removed after 100 ms.

### BLSR STS Squelch Tables in CTC

BLSR STS squelch tables show STSs that will be squelched for every isolated node. BLSR STS numbers, East and West source and destination information, and East and West incoming, or outgoing VT access indications are displayed in the BLSR Squelch Table window. BLSR squelching is performed on STSs that carry STS circuits only. Squelch table entries will not appear for STSs carrying VT circuits or Ethernet circuits to, or from E-Series Ethernet cards provisioned in a multicard Ethergroup.

### BLSR VT Squelch Tables in CTC

BLSR VT squelch tables only appear on the node dropping VTs from a BLSR and are used to perform VT-level squelching when a node is isolated. VT squelching is supported on the ONS 15454 and the ONS 15327 platforms. The ONS 15600 platform does not support VT squelching; however, when an ONS 15454 and an ONS 15600 are in the same network, the ONS 15600 node allows the ONS 15454 node to carry VT circuits in a VT tunnel. The ONS 15600 performs 100-ms STS-level squelching for each VT-access STS at the switching node in case of a node failure.

When using a VT circuit on a VT tunnel (VTT), or on a VT aggregation point (VAP), the VTT or VAP allows multiple VT circuits to be passed through on a single STS without consuming VT matrix resources on the cross-connect card.

In case of a source and destination node failure of a VTT, the switching node performs 100-ms STS-level squelching for the VTT STS. The node dropping VT traffic performs VT-level squelching. VT traffic on the VTT that is not coming from the failed node is protected.

An STS grooming node (VAP source) does not carry VT circuits through a VTT. The STS grooming node performs STS-level squelching for each STS timeslot at the switching node in case the VT-grooming (VAP destination) node fails. The node dropping VT traffic performs VT-level squelching for each VT timeslot in case the STS-grooming end node fails. No VT traffic on the VAP is protected during a failure of the STS-grooming node or the VT-grooming node.

The VT squelch table provides BLSR VT group number and channel indications, and East and West source information. To view the VT squelch table, double-click the STS with a check mark in the BLSR STS squelch table window. The check mark appears on every VT-access STS; however, the VT-squelch table appears only by double-clicking the check mark on the node dropping the VT. The intermediate node of the VT does not maintain the VT-squelch table.

## “Ring is Squelching STS Traffic” Condition

Release 7.0.x supports an informational Ring is Squelching STS Traffic (STS-SQUELCH-L) condition that can be raised on an OC-N facility. The STS-SQUELCH-L condition indicates that traffic is squelched due to node failure (traffic outage). If the node failure scenario includes the source or destination node, then switching the nodes that switched the traffic away from the failure will squelch all the STSs that originate from or are destined to the failure node. The condition resolves when the node is no longer failing.

## “Ring is Squelching VT Traffic” Condition

Release 7.0.x supports an informational Ring is Squelching VT Traffic (VT-SQUELCH-L) condition that can be raised on an OC-N facility. The VT-SQUELCH-L condition indicates that traffic is squelched due to node failure (traffic outage). If the node failure scenario includes the source node, the node dropping VT will squelch VT traffic. The condition resolves when the node failure is recovered.

## Link Consolidation

CTC provides the ability to consolidate the DCC and provisionable patchcord (PPC) links shown in the network view into a more streamlined view. Link consolidation allows you to condense multiple internodal links into a singular link. The link consolidation sorts links by class, meaning that all DCC links are consolidated together, for example. You can access individual links within consolidated links using the right-click shortcut menu. Each link has an associated icon.

Link consolidation is only available on non-detailed maps. Non-detailed maps display nodes in icon form instead of detailed form, meaning the nodes appear as rectangles with ports on the sides. Refer to the Cisco ONS 15454 Procedure Guide for more information about consolidated links.

## Data Communications Network Tool

Release 7.0.x CTC includes a data communications network (DCN) tool that assists with network troubleshooting for Open Shortest Path First (OSPF) networks. This tool, located in network view, executes an internal dump command to retrieve information about all nodes accessible from the entry point. The retrieved information is the same as you would get if you were to execute a dump using special networking commands. The contents of the dump file can be saved or printed and furnished to Cisco Technical Support for use in OSPF network support.

## Advanced Circuit Filtering and Export

Release 7.0.x adds an Advanced tab to the Circuit Filter dialog. With advanced circuit filtering you can filter on selected rings, nodes, links, or source/drop combinations.

Also, you can export the active Circuit window data in HTML, comma-separated values (CSV), or tab-separated values (TSV) format using the Export command from the File menu.

## Superuser Privileges for Provisioning Users

With Release 7.0.x Superusers can grant permission to Provisioning users to perform a set of tasks, including retrieving the audit log, restoring a database, clearing performance monitoring (PM) parameters, activating a software load, and reverting a software load. These privileges can only be set

using the node-level network element (NE) defaults, with the exception of the PM clearing privilege, which can be granted to a Provisioning user from the CTC Provisioning > Security > Access tabs. For more information about setting up Superuser privileges, refer to the Cisco ONS 15454 Procedure Guide.

## CTC Download Highest Level NET JAR File

As of Release 7.0.x CTC, during network topology discovery, polls each node in the network to determine which one contains the most recent version of the CTC software. If CTC discovers a node in the network that has a more recent version of the CTC software than the version you are currently running, CTC generates a message stating that a later version of CTC has been found in the network, and offers to install the CTC software upgrade JAR files. If you have network discovery disabled, CTC will not seek more recent versions of the software. Unreachable nodes are not included in the upgrade discovery.

## Local Domain Creation and Viewing

With Release 7.0.x a Superuser can control whether domains that any future users create and view persist globally (for all CTC sessions), or only locally (within the current CTC session in which they are created), as well as who can create domains (all users, or just Superusers). This control is given to Superusers by means of the NE default, CTC.network.LocalDomainCreationAndViewing. The factory pre-set default value is FALSE, meaning domain information is applied to all CTC sessions and only Superusers can create a domain or add a node to a domain. Setting the default to TRUE enables the option for local domain creation by any user.

## Enhanced Fault Management

Release 7.0.x adds increased flexibility for fault management. When an entity is put in the OOS,MT administrative state, the node suppresses all standing alarms on that entity. All alarms and events appear on the Conditions tab. You can change this behavior for the LPBKFACILITY and LPBKTERMINAL alarms. To display these alarms on the Alarms tab, you can set the NODE.general.ReportLoopbackConditionsOnOOS-MTPorts to TRUE in the NE Defaults editor.

## Rx and Tx Indication for TCAs

For electrical card or port PMs for which a direction, either Receive (Rx) or Transmit (Tx), can be detected, Release 7.0.x CTC and TL1 display the Rx or Tx value with the associated threshold crossing alert (TCA) description. For specific cards, port types, and PMs supported consult the Performance Monitoring chapter of the *Cisco ONS 15327 Reference Manual*.

## TL1

### TL1 Command Changes

#### Command Syntax Changes

The syntax of the following commands is changed in Release 7.0.x.

**ENT-TADRMAP** syntax:

ENT-TADRMAP[:<TID>]:<CTAG>::TIDNAME=<name>,[IPADDR=<ipAddr>],[PORT=<port>],[ENCODING=<encoding>],[NSAP=<nsapAddr>];

Is changed to:

ENT-TADRMAP[:<TID>]:<CTAG>::TIDNAME=<tidname>,[IPADDR=<ipaddr>],[PORT=<port>],[ENCODING=<encoding>],[NSAP=<nsap>];

**OPR-SYNCNSW** syntax:

OPR-SYNCNSW[:<TID>]:<CTAG>;

Is changed to:

OPR-SYNCNSW[:<TID>][:<aid>]:<CTAG>;

**RTRV-NE-SYNCN** syntax:

RTRV-NE-SYNCN[:<TID>]:<CTAG>[:::];

Is changed to:

RTRV-NE-SYNCN[:<TID>][:<aid>]:<CTAG>[:::];

**RTRV-SYNCN** syntax:

RTRV-SYNCN[:<TID>]:<aid>:<CTAG>[:::];

Is changed to:

RTRV-SYNCN[:<TID>][:<aid>]:<CTAG>[:::];

**RTRV-TADRMAP** syntax:

RTRV-TADRMAP[:<TID>][:<AID>]:<CTAG>:::MODE=<modeType>

Is changed to:

RTRV-TADRMAP[:<TID>][:<AID>]:<CTAG>[:::MODE=<modeType>]

**ED-NE-GEN** syntax:

ED-NE-GEN[:<TID>]:<CTAG>[:::NAME=<name>],[IPADDR=<ipaddr>],[IPMASK=<ipmask>],[DEFRTR=<defrtr>],[IIOPORT=<iioport>],[NTP=<ntp>],[SUPPRESSIP=<mode>];

Is changed to:

ED-NE-GEN[:<TID>]:<CTAG>[:::NAME=<name>],[IPADDR=<ipaddr>],[IPMASK=<ipmask>],[DEFRTR=<defrtr>],[IIOPORT=<iioport>],[NTP=<ntp>],[PROXYSRV=<isProxyServer>],[FIREWALL=<isFireWall>];

## Command Response Changes

The following TL1 response has changed in Release 7.0.x.

**RTRV-INV** response:

<aid>,<aidtype>::<pn>],[<hwrev>],[<fwrev>],[<sn>],[<clei>],[<twl1=nwl in code>],[<pluginvendorid>],[<pluginpn>],[<pluginhwrev>],[<pluginfwrev>],[<pluginsn>],[<ilossref>],[<productId>],[<versionId>],[<fpgaVersion>]

Is changed to:

<aid>,<aidtype>::<pn>],[<hwrev>],[<fwrev>],[<sn>],[<clei>],[<twl1=nwl in code>],[<pluginvendorid>],[<pluginpn>],[<pluginhwrev>],[<pluginfwrev>],[<pluginsn>],[<ilossref>],[<productId>],[<versionId>],[<fpgaVersion>],[<vendorId>]

## TL1 ENUM Items Added

Table 1 highlights ENUM items added for Release 7.0.x, by ENUM type.

**Table 1** *EQUIPMENT\_TYPE enum items added to Release 7.0.x*

Enum Name	Enum Value
EQUIPMENT_TYPE_ET_UNKNOWN	"UNKNOWN"
EQUIPMENT_TYPE_ET_UNPROVISIONED	"UNPROVISIONED"

EQUIPMENT\_TYPE is used in the following commands:

- CHG-EQPT
- ENT-EQPT

## Related Documentation

### Release-Specific Documents

- Release Notes for the Cisco ONS 15327, Release 7.0
- Release Notes for the Cisco ONS 15454 SDH, Release 7.0.2
- Release Notes for the Cisco ONS 15454, Release 7.0.2
- Release Notes for the Cisco ONS 15600, Release 7.0.2
- Release Notes for the Cisco ONS 15310-CL, Release 7.0.2
- Release Notes for the Cisco ONS 15310-MA, Release 7.0.2
- Cisco ONS 15327 Software Upgrade Guide, Release 7.0

### 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

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/techsupport>

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)

### Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

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

### Cisco Optical Networking Product Documentation CD-ROM

Optical networking-related documentation, including Cisco ONS 15xxx product documentation, is available in a CD-ROM package that ships with your product. The Optical Networking Product Documentation CD-ROM is updated periodically and may be more current than printed documentation.

### Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

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

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at [tech-doc-store-mkpl@external.cisco.com](mailto:tech-doc-store-mkpl@external.cisco.com) or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

## Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation 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 will find information about how to:

- 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, security notices, and security responses for Cisco products is available at this URL:

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

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at 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 have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—[security-alert@cisco.com](mailto:security-alert@cisco.com)

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For Nonemergencies—[psirt@cisco.com](mailto:psirt@cisco.com)

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

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

**Tip**

---

We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page 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)

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

---

## Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

## Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation 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, at this URL:

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

Access to all tools on the Cisco Technical Support & Documentation 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 & Documentation 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 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 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)—An existing 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 operations 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 the network is impaired, while 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.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, 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>  
or view the digital edition at this URL:  
<http://cisoiq.texterity.com/cisoiq/sample/>
- *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>
- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:  
<http://www.cisco.com/en/US/products/index.html>
- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:  
<http://www.cisco.com/discuss/networking>
- 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>

Use this document in conjunction with the documents listed in the “[Related Documentation](#)” section on page 15.

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)

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.

Copyright© 2007-2008 Cisco Systems, Inc. All rights reserved.

