

Upgrading Cisco ONS 15454 Release 2.2.x to 3.0.0 Using the TCC+ Card

Introduction

This document explains how to upgrade Cisco ONS 15454's Cisco Transport Controller (CTC) software from Release 2.2.x to Release 3.0.0 using the Timing, Communications, and Control + (TCC+) card.

Before beginning, write down the following information about your site; the data will be useful during and after the upgrade: Date, Street Address, Site Phone Number, and Dial Up Number.



Caution

Read each procedure before you begin the upgrade.



Caution

This procedure is only supported for Releases 2.2.0 and forward. If you wish to upgrade from a release prior to Release 2.2.0, you must call the Technical Assistance Center (TAC) at 877 323-7368 for assistance.



Caution

Cisco recommends Release 3.0.0 for new system installations (or what is commonly termed "Greenfield applications") only. When you upgrade from ONS 15454 Release 2.2.x to 3.0.0, a condition may arise that can cause a reset of the node at the point after the upgrade process after a provisioning change is performed on the node. During testing, this condition was experienced in less than 2% of the systems upgraded. If the node falls into this condition, traffic may be affected on provisioned circuits. If you choose to upgrade nodes to Release 3.0.0, perform the upgrade within a maintenance window and follow the procedure described in the caution after Step 9 of the ["Activate the New Load" section on page 8](#).



Corporate Headquarters:

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

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

Upgrade Requirements

This section contains critical information that you must read before the upgrade process.

Read the *Release Notes for Cisco ONS 15454 Release 3.0.0* before you begin this upgrade procedure.

CTC Workstation Requirements

Before upgrading the workstation to run CTC Release 3.0.0, verify all PC or UNIX workstation hardware and software requirements.

- A Windows or Unix workstation:
 - IBM-compatible PC with a 486 or higher processor, CD ROM drive, and 128 MB RAM running Windows 95, Windows 98, Windows 2000, or Windows NT
 - UNIX workstation running Solaris
- Browser software (select one):
 - Netscape Navigator 4.73 or higher (Netscape Navigator is included on the ONS 15454 software CD shipped with the node.)
 - Netscape Communicator 4.61 or higher
 - Internet Explorer 4.0 Service Pack 2 or higher
- The Java Policy File and Java Runtime Environment (JRE) file, Release 1.2.2_005 or later (1.3 is included on the ONS 15454 software CD)

**Note**

If you upgrade to JRE 1.3.0, you will no longer be able to log into an ONS 15454 running Release 2.2.1 or prior, or an ONS 15327 running release 1.0.0. If you are later forced to revert to a release that requires a previous version of JRE, you will then have to reinstall Java and delete the jar files from your workstation's system "temp" directory after reverting all of the nodes in the network. If you are currently running a release that is also compatible with JRE 1.3, or if you retain your JRE 1.2.2 installation, this will not be an issue.

IP Address Caveat

Disable all other Ethernet devices (such as a dial-up adapter) on the workstation that runs CTC.

If you have multiple IP addresses on your workstation, you should remove them; you cannot install CTC Release 3.0.0 if multiple IP addresses are configured.

LAN Caveat

If you have multiple ONS 15454 nodes configured in the same IP subnet, only one can be connected to a router. Otherwise, the remaining nodes might be unreachable. Refer to the *Cisco ONS 15454 User Documentation, Release 3.0.0* for LAN-connection suggestions.

Hardware Verification



Note This section applies to OC-48 nodes only.

If you have an OC-48 ring, you must verify the hardware revision on the OC-48 line cards before continuing.

-
- Step 1** From the CTC node view, click the **Inventory** tab.
 - Step 2** Check the hardware revision number of all OC-48 long reach (LR) line cards (OC48 LR 1550).
 - Step 3** If you have OC-48 LR 1550 cards with a 008C hardware revision you need to call the Technical Assistance Center (TAC) at 877 323-7368 and obtain a Return Materials Authorization (RMA) number for these cards.
-

TCC+ Verification



Caution You must be using TCC+, and not TCC cards to upgrade to Release 3.0. If you have any TCC cards installed, you must first upgrade to TCC+ before proceeding with the software upgrade. Refer to the Maintenance chapter of the *Troubleshooting and Reference Guide* for Release 3.0, or to the documentation accompanying your TCC+ cards, for the upgrade procedure.

You must now use CTC to check for duplex common modules.

-
- Step 1** Log into the node.
 - Step 2** Ensure that slots 7, 8, 10, and 11 have cards installed. Release 2.2.x does not support simplex operation.
 - Step 3** Repeat Steps 1 and 2 at every node in the network.
-

Telnet Session

Make sure all active telnet sessions to any node in the network are closed.

AIP Verification

If any of your nodes has an AIP board with the part number 67-11-00015, the board must be replaced. Perform the following steps to ensure that all of your AIP boards are good.

-
- Step 1** Look at the back of your ONS 15454 node and locate the green board with “AIP” stamped into the right hand side (the writing will be sideways as you face the board).
 - Step 2** Locate the sticker with the part number. The number should be preceded by “P/N” on the sticker.



Note

If there is no sticker with a part number, the number may be stamped into the board itself. If you cannot find the part number, you will need to contact the Technical Assistance Center (TAC) at 877 323-7368 for assistance.

- Step 3** If the part number is any other number than 67-11-00015, go to the next node and start from Step 1 again.
- Step 4** If the part number is 67-11-00015, contact the TAC at 877 323-7368 and have the board replaced.
- Step 5** Repeat Steps 1–4 for every node.

Back Up the Database

Before upgrading from Release 2.2.x to Release 3.0.0 software, you must back up the current database for all nodes in the network.

- Step 1** Log into CTC.
- Step 2** From the node view, click the **Maintenance > Database** tabs.
- Step 3** Click **Backup**.
- Step 4** Save the database on the workstation's hard drive or on network storage. Use an appropriate file name with the file extension .db (for example, myDatabase.db).
- Step 5** Click **Save**. A message appears indicating that the backup is complete.
- Step 6** Click **OK**.
- Step 7** Repeat Steps 1–6 for each node in the network.

Cisco recommends that you manually log critical information by either writing it down or printing screens where applicable. This step is optional after you have backed up the database. Use the following table to determine the information you should log; complete the table (or your own version) for every node in the network.

Item	Record data here (if applicable)
IP address of the node	
Node name	
Timing settings	
DCC connections; list all optical ports that have DCCs activated	
User IDs (List all, including at least one super user)	
Inventory; do a print screen from the inventory window	
Active TCC+	Slot 7 or Slot 11 (circle one)

Item	Record data here (if applicable)
Active XC	Slot 8 or Slot 10 (circle one)
Network information; do a print screen from the Provisioning tab in the network view.	
Current configuration: BLSR, linear, etc. (do print screens as needed)	
List all protection groups in the system; do a print screen from the protection group window	
List alarms; do a print screen from the alarm window	
List circuits; do a print screen from the circuit window	

Upgrade the Software

After backing up the database and logging all of the required information, insert the Release 3.0.0 software CD into the workstation (or otherwise acquire access to the software) and begin the upgrade process. You must download and then activate the software.



Caution

A traffic interruption of less than 60 ms on each circuit is possible during the activation, with Ethernet traffic disruption possibly lasting up to several minutes on each circuit.



Caution

Do not perform maintenance or provisioning activities during the activation process.



Note

Starting with the node most directly connected to your workstation will achieve the best download performance; however, in most networks it is usually safer to begin activation at the farthest node and proceed toward the one you are most directly connected to. This ensures that no node will be at risk of being stranded if unforeseen circumstances cause the upgrade to fail. This issue is a matter of network administration policy.

If you are upgrading from Release 2.2.0, you must now run the pftix.exe script (PC) or pftix.pl script (UNIX). If you are upgrading from Release 2.2.1 or greater, go to the [“Download” section on page 6](#).

There are two flash RAMs on the TCC+ card. An upgrade downloads the software to the backup RAM on both the backup and active TCC+ cards. This procedure does not affect traffic because the active software continues to run at the primary RAM location; therefore, you can download the software at any time.

Run the Script

This procedure is only necessary with Release 2.2.0 upgrades. If you are upgrading from Release 2.2.1 or greater, you can skip this procedure and continue with the [“Download” section on page 6](#).


Caution

Do not run the script on more than one node and one workstation at the same time.

Running the script takes approximately 2 to 3 minutes.

- Step 1** Using CTC Release 2.2.0, log into the node from which you will run the script.
- Step 2** Check the ONS 15454 for existing alarms. Resolve any outstanding alarms before proceeding.
- Step 3** From the node view, click the **Maintenance > Software** tabs.
- Step 4** Verify that the active load is 2.2.0 (02.20-001A-00.38).


Note

The script will only work for the Release 2.2.0 (02.20-001A-00.38) load.

- Step 5** Close all active telnet connections to the ONS 15454.
- Step 6** Run the script:
 - In a command window, from the CD software “Cisco15454” directory, run **ptfix.exe** (or **ptfix.pl**, in UNIX) using the IP address of the node you are running the script on.
 - EXAMPLE G:\Cisco15454> **ptfix 172.16.17.18**
 - This step takes approximately 2 to 3 minutes. When the script has completed successfully, an “Upgrade Preparation Complete” message appears.
- Step 7** Close CTC and then reconnect to the node.
- Step 8** From the network view, log into the node you ran the script on.
- Step 9** Click the **Maintenance > Software** tabs.
- Step 10** Verify that the protect software is now “none.”
- Step 11** Return to the network view.
- Step 12** Repeat Steps 1–11 for each node in the network running Release 2.2.0.


Caution

Rerun the script on any node for which the active/standby TCC+ reboots at any time before the Release 3.0.0 load is activated.

Download

- Step 1** Check all nodes in the ring for existing alarms. Resolve any outstanding alarms before proceeding.
- Step 2** After checking and resolving alarms on all nodes, download the software to each node.



Note During the software download process, an alarm, SWFTDWN, indicates that the software download is taking place. This is normal and clears when the download is complete.

- Step 3** From the CTC node view, click the **Maintenance > Software** tabs.
- Step 4** Click **Upgrade**. The File Open dialog box opens.
- Step 5** Browse to locate the software files on the ONS 15454 System Software CD (or on your hard drive, if you are working from a local copy).
- Step 6** Open the “Cisco15454” folder.
- Step 7** Select the file with the “.pkg” extension and click **Open**. CTC displays a status window so you can monitor the download process. A message indicating that your files transferred successfully will appear after the software has finished loading.
- Step 8** Repeat Steps 1–7 for each node.



Note The software download process can take 30 minutes or more per node.

Before You Activate

BLSR Nodes Only

If the node is in a bidirectional line switched ring (BLSR) configuration, you must perform a span lockout at each node before activating the software for Release 3.0.0. Follow this procedure to perform a span lockout on a BLSR using CTC Release 2.2.x.



Note During the lockout, BLSR spans will not be protected. Be sure to remove the lockout after activating all nodes in the ring.



Note To prevent ring or span switching, perform the lockout on both the east and west spans of each node.

- Step 1** Click the **Maintenance > Ring** tabs.
- Step 2** For each of the BLSR trunk cards (OC-12 or OC-48), go to the row in the table for that card and perform the following steps:
- a. Click in the West Operation column to show the pull-down menu.
 - b. From the menu options, choose **Ring Lockout**.
 - c. In the same row, click in the East Operation column to show the pull-down menu.
 - d. From the menu options, choose **Ring Lockout**.
 - e. Click **Apply** to activate the command.
- Step 3** Repeat Step 2 at every node in the BLSR.

Step 4 Leave the BLSR in the lockout state until you have finished activating all nodes.

**Note**

A Default K alarm or alarms on the protect STS timeslots can occur during this lockout period. Ignore these alarms if they occur.

All Nodes

Perform the following steps for all nodes in the network.

Step 1 Make sure all cards that are part of a protection group (1:1 and 1:N) are active on the working card of that protection group and that no protection switches are occurring. In other words, make sure protect cards are in standby before proceeding.

Step 2 To ensure database synchronization, run the memAudit utility:

- a. Close all active telnet connections to the ONS 15454.
- b. Copy the memAudit.exe from the ONS 15454 software CD or the following Cisco.com web page to a folder on your hard drive:

<http://www.cisco.com/cgi-bin/tablebuild.pl/ons15454>

- c. In a command window, change the prompt to the folder where the memAudit.exe is located.
- d. At the prompt, type the following command:

```
memAudit <nodename or IP address>
```

**Note**

Optional parameters exist for the memAudit command. For more information about the memAudit utility, view the memAudit_readme.htm file on the CD or Cisco.com web page.

Activate the New Load

Log into and activate each node in the network.

**Note**

Upon activation, you may receive a series of Java exception errors. Please disregard these messages as they are due to the changes instituted in the Java code base for 3.0.0 that 2.2.x is unable to interpret. The Java exceptions have no adverse effect.

Step 1 Log into a node.

Step 2 Record the IP address of that node.

Step 3 Verify that the node has no new alarms. If alarms exist, clear them before proceeding.

Step 4 From the CTC node view, click the **Maintenance > Software** tabs.

Step 5 Verify that the protect version is 3.0.0.

Step 6 Click **Activate**. The **Activate** dialog box appears with a warning message.

Step 7 Click **Yes** to proceed with the activation. The “Activation Successful” message appears upon successful completion of the activation.

Step 8 Click **OK** to begin the node rebooting process.

Step 9 After activating the node, wait until the software upgrade finishes at that node before continuing.

Each card in the node will reboot, beginning with the standby TCC+. Once the standby TCC+ is fully activated and fully rebooted, it becomes the active TCC+ and the other TCC+ reboots. When the TCC+s are finished, the standby XC/XCVT reboots and becomes active, and then the other XC/XCVT reboots. Next, the Ethernet cards reset all at once, then the line cards boot consecutively from left to right. The whole process can take up to 30 minutes, depending on how many cards are installed. This process is service affecting, so Cisco recommends that you activate the new load during a maintenance window. TDM traffic can endure a hit of up to 50 ms. Expect Ethernet traffic to remain down from the time the TCC+s switch to the time all Ethernet cards have finished resetting. Once all the cards finish rebooting and all alarms clear you can safely proceed to the next step. (If you are upgrading remotely and cannot see the nodes, wait for 30 minutes for the process to complete, then check to ensure all alarms have cleared before proceeding.)



Caution

When you upgrade from ONS 15454 Release 2.2.x to 3.0.0, a condition may arise during activation that can cause a reset of the node at the point after the upgrade process after a provisioning change is performed on the node. If a card fails to load the new software successfully, you may see a communication failure (CONTBUS) condition that persists after the activation is completed indicating the node has entered this state. Once the node is in this state, provisioning changes can cause the node to go into a system-wide reset wherein all cards (except for the card that failed to reset originally) will perform a soft reboot and reload the new software image. If the node falls into this condition, traffic may be affected on provisioned circuits.

If you see a CONTBUS alarm that does not clear after the upgrade is complete, manually reseal the card that generated the alarm.

To ensure that your upgrade activation has succeeded, Cisco recommends that you execute a provisioning change to the node as follows:

- a) In the node view, click the **Provisioning > Timing** tabs.
- b) In the Reference Lists pane, change one of the NE References and click **Apply**.
- c) Wait one minute, then change the same NE Reference back again, and click **Apply**.

If the problem exists, a 30 minute timer will be set in motion allowing the node reset to occur during the maintenance window, or while personnel are onsite. Look for a SYSBOOT alarm in the alarms panel for the node. If the node does not reset 30 minutes after the provisioning change and there is no SYSBOOT alarm present in the CTC alarms panel for the node, the software activation was successful.



Note

Steps 10–12 are only necessary after upgrading the first node. For the remaining nodes, you will still be disconnected and removed to the network view during the node reboot, but after the reboot is complete, CTC will restore connectivity to the node.

Step 10 In CTC, choose **File > Exit**.

Step 11 In your browser window, click “Delete CTC Cache.”

- Step 12** Reconnect to CTC using the IP address from Step 2 (if the IP address is still in the browser location bar you can simply hold down the shift key and click the browser Reload/Refresh button). The new CTC applet for Release 3.0.0 now uploads. Because CTC 3.0.0 is backwardly compatible with CTC Release 2.2.x, it affords you network visibility while you are upgrading.



Note Only activate one node at a time.

- Step 13** Log into each of the remaining nodes and perform the following procedures, one node at time. Each of these procedures must be performed for every node that has TCC+ cards and is running software Release 2.2.x. Allow each node to finish (all alarms cleared for 10 minutes) before activating the next node:

- [All Nodes, page 8](#)
- [Activate the New Load, page 8](#)

BLSR Nodes

Release the span lockouts on all BLSR nodes after the new software load is activated on all nodes. The following procedure restores a BLSR using Release 3.0.0.

- Step 1** In CTC node view, click the **Maintenance > Ring** tabs.
- Step 2** For each of the BLSR trunk cards (OC-12 or OC-48), go to the row in the table for that card and perform the following steps:
- a. Click in the West Switch column to show the pull-down menu.
 - b. From the menu options, choose **Clear**.
 - c. Click **Apply** to activate the command.



Note When removing a lockout, be sure to apply your changes after each selection of the Clear option. If you try to select Clear for more than one lockout at a time, you risk traffic loss on the first ring switch.

- d. In the same row, click in the East Switch column to show the pull-down menu.
 - e. From the menu options, choose **Clear**.
 - f. Click **Apply** to activate the command.
- Step 3** You might need to accept a new ring map to clear Default K byte or Node ID mismatch alarms. From the **Provisioning > Ring** tabs, click the **Ring Map** button. If a new ring map exists, click **Accept**.

Date/Time Setting

If you are not using SNTP, the upgrade procedure can cause the Date/Time setting to change.

- Step 1** In CTC node view, click the **Provisioning > General** tabs.
- Step 2** Set the correct date and time, then click **Apply**.

Step 3 Repeat Steps 1 and 2 for each remaining node.

Spare TCC+ Units

All spare TCC+ units should be upgraded to CTC Release 3.0.0.

To upgrade a spare TCC+, place it in the standby slot of a node running Release 3.0.0. The card will upgrade automatically from the active TCC+.

XC to XCVT Card Upgrade

If you need to upgrade your XC cards to XCVT, please refer to the user documentation for the software you are currently running.

Revert to Previous Load

Before upgrading from Release 2.2.x to Release 3.0.0 software, you must back up the current database at all nodes in the network (this is part of the [“Back Up the Database”](#) section on page 4). Cisco recommends that you record or export all critical information to your hard drive. If you need to revert to the backup database, use the following procedures.

BLSR Lockout

If you have a BLSR provisioned, before beginning the revert you must perform a span lockout at each node. Follow this procedure to perform a span lockout on a BLSR using CTC Release 3.0.0.



Note

During the lockout, BLSR spans will not be protected. Be sure to remove the lockout after activating all nodes in the ring.



Note

To prevent ring or span switching, perform the lockout on both the east and west spans of each node.

Step 1 Click the **Maintenance > Ring** tabs.

Step 2 For each of the BLSR trunk cards (OC-12 or OC48), go to the row in the table for that card and perform the following steps:

- a. Click the **East Switch** column to show the pull-down menu.
- b. From the menu options, choose **Span Lockout**.
- c. Click **West Switch** column to show the pull-down menu.
- d. From the menu options, choose **Span Lockout**.

e. Click **Apply** to activate the command.

Step 3 Repeat Step 2 at each node in the ring.

Step 4 Leave the BLSR in the lockout state until you have finished reverting all nodes.



Note A Default K alarm or alarms on the protect STS timeslots can occur during this lockout period. Ignore these alarms if they occur.

Revert to Protect Load



Note To perform a supported (non service-affecting) revert from Release 3.0, the release you wish to revert to must have been working at the time you activated to Release 3.0 on that node. Also, a supported revert automatically restores the node configuration to its state at the time of the previous activation. Thus, any configuration changes made after activation will be lost when you revert the software.



Note In the following procedure, the database is restored automatically as a part of the revert only for Releases 2.2.1 and later. If you were running Release 2.2.0 before activation, you will need to manually restore the database after performing the steps to revert. A manual database restoration is traffic affecting and should be performed during a service window.

Step 1 From the node view, click the **Maintenance > Software** tabs.

Step 2 Verify that the protect software displays 2.2.x (the release you upgraded from).

Step 3 Click **Revert**. Revert activates the protect software and restores the database from the previous load (except as noted). A dialog box asks you to confirm the choice.

Step 4 Click **OK**. This begins the revert and drops the connection to the node.

Step 5 After reverting the node, wait until the software revert finishes at that node before continuing.



Note Be patient. The system reboot might take up to 30 minutes to complete.

Step 6 Shut down your Netscape or Internet Explorer browser.

Step 7 Wait one minute before restoring another node.



Note If you upgraded to JRE 1.3.0, you cannot log into an ONS 15454 running Release 2.2.1 or prior (or an ONS 15327 running Release 1.0.0). If you are reverting to a release that required a previous version of JRE, you will need to reinstall Java and delete the jar files from your workstation's system "temp" directory after reverting all of the nodes in the network. If you are reverting to a release that also uses JRE 1.3, or if you retained your older version of JRE during the upgrade, this will not be an issue.

- Step 8** After reverting all of the nodes in the network, restart the browser and log back into the last node that was reverted. This uploads the appropriate CTC applet for Release 2.2.x to your workstation.

Manually Restore the Database

If you were upgrading from Release 2.2.0, or in certain other cases, it might be necessary to restore the pre-upgrade database manually.



Caution

Do not perform these steps unless you are restoring Release 2.2.0 or the software revert for a later release failed.



Caution

This process is traffic affecting and should be performed during a service window.

- Step 1** From the CTC node view, click the **Maintenance > Database** tabs.
- Step 2** Click **Backup**. The “Open...” dialog box appears.
- Step 3** Select the previously-saved file and choose **Open**.
The database will be restored and the TCC+s will reboot.
- Step 4** Once the TCC+s have rebooted, log back into CTC and verify that the database is restored.
Wait one minute before restoring the next node.

BLSR Lockout Removal

To restore BLSR protection you must clear the span lockouts on all BLSR nodes after reverting the software load and restoring the database on all nodes. Use the following procedure to restore a BLSR using Release 2.2.x.

- Step 1** In CTC node view, click the **Maintenance > Ring** tabs.
- Step 2** For each of the BLSR trunk cards (OC-12 or OC-48), go to the row in the table for that card and perform the following steps:
- a. Click the West Switch column to show the pull-down menu.
 - b. From the menu options, choose **Clear**.
 - c. Click **Apply** to activate the command.



Note

When removing a lockout, be sure to apply your changes after each selection of the Clear option. If you try to select Clear for more than one lockout at a time, you risk traffic loss on the first ring switch.

- d. In the same row, click in the East Switch column to show the pull-down menu.
- e. From the menu options, choose **Clear**.

f. Click **Apply** to activate the command.

Step 3 You might need to accept a new ring map to clear Default K byte or Node ID mismatch alarms. From the **Provisioning > Ring** tabs, click the **Ring Map** button. If a new ring map exists, click **Accept**.

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, iQ Net Readiness Scorecard, Networking Academy, and ScriptShare are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site 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. (0303R)

Copyright © 2003, Cisco Systems, Inc.
All rights reserved.