Release Notes for Cisco ONS 15454 Release 2.3.5

Release Notes address closed (maintenance) issues, caveats, and new features for the Cisco ONS 15454. For detailed information regarding features, capabilities, hardware, and software, refer to *Cisco ONS 15454 User Documentation, Release 2.2.1.*

Contents

These release notes contain the following sections:

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

Changes to the Release Notes

This section documents supplemental changes that have been added to the *Release Notes for Cisco ONS 15454 Release 4.6.2* since the production of the Cisco ONS 15454 System Software CD for Release 4.6.2.

The following changes have been added to the release notes for Release 4.6.2.

Changes to Resolved Caveats

The following closed items have been added.

JRE Updates, page 5

DDTS # CSCed06531, page 14

DDTS # CSCed86946, page 14

DDTS # CSCec88426, CSCec88508, CSCed85088, page 14

DDTS # CSCec59739, CSCed02439, CSCed22547, page 14

DDTS # CSCec88402, CSCed31918, CSCed83309, CSCec85982, page 14

Caveats

Review the notes listed below before deploying the ONS 15454. Caveats with DDTS tracking numbers are known system limitations that are scheduled to be addressed in a subsequent release. Caveats without DDTS tracking numbers are provided to point out procedural or situational considerations when deploying the product.

Note As of Release 2.2.0, CMS (Cerent Management System) is entitled CTC (Cisco Transport Controller). If you are working with a pre-2.2 software release and see the term "CTC," you can assume the reference is to CMS.

Software Upgrades

DDTS # CSCdy65290 Upgrade Script Needed

To upgrade from Release 2.2.x to 2.3.4 using TCC cards, you must run the vfix.exe utility to patch the running software. The script must always be run prior to activation when a TCC is running Release 2.2, 2.2.1 or 2.2.2. This does not apply to TCC+ cards or software reverts.

The vfix.exe utility runs on any win32 based PC. The utility requires IP connectivity from the PC to the ONS 15454 that will receive the patch.

The vfix.exe utility can also be run from a command shell, or using your Windows Start > Run... menu option with the following usage:

```
usage: vfix <nodename>
```

Where <nodename> is the hostname or IP address of the ONS 15454.

The script must be run for each node to be upgraded.

Transport Management Compatibility

Upgrading to a new CTC release can create limitations to your ability to use the Cisco Transport Manager (CTM). If you are using CTM, before you choose to upgrade to a new CTC release you should check the latest CTM Release Notes for any possible compatibility issues. The CTM Release Notes can be found at:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/optnet/ctm/index.htm

System Software Upgrades

Minor traffic disruptions in excess of 50 ms might occur when upgrading software to Release 2.2.2 from a previous release. You should perform software upgrades during a maintenance window.

Note You are limited to two concurrent CTC sessions when performing a software upgrade. This limitation will be resolved in a future release.

Traffic Protection

Deleting Protection Groups

Delete protection groups only after traffic that switched to the protection card reverts back to the working card. If the protection group is deleted after a protection switch and traffic is carried on the protection card, perform the following steps:

Step 1 Recreate the protection group

Step 2 Switch traffic back to the working card

Step 3 Delete the protection group

Protection During Upgrades

When upgrading from Release 2.0.0 to a newer release, temporarily remove any 1:N protection groups prior to the upgrade. If empty slots are present on the side of the shelf that has a 1:N protection group defined, traffic can be lost for all cards on that side of the shelf. This caveat is restricted to systems that are upgrading from Release 2.0.0 to newer releases. This limitation does not apply when upgrading to new releases from Release 2.0.1 or subsequent releases.

TCC Protection Switching

When performing a manually-initiated TCC protection switch, Cisco recommends resetting the TCC card through CTC or the TL1 interface. All TCC switches conform to protection switching standards for BER counts that are not in excess of E10-3 and where completion time is less than 50 ms, which results in minimal traffic interruption. Switch errors will be resolved in a future release.

Active TCC/TCC+ Removal

The removal of an active TCC/TCC+ is supported in this release, but might result in traffic hits. If you must remove the active TCC/TCC+, perform a protection switch to the standby TCC/TCC+ (follow the instructions provided in the "TCC Protection Switching" section on page 3). This issue will be resolved in a future release.

Line Cards

DDTS # CSCct03114

SONET section data communication channel (SDCC) is supported on Ports 1 and 3 of the four-port OC-3 card. SDCC from either an ONS 15454 node or another vendor's product is not supported on Ports 2 and 4 of the OC-3 card. Therefore, when using an OC-3 card as a transport span between ONS 15454 nodes, you must use Ports 1 and 3 to ensure CTC visibility across nodes. Also, when subtending another vendor's product from an OC-3 card, the other vendor's SDCC is supported on Ports 1 and 3 only. This limitation will be resolved in a future release.

DDTS # CSCds34584: E1000-2 Only

When provisioning VLANs, you cannot provision the same VLAN on more than one port at a time. Each port must have a separately-provisioned VLAN. When you initially provision the cards, set the VLAN membership before enabling the port.

E1000-2/E100T

Do not use the repair circuit option with provisioned Ethernet circuits. This issue will be resolved in a future release.

Single-card EtherSwitch

From Release 2.2.1 forward, each E100/E1000 card can be configured as a single-card EtherSwitch configuration to allow STS 12c of bandwidth to be dropped at each card. The following scenarios for provisioning are available:

1. 12c
2. 6c 6c
3. 6c 3c 3c
4. 6c 6 STS-1s
5. 3c 3c 3c 3c
6. 3c 3c 6 STS-1s
7. 12 STS-1s

When configuring scenario 3, the STS 6c must be provisoned before either of the STS 3c circuits. This issue will be resolved in a future release.

Single-card and Multicard EtherSwitch

When deleting and recreating Ethernet circuits that have different sizes, you must delete all STS circuits provisioned to the EtherSwitch before you create the new circuit scenario. (See the preceding section, "Single-card EtherSwitch," for details.) This issue will be resolved in a future release.

DDTS # CSCds02031 E1000-2/E100T

Whenever you drop two 3c multicard EtherSwitch circuits onto an Ethernet card and delete only the first circuit, you should not provision STS-1 circuits to the card without first deleting the remaining STS-3c circuit. If you attempt to create an STS-1 circuit after deleting the first STS-3c circuit, the STS-1 circuit will not work and no alarms will indicate this condition. To avoid a failed STS-1 circuit, delete the second STS-3c prior to creating the STS-1 circuit. This issue will be resolved in a future release.

Maintenance and Administration

Note Whenever a proposed change occurs, the "Are you sure" dialog box appears to warn you that the action can change existing provisioning states or can cause traffic disruptions.

Note Changing the AIP card might cause some circuits to become incomplete. In CTC, repair each circuit, one node at a time, using the Repair button from the Circuits tab. Some circuits might still erroneously appear as incomplete. After completing the repair operation, you must relaunch CTC.

Note Redundant host routes are not supported in Release 2.2.2.

JRE Updates

Cisco ONS platforms ship with a Java Runtime Environment (JRE) from Sun Microsystems. Occasionally Sun releases maintenance releases to the JRE. The Sun Microsystems website lists JRE maintenance releases and the issues resolved for each. Cisco recommends that you review these listings to determine if the issues resolved in any given JRE maintenance release warrant a JRE upgrade for your particular network. Cisco tests only with the specific JRE actually shipped with the ONS software CD.

DDTS # CSCea31229

A changed time zone may not reflect in subsequent alarm time stamps. This issue has been seen after changing a time zone on a LAN-connected node, using SNTP server. If the time zone is set to, say, "Alaska," the change may appear to take effect, but a subsequent alarm raised may still reflect the old time zone. This issue is resolved in Release 3.4.

DDTS # CSCdy80748

You must wait at least 30 seconds after the last provisioning change before resetting a TCC. The TCC needs time to save the database before any TCC reset. This is as designed.

DDTS # CSCdz10284 and CSCdy81915

Do not delete more than 20 circuits at a time in CTC. This issue is resolved in Release 3.4.

DDTS # CSCdy71862

In some circumstances, invalid Ethernet circuits may exist in CTC after a database restore. The workaround is to relaunch CTC. This issue is resolved in Release 3.3.

DDTS # CSCdt90247 and CSCdu58071 Fast Start Synchronization (FSTSYNC) Alarms

Timing offsets can generate fast start synchronization alarms. These alarms can remain uncleared for up to a few minutes, depending on the degree of the offset. They do not indicate any instability of the ONS 15454's timing, and this is expected behavior.

DDTS # CSCds15889: Add Node Feature

The Add Node feature is only supported when you add a new, isolated node (one not already participating in a network) in either BLSR or UPSR configuration. If a node is already part of a network, the Add Node feature is not supported. This issue will be resolved in a future release.

DDTS # CSCdt57008: Database Provisioning

Do not reset TCC cards for at least 30 seconds after the last provisioning change. If you change the database and reset the TCC card within one minute of the change, the database synchronization process might not have time to complete and the provisioning will be lost. This issue will be resolved in a future release.

Interoperability

DDTS # CSCds13769: Fujitsu FLM-150 and Nortel OC-3 Express

You cannot provision the FLM-150 and OC-3 Express in 1+1 revertive switching mode. The problem occurs when the ONS 15454 issues a user request in revertive mode to the protect channel. When the user request is cleared, the ONS 15454 issues a No Request. However, the FLM-150 and OC-3 Express issues a Do Not Revert, which causes traffic to remain on the protection channel. According to Telcordia standard GR-253, section 5.3.5.5, the FLM-150 and the OC-3 Express should respond with a No Request.

SONET/SDH

DDTS # CSCct04091

You must provision all circuits as bidirectional. Unidirectional circuits are not supported. If a unidirectional circuit is provisioned, loss of signal (LOS) alarms are generated. This is resolved in Release 3.1, but still exists in Release 2.3.4.

UPSR Functionality

DDTS # CSCct03852

When a UPSR or BLSR protection switch occurs, no alarm is reported to indicate that the protection switch occurred. An event is reported in the event log, but not as a standing alarm. The ability to make this event an alarm is being considered for a future release.

Note Once a UPSR circuit is created, the ONS 15454 does not support converting UPSR spans to 1+1 or BLSR. The event is reported in the event log but not as a standing alarm. A protection switch on the 1+1 or BLSR span can cause a traffic outage.

BLSR Functionality

DDTS # CSCea27917

A two-fiber BLSR can incur multiple traffic hits on a switch to working when the Wait to Restore (WTR) timer is set to zero minutes. To avoid this issue, make sure the WTR is set to 30 seconds or greater. This issue has been resolved in Release 3.0.3. The WTR of zero has been removed from Release 3.0.3 and later.

DDTS # CSCdz05588

Rarely, BLSR traffic may be temporarily lost following a user switch and subsequent lockout. To avoid this issue, always clear a user switch request before performing a lockout. This issue is resolved in Release 3.4.

DDTS # CSCdy73838

In two-fiber BLSR, if a higher priority switch is induced on top of an existing switch, switch times of several hundred ms can occur. This issue is resolved in Release 3.4.

DDTS # CSCdz12010

A BLSR default K byte alarm may become stuck after BLSR creation. This can occur when there are more than four nodes in a two-fiber BLSR. To recover from the stuck alarm, reset either the affected trunk card or the XC/XCVT. This issue is resolved in Release 3.4.

BLSR Database Restore

When restoring the database on a BLSR, follow these steps:

Step 1 To isolate the failed node, issue a Force switch toward the failure node from the adjacent east and west nodes.

Step 2 If more than one node has failed, restore the database one node at a time.

Step 3 After the TCC has reset and booted up, release the Force switch from each node.

BLSR STS Channel Numbering Restriction

When provisioning a BLSR you must ensure that the span STS channel number is the same for all spans from the source node to the destination node. This is true for all STS circuits. For VT circuits, the span STS channel number and the VT number within must also be the same from source to destination. Either auto-routing or manual routing can be used to route BLSR circuits, as long as the above constraints are met. This constraint also applies for VT tunnels. If these constraints are not followed, squelching will not work as expected in a node-isolation scenario.

Note VT squelching is not supported in this release.

Documentation

Spanning Tree

In section 7.6, Spanning Tree, of the *Cisco ONS 15454 User Documentation*, Release 2.2.1, paragraph 1, line 1, the reference to "IEEE 802.1Q STP" should read "IEEE 802.1D STP." This will be corrected in Release 3.0

Alarms

In section 9.71 and 9.72 of the *Cisco ONS 15454 User Documentation*, Release 2.2.1, the references to "SDBER" and "SFBER" should read "SD" and "SF," respectively. This will be corrected in Release 3.0.

In section 9.74 of the *Cisco ONS 15454 User Documentation*, Release 2.2.1, the reference to "Minor" should read "NR." This will be corrected in Release 3.0.

In section 9.51 of the *Cisco ONS 15454 User Documentation*, Release 2.2.1, the reference to "Critical and Minor" should include "Major." This will be corrected in Release 3.0.

In section 9 of the *Cisco ONS 15454 User Documentation*, Release 2.2.1, the FSTSYNC, ST3, TRMT, AUTOSW-UNEQ, AUTOSW-AIS, AIS and DUS alarms are not included. This will be addressed in Release 3.0.

UPSR and BLSR

For the BLSR and UPSR "drop a node" procedures, insert the replacement text below in the following locations of the *Cisco ONS 15454 User Documentation* :

Page 4-13, Step 8

Page 4-27, Step 6

"One circuit at a time, delete and recreate any circuits that ingressed and egressed through the deleted node on different STSs. For example, if the circuit arrives at the node on STS 1 and leaves the node on STS 2, you need to perform this step."

System Reset

The following updated procedure will be added to the *Cisco ONS 15454 User Documentation* :

Procedure: Perform a Soft Reset

Note This procedure is also used to switch traffic from the primary to the secondary TCC.

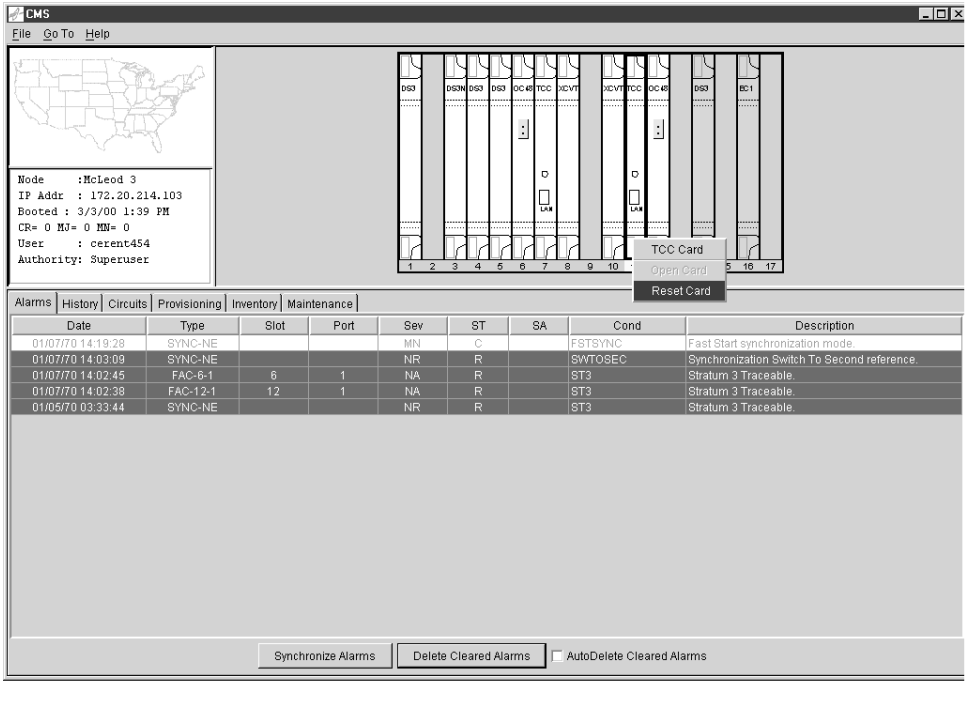
Step 1 Display the node view in CTC.

Step 2 Right-click the standby TCC card to reveal a pull down menu.

Step 3 Click **Reset Card** (see Figure 1). The "Are You Sure" dialog box appears.

Step 4 Click **Yes**.

Figure 1



Note To ensure that all temporary alarms have cleared, allow a minimum of 3 minutes to pass before performing Step 5.

Step 5 Confirm that the TCC returns to standby mode after the reset.

Step 6 Right-click the active TCC card to reveal a pull-down menu.

Step 7 Click **Reset Card** (see Figure 1). The "Are You Sure" dialog box appears.

Step 8 Click **Yes**. The "Lost Connection to Node, Changing to Network View" dialog box appears.

Step 9 Click **OK**.

Resetting, Removing, and Replacing XC/XCVT Cards

The following updated procedure will be added to the *Cisco ONS 15454 User Documentation* :

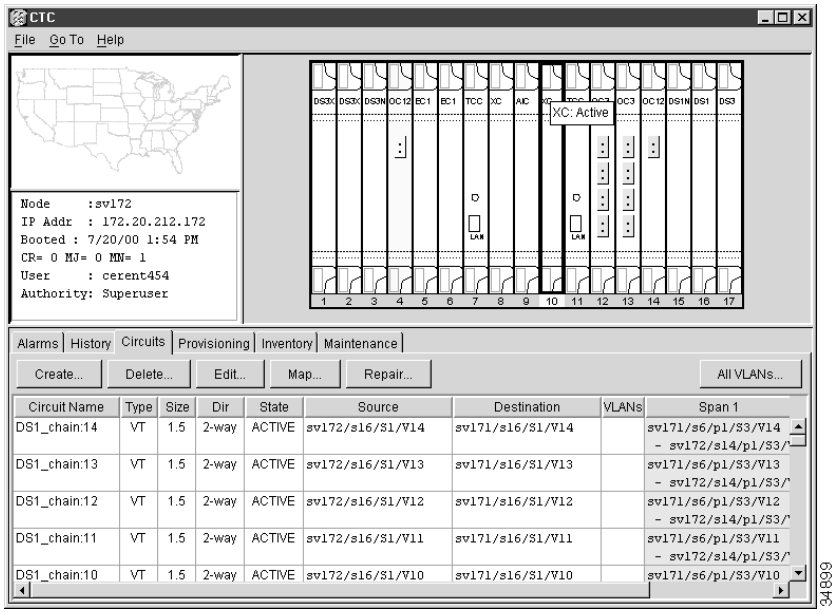
Procedure: Remove XC/XCVT Cards While In-Service

Caution The removal of any active traffic-bearing card from the ONS 15454 could result in traffic interruption. Use caution when replacing traffic-bearing cards and verify that only inactive or standby cards are being replaced. If the active card needs to be replaced, follow the steps below to switch the XC/XCVT card to standby prior to removing the card from the node.

Step 1 Determine the active XC/XCVT card. The ACT/STBY LED of the active card is green. The ACT/STBY LED of the standby card is yellow.

Note You can also place the cursor over the card graphic to display a tooltip identifying the card as active or standby.

Figure 2



Step 2 In the node view, select the **Maintenance > XC Cards** tabs.

Step 3 From the **Slot Operation** menu, choose **Manual**.

Step 4 Click **Apply**.

Note A minor alarm appears on the manually-switched slot. After the active XC/XCVT goes into standby, the original standby slot becomes active. This causes the ACT/STBY LED to become green on the former standby card.

Step 5 From the **Slot Operation** menu, choose **Clear.**

Step 6 Click **Apply**.

Step 7 Physically remove the new standby XC/XCVT card from the ONS 15454.

Step 8 Insert the replacement XC/XCVT card into the empty slot. The replacement card boots up and becomes ready for service after approximately one (1) minute.

TL1

DDTS # CSCdy87404

You must ensure that you use the canc-user command on completion of a TL1 superuser session if you want that session closed. This issue is resolved in Release 3.2.1.

Commands not Supported as of Release 2.2

The following commands are not supported as of Release 2.2:

- DLT-<MOD2>, ENT-<MOD2>, RMV-<MOD2>, and RST-<MOD2> do not apply to DS1, STS1, STS3C, STS12C, STS48C, VT1
- ED-EQPT
- RTRV-USER-SECU
- ED-VT1
- RTRV-VT1

These commands will be supported in a future release.

False Positives

Although the system responds with COMPLD for each of the following commands, the operation requested by the command does not occur.

- ALW-SWDX-EQPT
- INH-SWDX-EQPT
- OPR/RLS-LPBK-DS1 (terminal loopback)
- OPR-SYNCNSW
- OPR-UPGRADE
- RLS-SYNCNSW
- SW-DX-EQPT

This will be corrected in a future release.

Commands Removed as of Release 2.2

The RTRV-ALM-LOG command is no longer supported. It has been replaced with the RTRV-LOG command.

Cross-Connect Types for ENT-CRS Commands

The Release 2.2 and Release 2.2.1 user manual sections on TL1 do not include possible values for cct (type CCT_SUB) in ENT-CRS-<STS_PATH>. These will be included in Release 3.0. The acceptable values are:

CCT Values	Description
1WAY	A unidirectional connection from a source tributary to a destination tributary
2WAY	A bidirectional connection between the two tributaries
MON	Monitored cross-connection
UPSR	Bidirectional UPSR entrance/exit
UPSR-DC	UPSR multicast drop with 2-way continue
UPSR-DROP	UPSR unicast drop
UPSR-EN	UPSR multicast End Node with 1-way continue
UPSR-HEAD	UPSR uni/multicast ring entrance
UPSR-UPSR	Single-node UPSR interconnect

The Release 2.2 user manual section on TL1 does not include possible values for cct (type CCT_SUB) in ENT-CRS-VT1. These will be included in Release 3.0. The acceptable values are:

CCT Values	Description
1WAY	A unidirectional connection from a source tributary to a destination tributary
2WAY	A bidirectional connection between the two tributaries
MON	Monitored cross-connection

Caution Using any of the UPSR cct types from CCT_SUB (for example, UPSR, UPSR-DC, UPSR-DROP, UPSR-EN, UPSR-HEAD, and UPSR-UPSR) is blocked with Release 2.2.2. However, trying to delete CTC-created VT UPSR circuits using TL1 can cause the TCC to reboot. This only applies to VT circuits and will be corrected in Release 3.0.

Deletion of UPSR Circuits

In the case where a UPSR circuit is created from S1&S2 to D1 (for example, ENT-CRS-STS1::S1&S2,D1:::UPSR;), this entire UPSR circuit is created as one unit within the ONS 15454. A command to delete a portion of the circuit deletes the entire unit. Thus, the command DLT-CRS-STS1::S1,D1; or DLT-CRS-STS1::S2,D1; deletes both the S1-D1 and S2-D1 connections.

Using the full UPSR circuit identification in the delete command, for example, DLT-CRS-STS1:: S1&S2,D1; results in an IIAC /*AID List Length Mismatch */ error message.

This will be resolved in a future release.

Creation of UPSR Circuits

Consider these variations when you create STS UPSR circuits in the ONS 15454:

a) S1&S2,D1

Using the S1&S2,D1 parameter order, for example, in the ENT-CRS-STS1::S1&S2,D1:::UPSR; command, works correctly and sets up a 2WAY UPSR circuit.

b) S1&S2, D1&D2

Using the S1&S2, D1&D2 parameter order, for example, in the ENT-CRS-STS1::S1&S2,D1&D2:::UPSR; command, yields UPSR circuits between S1&S2 and D2. Thus, ENT-CRS-STS1::S1&S2,D1&D2:::UPSR; and ENT-CRS-STS1::S1&S2,D2:::UPSR; function identically.

If the second parameter is invalid, for example, in the ENT-CRS-STS1::S1&S2,D1&BAD_VALUE:::UPSR; command, a UPSR circuit between S1&S2 and D1 is created.

c) S1,D1&D2

Use of the S1,D1&D2 parameter order, for example, in the ENT-CRS-STS1::S1,D1&D2:::UPSR; command, is rejected with an SDBE /*Cannot Create UPSR Crossconnect */ error message.

As a workaround to create the same two-way UPSR cross-connect, list the two-parameter portion of the circuit first (for example, ENT-CRS-STS1::D1&D2,S1:::UPSR;).

This will be resolved in a future release.

Maintenance Issues Closed in Release 2.3.5

Line Cards

DDTS # CSCed06531

Malformed IP packets can potentially cause the XTC, TCC/TCC+/TCC2 and TCCi/TCC2 control cards to reset. Repeated transmission of these malformed packets could cause both the control cards to reset at the same time. This issue is resolved in Release 5.0, and maintenance Releases 4.1.4, 2.3.5, 4.0.3, and 4.6.2.

DDTS # CSCed86946

Malformed ICMP packets can potentially cause the XTC, TCC/TCC+/TCC2 and TCCi/TCC2 control cards to reset. Repeated transmission of these malformed packets could cause both the control cards to reset at the same time. This issue is resolved in Release 5.0, and maintenance Releases 4.1.4, 2.3.5, 4.0.3, and 4.6.2.

DDTS # CSCec88426, CSCec88508, CSCed85088

Malformed TCP packets can potentially cause the XTC, TCC/TCC+/TCC2, and TCCi/TCC2 control cards to reset. Repeated transmission of these malformed packets could cause both the control cards to reset at the same time. This issue is resolved in Release 5.0, and maintenance Releases 4.1.4, 2.3.5, 4.0.3, and 4.6.2.

DDTS # CSCec59739, CSCed02439, CSCed22547

The XTC, TCC/TCC+/TCC2 and TCCi/TCC2 control cards are susceptible to a TCP-ACK Denial of Service (DoS) attack on open TCP ports. The controller card on the optical device will reset under such an attack.

A TCP-ACK DoS attack is conducted by withholding the required final ACK (acknowledgement) for a 3-way TCP handshake to complete, and instead sending an invalid response to move the connection to an invalid TCP state. This issue is resolved in maintenance Releases 4.1.4, 2.3.5, 4.0.3, and 4.6.2.

DDTS # CSCec88402, CSCed31918, CSCed83309, CSCec85982

Malformed UDP packets can potentially cause the XTC, TCC/TCC+/TCC2, and TCCi/TCC2 control cards to reset. Repeated transmission of these malformed packets could cause both the control cards to reset at the same time. This issue is resolved in Release 5.0, and maintenance Releases 4.1.4, 2.3.5, 4.0.3, and 4.6.2.

DDTS # CSCdw48828

If a near end protection switch is initiated within 30 seconds of a TCC switch, traffic will be lost. Traffic can be restored by forcing traffic away from the active span and then releasing the force. To avoid this issue, lock the spans on the neighboring nodes before doing the TCC reset or reseat. This will prevent an outage as long as all spans remain intact. This issue is resolved in Releases 2.3.4, 3.2.1, and later.

DDTS # CSCdy31096

A TCC memory corruption can occur when either of the following occur:

- A user logs into the VxWorks shell with a telnet client that sends only \r (e.g no \n) after entering the password.
- A user types more than 512 characters at the login prompt.

If the former occurs the TCC may reset after closing the telnet session.

If the latter occurs the TCC will typically reset immediately.

To avoid this issue, do not use the VxWorks telnet interface if your telnet client does not send \r\n to terminate lines; and also, do not type more than 512 characters at the logon prompt. This issue is resolved in Releases 2.3.4, 3.4, and later.

DDTS # CSCdv44748

After resetting or replacing the standby TCC, the standby TCC may change to the READY state (standby light illuminates indicating the TCC is ready to become active) before a database synchronization has necessarily taken place. A TCC switch before database synchronization can result in partial or complete provisioning loss. This issue is resolved in Release 2.3.4.

DDTS # CSCdz18060

Rarely, the standby TCC may fail to copy the database from the active TCC after a provisioning change. This may occur due to heavy load on the node at the time of transfer. If this occurs, the database on the standby TCC will be out of sync with the database on the active TCC. To correct this situation, make a provisioning change that will have no service affecting implications (for example, a change to contact information, or a description) to force another database save. This issue is resolved in Release 2.3.4, Release 3.4.1, and later.

Note To ensure proper database synchronization on Release 2.x prior to Release 2.3.4, or on Release 3.x prior to Release 3.4.1, run the memAudit.exe script, located on the software CD. For instructions, see the memAudit_readme1.htm file, also located on the software CD.

DDTS # CSCea03171

TCC memory exhaustion (the MEM-LOW or MEM-GONE alarm will be raised) can lead to unpredictable behavior. This issue has been resolved in Release 2.3.4 (and Release 5.0 forward) by increasing the threshold at which the memory related alarms are raised. Also, an automatic TCC reset will occur when memory reaches 180 K in Release 2.3.4 (and Release 5.0 forward).

DDTS # CSCdv65569

In software releases prior to Release 3.0, when a TCC resets, DS-N protection may fail, causing traffic loss. This can result in the protect card becoming active while the working card is also active. To restore the protect card to the correct state, reset it. This issue is resolved in Release 2.3.3.

DDTS # CSCds86889

If you insert or soft-reset a TCC card while in node view, when the GUI indicates that the card has gone into standby, switch to card view to ensure that the card has truly entered the standby state. The card view may reveal that the card is still loading. Wait until the card view indicates that the card is in standby before relying on the card for traffic protection. This issue is resolved in Release 2.2.2.

DDTS # CSCdu14682

In Release 2.2.2 traffic loss can occur after removing a Slot 7 standby TCC. This issue is resolved in Release 2.3.3.

DDTS # CSCdu49768 and CSCdu34969

When you reset or reseat an active TCC, if a near end protection switch is initiated within 30 seconds of the TCC switch, traffic will be lost. Traffic can be restored by forcing traffic away from the active span and then releasing the force. To avoid this issue, lock the spans on the neighboring nodes before performing the TCC reset or reseat. This will prevent an outage as long as all spans remain intact. This issue is resolved in Releases 2.3.4, 3.2.1 and later.

DDTS # CSCds50463

E100 and E1000 improperly filter IS-IS Hello frames, preventing dynamic routing in IS-IS networks. This issue is resolved in Release 2.2.2.

DDTS # CSCdt03823 and # CSCdr94635

CV-Ls and the associated PMs (ES-L, SES-L, and UAS-L) can fail to count on EC1-12 or OC-3 cards. This issue is resolved in Release 2.2.2.

Ethernet Functionality

DDTS # CSCds87459

Changing the VLAN configuration of an Ethernet port causes a traffic outage that exceeds 15 seconds. If this change causes the Spanning Tree Protocol to reconverge, the outage will last roughly 45 seconds. Traffic recovery time will typically be less than 0.5 seconds when adding a VLAN to a port. This issue is resolved in Release 2.2.2.

Note Adding a VLAN to a circuit will still result in a 45 second outage when spanning tree reconverges.

DDTS # CSCdr94172

Multicast traffic can cause minimal packet loss on the E1000-2 boards. If packet loss occurs, it is expected to be less than 1%. This issue is resolved for broadcast in Release 2.2.1, and for broadcast, OSPF, and low-rate BPDU multicast in Release 2.2.2. Line-rate multicast traffic is supported in Release 4.0 on E-series, or with a hardware upgrade.

DDTS # CSCds46919

Low-rate multicast traffic can cause unicast frame loss if multicast frames are followed immediately by unicast frames. This issue is resolved in Release 2.2.2 for the most commonly-used frame types, including broadcast, OSPF, and BPDU multicast.

DDTS # CSCds07778

Excessive Ethernet traffic on the TCC/TCC+ management port might have reset the TCC/TCC+. You can retrieve a LAN Overflow alarm with the RTRV-ALM-ALL TL1 command. (After the traffic has passed you can also see this alarm in CTC.) This issue is resolved in Release 2.2.2. Interrupts are now limited so that the TCC CPU cannot be overwhelmed by a broadcast storm or a unicast attack.

Synchronization

DDTS# CSCdr03214

During software upgrades, line-timed network elements (NEs) can lose connectivity to their primary reference source. Connectivity loss forces the NEs into hold-over or causes a switch to the secondary reference source, but does not affect traffic. This issue is resolved in Release 2.2.2.

Maintenance and Administration

Transmission Control Protocol Specification

A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection might be automatically reestablished. In other cases, a user must repeat the action (for example, open a new Telnet or SSH session). Depending on the attacked protocol, a successful attack might have consequences beyond terminated connection that also must be considered. This attack vector is only applicable to those sessions that terminate on a device (such as a router, switch, or computer) and not to those sessions that only pass through the device (for example, transit traffic that is being routed by a router). Also, this attack vector does not directly compromise data integrity or confidentiality.

All Cisco products that contain TCP stack are susceptible to this vulnerability.

This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and describes the vulnerability as it applies to Cisco products that run Cisco IOS® software.

A companion advisory that describes the vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

This issue is resolved in Releases 2.3.5, 4.1.4 and 4.6.2.

DDTS # CSCec20521

After adding or deleting a static route with a destination address that is included in the 192.168.190.x range, cards in the node reboot. This issue is resolved in Releases 2.3.5, 4.0.2, 4.1.1, and 4.6.

DDTS # CSCdy47156

A memory leak can occur after bulk PM retrieval. The only application that is likely to trigger this issue is the Cisco Transport Manager (CTM). Although the memory leak is small, CTM gathers PM data every fifteen minutes, so the amount of memory lost grows over time, and thus, can become more serious over time. To avoid this issue, do not use CTM to gather PM data. This issue is resolved in Release 2.3.4.

DDTS # CSCds52295

In previous releases it was possible to establish an FTP session to the TCC, or TCC+ by entering any strings for the userid and password. This issue is resolved in Release 2.3.3.

DDTS # CSCdt65864

In previous releases, if a 1+1 lockout is in place and the working/active card is removed, traffic does not restore after releasing the lockout. This issue is resolved in Release 2.3.3.

DDTS # CSCdt84146 and CSCdy70756

In previous releases passwords were stored in plain text in the running Cisco ONS image of the database on the TCC, TCC+ or XTC. This issue is resolved in Release 2.3.3.

DDTS # CSCdt86355

In previous releases, an apparent mismatch of information between CTC and a node (for example, an I/O card is reported missing but is actually up and running; bogus alarm conditions are raised; etc.) could occur if CTC was improperly initialized and operating in a large (20+ node) DCC domain. This issue is resolved in Release 2.3.3.

DDTS # CSCdt95923

In previous releases, under certain conditions, the Ethernet transmit queue would become corrupted and cease to transmit packets. The primary symptom is that the TCC will no longer respond to a ping of the LAN interface. However, the GNE would still be accessible via the DCC if the LAN interface is disconnected. This issue is resolved in Release 2.3.3.

DDTS # CSCdt73033

In previous releases, if you were supporting a proxy ARP-based SDCC interconnected network and the network required redundant gateway network elements (GNEs), you could lose management network connectivity due to lack of ability to provision such redundancy. This issue is resolved in Release 2.2.2. You can now have redundant GNEs on the same network span.

DDTS # CSCct01212: Daylight Savings Time

The CTC clock daylight savings time activation for October, which sets the clock back one hour, occurs at 4:00 a.m. (0400) rather than at 2:00 a.m. (0200). This issue is resolved with Release 2.2.2.

DDTS # CSCct02396: Time Zone Display

The CTC time zone is shown as Pacific Time regardless of the setting chosen. This issue is resolved in Release 2.2.2, and time zones display correctly for all locations.

DDTS # CSCds71355: Timing Pane

The timing pane in the Maintenance tab of the node view does not refresh in real time. This issue is resolved in Release 2.2.2.

DDTS # CSCds71415: Inventory Pane

The inventory pane does not refresh in real time. This issue is resolved in Release 2.2.2.

DDTS # CSCds91623: Provisioning Screen

The advice displayed on the provisioning screen for protect cards can be confusing to some users, because it might not make it clear that users should not attempt to provision a protect card. This issue is resolved in Release 2.2.2. The text of the advice has been edited for clarity. To enforce the advice on the screen, the user is no longer allowed to enter provisioning data for a protect card.

DDTS # CSCdr98353

Physically pulling a card to switch traffic back to a working card might have affected traffic. This issue is resolved for optical cards in Release 2.2.2.

DDTS # CSCds79099

On a Windows 2000 system, CTC did not start from a browser. This issue is resolved in Release 2.2.2.

DDTS # CSCds86889

Prior to Release 2.2.2, the node view of a recently inserted or soft-reset TCC card might have prematurely shown that the card moved from loading to standby. This issue is resolved in Release 2.2.2.

SNMP

DDTS # CSCdw75755

In previous releases, malformed SNMP traps could cause TCC resets. Firewalling or Access Control Lists were necessary to prevent the possibility of SNMP traps being sent into an ONS 15454 from external systems. (For more information, please consult the PSIRT notification on SNMP vulnerabilities.) This issue is resolved in Release 2.3.3.

DDTS # CSCdv62307

In previous releases, the community string “public” is hard coded and it is not possible to change it. By using it, an attacker is able to extract information available in the SNMP MIB on the TCC, TCC+ or XTC. User names and passwords cannot be extracted using this method. This issue is resolved in Release 2.3.3.

SONET

DDTS # CSCdr12777

When changing the mode from SONET to SDH or vice versa on an OC-3 card participating in a 1+1 linear APS group, perform the following procedure in CTC to ensure correct 1+1 linear switching:

Step 1 Display the node view and click the Provisioning tab.

Step 2 Select the correct protection group.

Step 3 Toggle the Bidirectional switching mode check box, and click Apply.

Step 4 Toggle the Bidirectional switching mode check box again and click Apply.

Improvements in Release 2.2.2 have eliminated the need for this procedure.

TL1

DDTS # CSCdy53297

Logging into TL1 generates a minor memory leak (32 bytes). This issue is resolved in Release 2.3.4.

New Features and Functionality

This section describes new features and functionality for Release 2.2.2.

Software

Microsoft Windows 2000 Support

As of Release 2.2.2, CTC is fully supported for use with the Microsoft Windows 2000 operating system.

Java Runtime Environment Compatibility

Release 2.2.2 supports web browsers running Java Runtime Environment (JRE) 1.2.2 and JRE 1.3.0.

Note A workstation running JRE 1.3.0 cannot log into an ONS 15454 running Release 2.2.1 or prior.

Warning Message on Circuit Switch

If you attempt a Manual or Force switch, you receive a warning message stating that if a failure condition exists the action might not be taken immediately, in which case the request will be queued. This message is designed to alert you to the fact that the action might be delayed pending cleared conditions. The CTC might not complete a Manual switch if conditions are present that can result in traffic loss.

Database Restore Warning Added

As of Release 2.2.2, a dialog box warns you of possible traffic loss before allowing a database restore from another node or a database restore from a prior release on the same node.

Default User Name Change

The default user name of CISCO15 (case sensitive) has been added to the list of users in the security panel. When a Cisco ONS 15454 has been upgraded with software release 2.2.1 or greater, both the old and new default user names appear. A new ONS 15454 with software release 2.2.1 only supports the CISCO15 default user name only. The CISCO15 user, by default, has a security level of superuser and cannot be deleted or have its security level changed; however, a new password can be assigned for either default user name.

Software Revert

New to Release 2.2.1, the ONS 15454 introduces software revert. The provisioning database stores all system-provisioning data including cross-connects, I/O card types, port states, timing information, and SDCC settings. The node name, IP address, subnet mask, and default gateway are stored in the system database and will remain intact after a software revert.

In prior software releases, software reverts required a backup to upload the former software load. Although a copy of the former software load is stored in memory, Cisco recommends creating a backup with every software upload.

When upgrading to a new software load, a copy of the former software load (that is, a snapshot of the software load and provisioning database) is stored in the standby sector of memory. If the provisioning database has been updated after a software upload, a software revert will not revert the updates to the provisioning database.

Release 2.2.1 establishes a baseline for the software revert feature.

Note Reverting to a provisioning database requires a TCC+ rather than a TCC because of the additional memory required to store a copy of the previous provisioning database.

Single-Card EtherSwitch Over UPSR

You can now configure single-card EtherSwitch circuits over a UPSR and enable UPSR type protection for the Ethernet circuit under this configuration. The UPSR circuits can be provisioned as you would a SONET circuit.

Caution You can configure multi-card EtherSwitch circuits over UPSR spans, but only if no UPSR span is provisioned touching a node that is an Ethernet drop. This precludes provisioning end-to-end UPSRs (disallowed in Release 2.2.2). Also, when you configure multi-card EtherSwitch over a UPSR, you must provision the spans manually and ensure that all of the arrows on each UPSR span point in the same direction.

Subnet IDs

CTC now supports the setting of a subnet field (or ID) to all zeros or all ones.

Background:

CTC has not previously supported IP addresses having the value 0 or -1 (all zeros or all ones) for any of the <Host-number>, <Network-number>, or <Subnet-number> fields. Disallowing all-one or all-zero field values forces you to use fields that are at least two bits long. However, the International Organization for Standardization (IOS) supports subnet fields with all zeros or all ones.

TL1

Commands Changed

- In the DLT-CRS-<STS_PATH> and DLT-CRS-VT1 commands, <to> was added to comply with Telcordia standard GR-199.
- In the ED-FFP-<OCN_TYPE>, ED-FFP-EQPT, ENT-FFP-<OCN_TYPE>, ENT-FFP-EQPT, RTRV-FFP-<OCN_TYPE>, and RTRV-FFP-EQPT commands, the order of the <RVTT> and <RVTM> parameters was changed.
- The INIT-SYS: command only resets equipment. We do not support the phase parameter in this release.
- The OPR-LPBK-<OCN_TYPE>, OPR-LPBK-DS1, OPR-LPBK-EC1, OPR-LPBK-T1, OPR-LPBK-T3, RLS-LPBK-<OCN_TYPE>, RLS-LPBK-DS1, RLS-LPBK-EC1, RLS-LPBK-T1, and RLS-LPBK-T3 commands no longer use the <location> parameter.
- In the OPR-PROTNSW-<OCN_TYPE> command, the <cc> and <dirn> parameters were removed and the <dnfield> parameter was added.

- In the RLS-PROTNSW-<OCN_TYPE> command, the <dirn> parameter was removed.
- In the RTRV-LOG command, the <log_type> parameter was removed.

Response Changes

In response to the RTRV-LOG command, the Release 2.1.x system replied with a logtype (for example, REBOOT). As of Release 2.2, the system replies with the response:

"<aid>,<seq>:CURRENT=<current>,PREVIOUS=<previous>,<condition>, <serv_eff>,TIME=<time>,DATE=<date>:[<desc>]"

For the RTRV-EQPT command, if_grp has been removed from the response.

As of Release 2.2.2, alarm messages have been improved to include the type (path or line) for BER Threshold Alarms, in addition to the other information given.

Access Identifier Additions

In the ALL_THR parameter table, the T-CVS, T-ESS, T-SESS, T-PJNEG-GEN, and T-PJPOS-GE values were added.

New Conditions

The following new conditions are reported via TL1 in this release:

LANOVERFLOW indicates there is a broadcast storm on the network management LAN.

MEM-GONE indicates that software operations exceed the memory capacity of the TCC/TCC+ card.

MEM-LOW indicates that data generated by software operations is close to exceeding the memory capacity of the TCC/TCC+ card.

RMON-ALARM indicates that a Remote Monitoring (RMON) alarm occurred.

RMON-RESET indicates that RMON histories and alarms have been reset because of chipset reboot.

The following new BER alarm conditions have been added:

Condition	Alarm Description	Type
SD-L	BER Threshold exceeded for Signal Degrade	Line
SD-P	BER Threshold exceeded for Signal Degrade	Path
SF-L	BER Threshold exceeded for Signal Failure	Line
SF-P	BER Threshold exceeded for Signal Failure	Path

Changed Conditions

The TOPOLOGY-CHANGE condition has been renamed to the TOP-CHANGE condition.

Related Documentation

- *Cisco ONS 15454 User Documentation*, Release 2.2.0, August 2000
- *Cisco ONS 15454 User Documentation*, Release 2.2.1, October 2000
- *Release Notes for the Cisco ONS 15454*, Release 2.2.0, August 2000
- *Release Notes for the Cisco ONS 15454*, Release 2.2.1, November 2000

Obtaining Documentation

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.cisco.com.

Optical Networking Group CD-ROM

Optical networking-related documentation, including the *Cisco ONS 15454 User Documentation*, is available in a CD-ROM package that ships with your product. The ONG CD-ROM, a member of the Cisco Connection Family, is updated as required. Therefore, it might be more current than printed documentation. To order additional copies of the ONG CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www.europe.cisco.com.

Ordering Documentation

Registered CCO users can order the ONG CD-ROM and other Cisco Product documentation through our online Cisco Marketplace. Select Online Ordering from CCO.

Nonregistered CCO users can order documentation through a local account representative by calling Cisco's corporate headquarters (California, USA) at 408 526-4000 or, in North America, call 800 553-NETS (6387).

Obtaining Technical Assistance

Cisco provides Cisco Connection Online (CCO) as a starting point for all technical assistance. Warranty or maintenance contract customers can use the Technical Assistance Center. All customers can submit technical feedback on Cisco documentation using the web, email, a self-addressed stamped response card included in many printed docs, or by sending mail to Cisco.

Cisco Connection Online

Cisco continues to revolutionize how business is done on the Internet. Cisco Connection Online is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

CCO's broad range of features and services helps customers and partners to streamline business processes and improve productivity. Through CCO, you will find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online support services, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on CCO to obtain additional personalized information and services. Registered users can order products, check on the status of an order and view benefits specific to their relationships with Cisco.

You can access CCO in the following ways:

- WWW: www.cisco.com
- Telnet: cco.cisco.com
- Modem using standard connection rates and the following terminal settings: VT100 emulation; 8 data bits; no parity; and 1 stop bit.
  - From North America, call 408 526-8070
  - From Europe, call 33 1 64 46 40 82

You can e-mail questions about using CCO to cco-team@cisco.com.

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to warranty or maintenance contract customers who need technical assistance with a Cisco product that is under warranty or covered by a maintenance contract.

To display the TAC web site that includes links to technical support information and software upgrades and for requesting TAC support, use www.cisco.com/techsupport.

To contact by e-mail, use one of the following:

Language	E-mail Address
English	tac@cisco.com
Hanzi (Chinese)	chinese-tac@cisco.com
Kanji (Japanese)	japan-tac@cisco.com

Language	E-mail Address
Hangul (Korean)	korea-tac@cisco.com
Spanish	tac@cisco.com
Thai	thai-tac@cisco.com

In North America, TAC can be reached at 877 323-7368. For other telephone numbers and TAC e-mail addresses worldwide, consult the following web site: http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml.

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc.
Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate and value your comments.

This document is to be used in conjunction with the Cisco ONS 15454 User Documentation.