Upgrading Cisco ONS 15454 Release 3.0.x to 3.0.2 Using the TCC+ Card

Introduction

This document explains how to upgrade Cisco ONS 15454's Cisco Transport Controller (CTC) software from Release 3.0.x to Release 3.0.2 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 Release 3.0.x. If you wish to upgrade from Releases 2.2.0 – 2.2.2, use the procedures in *Upgrading Cisco ONS 15454 Release 2.2.x to 3.0.2 Using the TCC+ Card*. 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.

Note Procedures in this document are to be performed in consecutive order unless otherwise noted. In general, you are not done with a procedure until you have completed it for each node you are upgrading, and you are not done with the upgrade until you have completed each procedure that applies to your network. If you are new to upgrading the ONS 15454, you may wish to check off each procedure on your printed copy of this document as you complete it.

CISCO SYSTEMS

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

Upgrade Requirements

This section contains critical information and procedures that you must read and complete before beginning the upgrade process.

Read the *Release Notes for Cisco ONS 15454 Release 3.0.2* before you begin this upgrade procedure.

CTC Workstation Requirements

Before upgrading the workstation to run CTC Release 3.0.2, verify all PC or UNIX workstation hardware and software requirements.

- A Windows or Unix workstation:
  - IBM-compatible PC with a Pentium 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 must later revert to a release that requires a previous version of the JRE, you will have to reinstall Java and delete the jar files from your workstation's user "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, the extra steps are not necessary.

Once you have verified that your workstation meets CTC Release 3.0.2 requirements, proceed to the IP Address Check.

IP Address Check

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 3.0.2 if multiple IP addresses are configured.

You have completed the IP address check procedure. Now perform the LAN Check.

LAN Check

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 Installation and Operations Guide, Release 3.0* for LAN-connection suggestions.

After verifying that your LAN is properly configured, proceed to the Verification of Duplex Common Control Cards procedure.

Verification of Duplex Common Control Cards

You must now use CTC to check for duplex common control cards. The node must have two TCC+ cards and two cross-connect cards (two XCs, two XCVTs, or two XC10Gs).

Step 1 Log into the node.

Step 2 Ensure that Slots 7, 8, 10, and 11 have cards installed. Release 3.0.x does not support simplex operation.

Step 3 Repeat Steps 1 and 2 at every node in the network.

You have completed the verification of duplex common control cards. Proceed to the Telnet Session Check.

Telnet Session Check

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

When you have ensured that there are no open telnet sessions to any node, proceed to the AIP Verification.

AIP Verification

If any of your nodes has an AIP board with the part number 67-11-00015 or 67-11-00002, 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 must contact the Technical Assistance Center (TAC) at 877 323-7368 for assistance.

Step 3 If the part number is any number other 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 or 67-11-00002, contact the TAC at 877 323-7368 to request a Return Materials Authorization (RMA).

Step 5 Repeat Steps 1 – 4 for every node.

You have completed the AIP verification. Before you upgrade your CTC software you must now back up the database for each node you will upgrade. Proceed to the Back Up the Database procedure.

Back Up the Database

Before upgrading from Release 3.0.x to Release 3.0.2 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)
Active XC	Slot 8 or Slot 10 (circle one)
Network information; do a print screen from the Provisioning tab in the network view.	

Item	Record data here (if applicable)
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	

Once you have backed up all databases and recorded all necessary information using the checklist, you can begin the Upgrade the Software procedure.

Upgrade the Software

To upgrade your CTC software, read and follow all directions in this section.

Insert the Release 3.0.2 software CD into the workstation CD-ROM (or otherwise acquire access to the software) to begin the upgrade process.

Note Inserting the software CD activates the CTC Setup Wizard. You can use the setup wizard to install components or click **Cancel** to continue with the upgrade.

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

Caution Do not perform maintenance or provisioning activities during the activation procedure.

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.

The software upgrade consists of the following procedures:

1. Download, page 6 (all nodes)
2. Before You Activate, page 7 (BLSR nodes only)
3. Activate the New Load, page 8 (all nodes)
4. Delete Cached Jar Files, page 9 (as needed—see the note following Step 11 of the "Activate the New Load" section on page 8)

5. BLSR Lockout Removal, page 10 (BLSR nodes only)
6. Date/Time Setting, page 11 (any nodes not using SNTP)
7. Spare TCC+ Units, page 11 (as needed for upgrading spare TCC+ cards)

To upgrade the software successfully, you must read and perform each of the procedures that applies to your network in the proper order. Begin with the Download, page 6.

Download

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. The download 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.

Step 1 Check all nodes in the ring for existing alarms. Resolve any outstanding alarms before proceeding.

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

Step 2 From the CTC node view, click the **Maintenance > Software** tabs.

Step 3 Click **Download**. The Download Selection dialog box opens.

Step 4 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 5 Open the "Cisco15454" folder.

Step 6 Select the file with the ".pkg" extension and click **Open**.

Step 7 In the list of compatible nodes, select the checkboxes for all nodes you are downloading the software to.

Note Cisco advises that you limit concurrent software downloads to 3 nodes at once.

Step 8 Click **OK**. The Download Status column monitors the progress of the download.

Caution Do not close CTC during the download. Closing CTC will abort the download process.

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

Once you have successfully downloaded the CTC Release 3.0.2 software to each node you are upgrading, perform the "Before You Activate" section on page 7.

Before You Activate

BLSR Nodes Only

If any node you are upgrading is in a bidirectional line switched ring (BLSR) configuration, you must perform a span lockout at each node in the ring before activating the software for Release 3.0.2. Follow this procedure to perform a span lockout on a BLSR using CTC Release 3.0.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 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.

Note Ignore any Default K alarm or alarms that occur on the protect STS timeslots during this lockout period.

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

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 using the following procedure.

Note Cisco recommends that the first node you activate be a LAN-connected node. This ensures that the new CTC jar files will download to your workstation as quickly as possible.

Note 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 that the protect cards are in standby before proceeding.

Step 1 Log into a node.

Step 2 Verify that the node has no new alarms. If alarms exist, clear them before proceeding.

Step 3 From the CTC node view, click the **Maintenance > Software** tabs.

Step 4 Verify that the protect version is 3.0.2.

Step 5 Click **Activate**. The **Activate** dialog box appears with a warning message.

Step 6 Click **Yes** to proceed with the activation. The "Activation Successful" message appears when the software is successfully activated.

Step 7 Click **OK** to begin the node rebooting process.

Step 8 After activating the node, wait until the software upgrade reboot finishes at that node before continuing. A system reboot (SYSBOOT) alarm is raised while activation is in progress. Once all cards have reset, this alarm clears.

Each card in the node reboots, 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 XC/XCVT in Slot 8 reboots, and then the XC/XCVT in Slot 10 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.)

Note Steps 10 to 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 9 In CTC, choose **File > Exit**.

Step 10 In your browser window, click "Delete CTC Cache."

Note It might also be necessary to delete cache files from your browser's directory, or from the "temp" directory on your MS Windows workstation. If you have trouble reconnecting to CTC, refer the "Delete Cached Jar Files" section on page 9.

Step 11 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 3.0.2 uploads. Because CTC Release 3.0.2 is backwardly compatible with CTC Release 3.0.x, it affords you network visibility while you are upgrading.

Note Only activate one node at a time.

Step 12 Log into each of the remaining nodes and perform the procedure to Activate the New Load, page 8. The activation must be performed for every node that is running software Release 3.0.x. Allow each node to finish (all alarms cleared for 10 minutes) before activating the next node.

You have completed the activation procedure when you have activated all nodes with the Release 3.0.2 software.

If you performed a BLSR lockout before you began activation, you must now perform the procedure for BLSR Lockout Removal, page 10. Otherwise, go to the procedure for Date/Time Setting, page 11.

Delete Cached Jar Files

When you upgrade or revert to a different CTC software load, you must reload CTC to your browser. In most cases, you can do this by simply clicking "Delete CTC Cache" in your browser window; however, in some circumstances, you may need to delete cache files from your browser's directory, or from the "temp" directory on your MS Windows workstation. If you have trouble reconnecting to CTC after upgrading or reverting, follow the procedures below.

Step 1 Delete cache files from your browser directory.

In Netscape:

a. Choose **Edit > Preferences > Advanced > Cache**.

b. Click **Clear Memory Cache**.

c. Click **OK**.

d. Click **Clear Disk Cache**.

e. Click **OK** twice.

In Microsoft Internet Explorer:

a. Choose **Tools > Internet Options > General**.

b. Choose **Delete Files**.

c. Select the **Delete all offline content** checkbox.

d. Click **OK** twice.

Step 2 Close your browser.

Step 3 Delete cached files from your workstation (Windows systems only).

a. In your Windows start menu, choose **Settings > Control Panel > System > Advanced**.

b. Click **Environment Variables**. This will show you a list of user variables and a list of system variables.

c. In the list of user variables, look for the variable "TEMP." The value associated with this variable is the path to your temporary directory where jar files are stored.

d. Open the "TEMP" directory located in the path you just looked up.

e. Select **View > Details**.

f. Select and delete all files with "jar" in either the name or type field.

Step 4 Reopen your browser. You should now be able to connect to CTC.

After deleting cached jar files, you should return to the referring procedure, either procedure Activate the New Load, page 8, or Revert to Protect Load, page 12, and continue with the steps there.

BLSR Lockout Removal

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 3.0.2.

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 time you choose 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**.

When all BLSR span lockouts are released, you have completed this procedure and should go to the procedure for Date/Time Setting.

Date/Time Setting

If you are using SNTP, you do not need this procedure and can go to the procedure for upgrading Spare TCC+ Units, page 11.

If you are not using SNTP, the upgrade procedure can cause the Date/Time setting to change. Follow this procedure to reset the date and time at each node.

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.

When all nodes have the correct date and time settings, go to the procedure for upgrading Spare TCC+ Units, page 11.

Spare TCC+ Units

All spare TCC+ units should be upgraded to CTC Release 3.0.2.

To upgrade a spare TCC+, place it in the standby slot of a node running Release 3.0.2. The card will upgrade automatically from the active TCC+.

Note This procedure could take up to 30 minutes per TCC+ card. During this time, the LEDs on the upgrading card will flash alternately between “fail” and “standby.”

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 (this procedure can be performed before or after the upgrade).

Revert to Previous Load

Before you upgraded from Release 3.0.x to Release 3.0.2 software, you should have backed up the existing 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, in order.

BLSR Lockout

If you have a BLSR provisioned, before beginning the revert you must perform a span lockout at each node. Follow the procedure in the "Before You Activate" section on page 7 to perform a span lockout on a BLSR using CTC Release 3.0.2.

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

Once you have performed the BLSR lockout on all BLSR nodes, perform the procedure to Revert to Protect Load, page 12.

Revert to Protect Load

Note To perform a supported (non service-affecting) revert from Release 3.0.2, the release you wish to revert to must have been working at the time you activated to Release 3.0.2 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.

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

Step 2 Verify that the protect software displays 3.0.x (the release you upgraded from).

Step 3 Click **Revert**. Revert activates the protect software and restores the database from the previous load. 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 3.0.x to your workstation.

Note It might also be necessary to delete cache files from your browser's directory, or from the "temp" directory on your MS Windows workstation. If you have trouble reconnecting to CTC, see the procedure Delete Cached Jar Files, page 9.

After reverting all nodes, remove any BLSR lockout using the procedure for BLSR Lockout Removal.

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. Follow the procedure in the "BLSR Lockout Removal" section on page 10 to restore a BLSR using Release 3.0.x.

You have now completed the software revert procedure. All nodes should be provisioned as they were before the last activation; however, in case of trouble, Cisco provides the following Manually Restore the Database procedure to retrieve your databases.

Manually Restore the Database

The revert procedure should have restored your Release 3.0.x database completely; however, as a precaution, Cisco includes here the steps to restore the pre-upgrade database manually.

Caution Do not perform these steps unless the software revert failed.

Caution This process is service 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.

This document is to be used in conjunction with the *Release Notes for Cisco ONS 15454 Release 3.0.2* publication.