Upgrading the Cisco ONS 15454 to Release 6.2

This document explains how to upgrade Cisco ONS 15454 Cisco Transport Controller (CTC) software from Release 4.x, 5.x, or 6.0.x to Release 6.2 using the Advanced Timing, Communications, and Control (TCC2) or Advanced Timing, Communications, and Control Plus (TCC2P) card.

Note The TCC2P card is an enhanced version of the TCC2 card. The primary enhancements are Ethernet security features and 64K composite clock BITS timing.

Contents

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

Before You Begin

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

Caution Read all procedures before you begin the upgrade.

Caution This upgrade is supported only for Software Releases 4.0.x, 4.1.x, 4.5, 4.6.x, 4.7, 5.x, and 6.0.x. If you wish to upgrade from an earlier software release, you must contact Cisco Technical Assistance Center (Cisco TAC). For more information, see the "Obtaining Technical Assistance" section on page 31.

Note Release 6.2 supports parallel upgrades for multiple nodes in a network. In a parallel upgrade you can still only activate one node at a time; however, you can begin activation of the next node as soon as the controller cards for the current node have rebooted successfully (or five minutes after the onset of activation, if you do not have visibility to the node).

Note Release 4.x nodes must already be running TCC2 or TCC2P cards prior to the upgrade. If your Release 4.x nodes are running TCC+ cards, you must first upgrade to TCC2 or TCC2P cards. Uploading the Release 6.2 software to a TCC+ will cause a reboot. See the "NTP-U131 Upgrade the TCC+ Card to the TCC2/TCC2P Card" procedure on page 22 for more information.

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

Note LDCC is not supported in Release 6.2. A BLSR running LDCC in Release 4.6.x must be converted to SDCC prior to upgrading to Release 6.2

Errorless Upgrades and Exceptions

The following tables, organized by cross-connect card type, define where errorless upgrades are expected for Release 6.2 and where exceptions can occur. Please review the table for your particular cross-connect card type.

Note Upgrades from releases prior to 4.6 are not expected to be errorless.

Note Upgrades for DWDM configurations are expected to be errorless.

Note On nodes with DS3/EC1-48 cards, where port line buildouts are set to long (for use with 900 ft cables), a software upgrade from Release 5.0 or maintenance Release 5.0.2 to any release after 5.0.2 can result in traffic hits up to 50 ms on the ports set to long line buildout. The length of the hit depends on the operative slot, port, actual cable length, UBIC type, and cable type. This issue cannot be resolved for upgrades from the two affected releases. No other release has this issue.

Note To preserve OSC connections while upgrading a network to Release 6.2, ensure that the upgrade is conducted in the following manner:

- For a linear configuration with a single GNE, activate the node furthest from the GNE first, repeating this rule until all nodes including the GNE are activated.
- For a ring configuration with a single GNE, activate the node half way around the ring from the GNE first, then proceed with each remaining ring section as though for a linear configuration (furthest node first).

XC-VXC-10G

This table applies to nodes equipped with XC-VXC-10G cards.

Table 1 XC-VXC-10G

Card Type	Expected Traffic Effect
E1	Errorless
E3	Errorless
E1-42	Errorless
DS3I	Errorless
STMn	Errorless
MRC-12	Errorless
E-Series Ethernet	Traffic hits up to 5 minutes (approximately)
ML-series Ethernet	Traffic hits 3–8 minutes (approximately)
CE-Series Ethernet	Errorless
G-series Ethernet	Errorless

XC10G

This table applies to nodes equipped with XC10G cards.

Table 2 XC10G

Card Type	Expected Traffic Effect
DS-1	Errorless
DS-3	Errorless
DS3E	Errorless

Table 2 XC10G

Card Type	Expected Traffic Effect
DS3XM	Errorless
EC-1	Errorless
OC-N	Errorless
E-Series Ethernet	Traffic hits up to 5 minutes (approximately)
ML-Series Ethernet	Traffic hits 3–8 minutes (approximately)
CE-Series Ethernet	Errorless
G-Series Ethernet	Errorless

XCVT

This table applies to nodes equipped with XCVT cards. (Errorless upgrade is not guaranteed in this case.)

Table 3 XCVT

Card Type	Expected Traffic Effect
DS-1	Traffic hits < 60ms (hitless)
DS-3	Traffic hits < 60ms (hitless)
DS3E	Traffic hits < 60ms (hitless)
DS3XM	Traffic hits < 60ms (hitless)
EC-1	Traffic hits < 60ms (hitless)
OC-N	Traffic hits < 60ms (hitless)
E-Series Ethernet	Traffic hits up to 5 minutes (approximately)
ML-Series Ethernet	Traffic hits 3–8 minutes (approximately)
CE-Series Ethernet	Traffic hits < 60ms (hitless)
G-Series Ethernet	Traffic hits < 60ms (hitless)

Document Procedures

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 might want to check off each procedure on your printed copy of this document as you complete it.

Each non-trouble procedure (NTP) is a list of steps designed to accomplish a specific procedure. Follow the steps until the procedure is complete. If you need more detailed instructions, refer to the detail-level procedure (DLP) specified in the procedure steps. Throughout this guide, NTPs are referred to as “procedures” and DLPs are termed “tasks.” Every reference to a procedure includes its NTP number, and every reference to a task includes its DLP number.

The DLP (task) supplies additional task details to support the NTP. The DLP lists numbered steps that lead you through completion of a task. Some steps require that equipment indications be checked for verification. When the proper response is not obtained, a trouble clearing reference is provided. This section lists the document procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. NTP-U127 Prepare for Upgrade to Release 6.2, page 5—This section contains critical information and tasks that you must read and complete before beginning the upgrade process.
2. NTP-U128 Back Up the Software Database, page 8—Complete the database backup to ensure that you have preserved your node and network provisioning in the event that you need to restore them.
3. NTP-U129 Upgrade to Release 6.2, page 9—You must complete this entire procedure before the upgrade is finished.
4. NTP-U103 Install Public-Key Security Certificate, page 18—You must complete this procedure to be able to run ONS 15454 Software R6.2.
5. NTP-U130 Revert to Previous Software Load and Database, page 19—Complete this procedure only if you need to return to the software load you were running before activating the Release 6.2 software.
6. NTP-U131 Upgrade the TCC+ Card to the TCC2/TCC2P Card, page 22—Complete this procedure only if you currently have the TCC+ card installed.
7. NTP-U132 Upgrade to Release 6.2 Using TL1, page 24—Complete this procedure only if you want to upgrade to Software R6.2 using TL1.

NTP-U127 Prepare for Upgrade to Release 6.2

Purpose	This procedure provides the critical information checks and tasks you must complete before beginning an upgrade.
Tools/Equipment	ONS 15454s to upgrade PC or UNIX workstation Cisco ONS 15454 Release 6.2 software
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 Read the *Release Notes for Cisco ONS 15454 Release 6.2*.

Step 2 Log into the node that you will upgrade. For detailed instructions, refer to the *Cisco ONS 15454 Procedure Guide* or the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Step 3 Complete the "DLP-U199 Verify CTC Workstation Requirements" task on page 6.

Step 4 If you have multiple ONS 15454 nodes configured in the same IP subnet, ensure that only one is connected to a router. Otherwise, the remaining nodes might be unreachable. Refer to the *Cisco ONS 15454 Reference Manual* or the *Cisco ONS 15454 DWDM Installation and Operations Guide* for LAN-connection suggestions.

Step 5 Complete the "DLP-U200 Verify Common Control Cards" task on page 7.

Step 6 When you have completed the tasks for this section, proceed with the "NTP-U128 Back Up the Software Database" procedure on page 8.

Stop. You have completed this procedure.

DLP-U199 Verify CTC Workstation Requirements

Purpose	This task verifies all PC or UNIX workstation hardware and software requirements. Perform this task before upgrading the workstation to run CTC Software R6.2.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of the workstation)
Security Level	Superuser

Step 1 Ensure that your workstation is either one of the following:

- IBM-compatible PC with a Pentium III/700 or faster processor, CD-ROM drive, a minimum of 384 MB RAM and 190 MB of available hard drive space, running Windows 98, Windows NT 4.0 (with Service Pack 6a), Windows 2000 Professional (with Service Pack 3), or Windows XP Professional (with Service Pack 1)
- UNIX workstation with Solaris Versions 8 or 9, on an UltraSPARC or faster processor, with a minimum of 384 MB RAM and a minimum of 190 MB of available hard drive space

Step 2 Ensure that your web browser software is one of the following:

- Netscape Navigator 7.x or higher
- Internet Explorer 6.x or higher

Note Cisco recommends you use either Internet Explorer 6.x or Netscape 7.x for Windows workstations running Release 6.2. However, if you upgrade to Netscape 7 or JRE 1.4.2 and you still need to launch CTC directly from nodes running software prior to Release 4.6, you must first run the pre-caching utility supplied in the setup program on the software CD. Run the pre-caching utility during the activation (Step 13) in this case.

Step 3 Verify that the Java Version installed on your computer is:

– Java Runtime Environment (JRE) 1.4.2, and Java Plug-in 1.4.2

Tip You can check the JRE version in your browser window after entering the node IP address in the URL window under Java Version.

- The Java Policy file is installed on your computer.

Note For important information on CTC backward compatibility affected by your choice of JRE versions, see the Readme.txt or Readme.html file on the software CD.

Note To install JRE 1.4.2, the Java Policy file, or the Release 6.2 online help, refer to the installation instructions in the *Cisco ONS 15454 Procedure Guide* or the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Step 4 Return to your originating procedure (NTP).

DLP-U200 Verify Common Control Cards

Purpose	This task verifies that two TCC2 or TCC2P cards, and two XC-VXC-10G, XC10G, or XCVT cards (SONET/SDH only) are installed at each node, as appropriate for your network configuration.
Tools/Equipment	PC or UNIX workstation with CTC installed
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of the workstation)
Security Level	Superuser

Note The TCC2P card is an enhanced version of the TCC2 card. The primary enhancements are Ethernet security features and 64K composite clock BITS timing.

Note Release 4.x nodes must already be running TCC2 or TCC2P cards prior to the upgrade. If your Release 4.x nodes are running TCC+ cards, you must first upgrade to TCC2 or TCC2P cards. See the "NTP-U131 Upgrade the TCC+ Card to the TCC2/TCC2P Card" procedure on page 22 for more information.

Note Dense wavelength division multiplexing (DWDM) nodes need only TCC2/TCC2P cards installed during the upgrade.

Step 1 Ensure that the cards are installed. The TCC2 or TCC2P cards are in Slots 7 and 11 and the XC-VXC-10G, XC10G, or XCVT cards (as needed for SONET or SDH operation) are in Slots 8 and 10. Software R6.2 does not support simplex operation.

Step 2 Repeat Step 1 at every node in the network.

Step 3 Return to your originating procedure (NTP).

NTP-U128 Back Up the Software Database

Purpose	This procedure preserves all configuration data for your network before performing the upgrade.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-U127 Prepare for Upgrade to Release 6.2, page 5
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of the workstation)
Security Level	Maintenance user or higher

Step 1 Log into CTC. For detailed instructions, refer to the *Cisco ONS 15454 Procedure Guide* or the *Cisco ONS 15454 DWDM Installation and Operations Guide.* If you are already logged in, continue with Step 2.

Step 2 In the node (default) 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. (We recommend that you use the IP address of the node and the date, for example 1010120192061103.db.)

Step 5 Click **Save**. A message appears indicating that the backup is complete.

Step 6 Click **OK**.

Step 7 Repeat Steps 1 through 6 for each node in the network.

Step 8 (Optional) Cisco recommends that you manually log critical information by either writing it down or printing screens where applicable. Use the following table to determine the information you should log; complete the table (or your own version) for every node in the network.

Note When upgrading from Release 4.0.x alarm and audit logs will be deleted due to changes in the alarm log structure.

Table 4 Manually Recorded Data

Item	Record Data Here (If Applicable)
IP address of the node.	
Node name.	
Timing settings.	
DCC[1] connections; list all optical ports that have DCCs activated.	
User IDs; list all, including at least one Superuser.	
Inventory; do a print screen from the Inventory window.	
Active TCC2/TCC2P.	Slot 7 or Slot 11 (circle one)
Active XC-VXC-10G, XC10G, or XCVT (as needed for SONET or SDH configurations).	Slot 8 or Slot 10 (circle one)
Network information; do a print screen from the Provisioning tab in the network view.	

Table 4 Manually Recorded Data (Continued)

Item	Record Data Here (If Applicable)
Current configuration (BLSR[2], 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.	

1. DCC = data communications channel
2. BLSR = bidirectional line switch ring

Stop. You have completed this procedure.

NTP-U129 Upgrade to Release 6.2

Purpose	This procedure upgrades your CTC software to Software R6.2.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-U128 Back Up the Software Database, page 8
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of the workstation)
Security Level	Superuser

Caution When managing end-to-end circuits participating in an ML-series RPR ring across multiple nodes involved in a parallel upgrade, all nodes participating in these circuits must have completed the activation before the end-to-end traffic will resume.

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

Step 1 Insert the Release 6.2 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.

Step 2 Complete the "DLP-U201 Download Release 6.2 Software" task on page 10 for all nodes, or groups of nodes you are upgrading.

Step 3 Complete the "DLP-U202 Perform a BLSR Lockout" task on page 12 (BLSR nodes only).

Step 4 Complete the "DLP-U203 Activate the New Load" task on page 13 for all nodes you are upgrading.

Note You can only activate one node at a time; however, you can begin activation of the next node as soon as the controller cards for the current node have rebooted successfully.

Step 5 If necessary, complete the "DLP-U102 Delete Cached JAR Files" task on page 16.

Step 6 (Optional) If you wish to ensure that a software revert to the previous software release will no longer be possible, complete the "DLP-U201 Download Release 6.2 Software" task on page 10 for all nodes, or groups of nodes you are upgrading a second time.

Step 7 Complete the "DLP-U204 Remove the BLSR Lockout" task on page 17 for all BLSR nodes in the network.

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

Step 8 Complete the "DLP-U66 Set the Date and Time" task on page 17 (any nodes not using Simple Network Time Protocol [SNTP]).

Step 9 As needed, upgrade any spare TCC2 or TCC2P cards by installing the spare in the standby slot of a Release 6.2 node.

Note The standby TCC2 or TCC2P card copies one or both software releases from the active TCC2 or TCC2P card, as needed. Each software copy takes about 5 minutes, and the TCC2 or TCC2P card resets after each copy. Thus, for a TCC2 or TCC2P card that has no matching software with the active TCC2 or TCC2P card, you should expect to see two TCC2 or TCC2P card resets and software copying lasting about 10 minutes total.

Step 10 If you need to return to the software and database you had before activating Software R6.2, proceed with the "NTP-U130 Revert to Previous Software Load and Database" procedure on page 19.

Step 11 To back up the Release 6.2 database for the Working software load, see "NTP-U128 Back Up the Software Database" procedure on page 8 in order to preserve the database for the Release 6.2 software

Stop. You have completed this procedure.

DLP-U201 Download Release 6.2 Software

Purpose	This task downloads Software R6.2 to the ONS 15454 nodes prior to activation.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-U128 Back Up the Software Database, page 8
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of the workstation)
Security Level	Maintenance user or higher

Note The TCC2/TCC2P card has two flash RAMs. An upgrade downloads the software to the backup RAM on both the standby and active TCC2/TCC2P cards. The download task 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.

Note To download and upgrade the software using TL1, see the "NTP-U132 Upgrade to Release 6.2 Using TL1" procedure on page 24.

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Verify that the alarm filter is not on:

a. Click the **Alarms** tab.

b. Click the **Filter** tool at the lower-right side of the bottom toolbar.

Alarm filtering is enabled if the tool is depressed (selected) and disabled if the tool is raised (not selected).

Step 3 On the Alarms tab, check all nodes 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 4 Return to node view and click the **Maintenance** > **Software** tabs.

Step 5 Click **Download**. The Download Selection dialog box appears.

Step 6 Browse to locate the software files on the ONS 15454 software CD or on your hard drive, if you are working from a local copy.

Step 7 Open the Cisco15454 folder.

Step 8 Select the file with the .pkg extension and click **Open**.

Step 9 In the list of compatible nodes, select the check boxes for all nodes you are downloading the software to.

Note Cisco advises that you limit concurrent software downloads on a section data communications channel (SDCC) to eight nodes at once, using the central node to complete the download.

Note If you attempt more than eight concurrent software downloads at once, the downloads in excess of eight will be placed in a queue.

Step 10 Click OK. The Download Status column monitors the progress of the download.

Note The software download process can take typically less than 10 minutes per node.

Step 11 Return to your originating procedure (NTP).

DLP-U202 Perform a BLSR Lockout

Purpose	This task performs a Release 6.2 BLSR lockout. If you have a BLSR provisioned, you must perform this task before beginning the upgrade.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-U128 Back Up the Software Database, page 8
Required/As Needed	Required for BLSR only
Onsite/Remote	Onsite or remote (but in the presence of the workstation)
Security Level	Superuser

Note During the activation, BLSR spans are not protected. You must leave the BLSR in the lockout state until you have finished activating all nodes in the ring, but then you must be sure to remove the lockout after you are finished activating.

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

Step 1 In node view, click the **Maintenance > BLSR** tabs.

Step 2 For each of the BLSR trunk (span) cards (OC-12, OC-48, OC-192, MRC-12), perform the following steps:

a. Next to the trunk card row, click the **East Switch** column to show the pull-down menu.

b. From the menu options, choose **Lockout Span**.

c. Click **Apply**.

d. In the same row, click the **West Switch** column to show the pull-down menu.

e. From the menu options, choose **Lockout Span**.

f. Click **Apply**.

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

Note Certain BLSR or MSSP-related alarms might be raised following activation of the first node in the ring. The following alarms, if raised, are normal, and should not cause concern. They clear upon completion of the upgrade, after all nodes have been activated.

- BLSR-OOSYNC (MN)
- RING-MISMATCH (MJ)
- APSCDFLTK (MN)

- BLSR-RESYNC (NA)

Step 3 Return to your originating procedure (NTP).

DLP-U203 Activate the New Load

Purpose	This task activates Software R6.2 in each node in the network.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	DLP-U201 Download Release 6.2 Software, page 10 DLP-U202 Perform a BLSR Lockout, page 12 (if required)
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of the workstation)
Security Level	Superuser

Note Ensure that all cards that are part of a protection group (1+1, 1:1, or 1:N) are active on the working card of that protection group and that no protection switches are occurring. To ensure that traffic carrying protect cards are in a standby state, in the node view, Maintenance > Protection tab select each of the listed protection groups, then view the Active/Standby status of each card in the Selected Group area.

Note Cisco recommends you run the optional Cache Loader pre-caching utility in Step 13 or the activation task. If you do not plan to run the pre-caching utility, Cisco recommends that the first node you activate be a LAN-connected node. This ensures that the new CTC JAR files download to your workstation as quickly as possible.

Note ML cards undergo a cold restart during an upgrade. The following alarms might be raised in conjunction with the ML cold restart. These should clear once the upgrade is complete.

On the ML port:

- LOA
- TPTFAIL
- VCG DOWN

On the paths traversed by the ML circuits:

- SD-P
- SF-P
- PDI-P

Note If the Cisco IOS version has changed from the previous release to the new release, an ERROR-CONFIG alarm is raised on each ML card after the reset. To clear this alarm, perform a "copy running-config startup-config" (or a "write mem") on each ML card. See the "Initial Configuration" chapter of the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Step 1 Record the IP address of the node. The IP address can be obtained either on the LCD or on the upper left corner of the CTC window.

Step 2 Verify that the alarm filter is not on:

a. Click the **Alarms** tab.

b. Click the **Filter** tool at the lower-right side of the bottom toolbar.

Alarm filtering is enabled if the tool is depressed (selected) and disabled if the tool is raised (not selected).

Step 3 On the Alarms tab, check all nodes for existing alarms. Resolve any outstanding alarms before proceeding.

Step 4 Click the **Maintenance** > **Software** tabs.

Step 5 Verify that the protect version is 6.2.

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 when the software is successfully activated.

Step 8 Click **OK** in the message box.

When you click OK, CTC loses connection to the node and displays the network view.

Step 9 After activating the node, the software upgrade reboot occurs as follows:

- Each card in the node reboots, beginning with the standby TCC2 or TCC2P card. When the standby TCC2/TCC2P comes back up, it signals to the active TCC2/TCC2P that it is ready to take over. When the active TCC2/TCC2P receives this signal, it resets itself, and the standby TCC2/TCC2P takes over and transitions to active. The originally active TCC2/TCC2P then comes back up as the standby TCC2/TCC2P.
- While the second TCC2/TCC2P is rebooting, the cross-connect card (SONET/SDH only) in Slot 8 reboots, and then the cross-connect card (SONET/SDH only) in Slot 10 reboots.
- Next, the E-series Ethernet cards reset simultaneously.
- Next, the traffic cards, G-series Ethernet cards, CE-series Ethernet cards, and ML-series Ethernet cards boot consecutively from left to right, first standby, then working, for each card pair.
- A system reboot (SYSBOOT) alarm is raised while activation is in progress (following the TCC2/TCC2P and cross connect card resets). When all cards have reset, this alarm clears. The activation process can take up to 30 minutes, depending on how many cards are installed.

After the common control cards finish resetting and all associated alarms clear, you can safely proceed to the next step. (If you are upgrading remotely and cannot see the nodes, wait for 5 minutes for the process to complete, then check to ensure that related alarms have cleared before proceeding.)

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

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

Note You must ensure that CTC is closed before clicking the Delete CTC Cache button. CTC behavior is unreliable if the button is clicked while the software is still running.

Note It might also be necessary to delete cached files from your browser's directory, or from the temp directory on your MS Windows workstation. If you have trouble reconnecting to CTC, complete the "DLP-U102 Delete Cached JAR Files" task on page 16.

Step 12 Close your browser and then reopen it.

Step 13 (Optional) Run the Cache Loader pre-caching utility, which can improve your speed logging back into CTC after an upgrade, and which is required to log into nodes running releases prior to Release 4.6. Perform the following steps to run the Cache Loader.

- **a.** Load the Release 6.2 CD into your CD-ROM drive. If the directory of the CD does not open automatically, open it.
- **b.** Double-click the setup.exe file to run the Installation Wizard. The CTC installation wizard dialog box opens.
- **c.** Click Next. The setup options dialog box opens.
- **d.** Choose Custom, and click Next. The custom options dialog box opens.
- **e.** Select Cisco Transport Controller, and CTC JAR files (deselect any other preselected options), then click Next. A confirmation box opens.
- **f.** Click Next again. The CTC Cache Loader pre-caches the JAR files to your workstation, displaying a progress status box.
- **g.** When the utility finishes, click OK, and then in the wizard, click Finish.

Step 14 Reconnect to CTC using the IP address from Step 1. The new CTC applet for Software R6.2 uploads. During this logon, type the user name CISCO15. A password is not required.

Note Steps 10 through 14 are necessary only after upgrading the first node in a network because cached files need to be removed from your workstation only once. 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 restores connectivity to the node.

Step 15 Return to your originating procedure (NTP).

DLP-U102 Delete Cached JAR Files

Purpose	This task deletes cached Jar files. When you upgrade or revert to a different CTC software load, you must reload CTC to your browser. Before you can reload CTC, you must ensure that previously cached files are cleared from your browser and hard drive.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	None
Required/As Needed	You need to complete this task only after you activate the first node in the network.
Onsite/Remote	Onsite or remote (but in the presence of the workstation)
Security Level	Maintenance user or higher

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** check box.

d. Click **OK** twice.

Step 2 Close your browser.

Note You cannot delete cached JAR files from your hard drive until you have closed your browser. If you have other applications open that use JAR files, you must also close them.

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 shows you a list of user variables and a list of system variables.

c. In the list of user variables, look for the TEMP variable. 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 discovered path.

e. Select **View** > **Details**.

f. Select and delete all files with “jar” in the Name or Type field.

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

Step 5 Return to your originating procedure (NTP).

DLP-U204 Remove the BLSR Lockout

Purpose	This task removes a BLSR lockout. Release the span lockouts on all BLSR nodes after the new software load is activated on all nodes.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	DLP-U203 Activate the New Load, page 13
Required/As Needed	Required for BLSR
Onsite/Remote	Onsite or remote (but in the presence of the workstation)
Security Level	Superuser

Step 1 In CTC node view, click the **Maintenance** > **BLSR** tabs.

Step 2 For each of the BLSR trunk (span) cards (OC-12, OC-48, OC-192, MRC-12), perform the following steps:

a. Next to the trunk card row, 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 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 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 Repeat this task as many times as necessary to remove all BLSR span lockouts on the upgrade nodes.

Step 4 Return to your originating procedure (NTP).

DLP-U66 Set the Date and Time

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

Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote (but in the presence of the workstation)
Security Level	Superuser

Note If you are using SNTP, you do not need this task.

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.

Step 4 Return to your originating procedure (NTP).

NTP-U103 Install Public-Key Security Certificate

Purpose	This procedure installs the ITU Recommendation X.509 public-key security certificate. The public-key certificate is required to run Software R4.1 or later.
Tools/Equipment	None
Prerequisite Procedures	This procedure is performed when logging into CTC. You cannot perform it at any other time.
Required/As Needed	This procedure is required to run ONS 15454 Software R4.1 or later.
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Log into CTC.

Step 2 If the Java Plug-in Security Warning dialog box appears, choose one of the following options:

- Grant This Session—Installs the public-key certificate to your PC only for the current session. After the session is ended, the certificate is deleted. This dialog box will appear the next time you log into the ONS 15454.
- Deny—Denies permission to install the certificate. If you choose this option, you cannot log into the ONS 15454.
- Grant always—Installs the public-key certificate and does not delete it after the session is over. Cisco recommends this option.
- View Certificate—Allows you to view the public-key security certificate.

After you complete the security certificate dialog boxes, the web browser displays information about your Java and system environments. If this is the first login, a CTC downloading message appears while CTC files are downloaded to your computer. The first time you connect to an ONS 15454, this process can take several minutes. After the download, the CTC Login dialog box appears.

Step 3 If you need to return to the software and database you had before activating Software R4.7, proceed with the "NTP-U130 Revert to Previous Software Load and Database" procedure on page 19.

Stop. You have completed this procedure.

NTP-U130 Revert to Previous Software Load and Database

Purpose	This procedure returns you to the software and database provisioning you had before you activated Software R6.2.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-U127 Prepare for Upgrade to Release 6.2, page 5 NTP-U128 Back Up the Software Database, page 8 NTP-U129 Upgrade to Release 6.2, page 9
Required/As Needed	As needed
Onsite/Remote	Onsite or remote (but in the presence of the workstation)
Security Level	Superuser

Note The tasks to revert to a previous load are not a part of the upgrade. They are provided here as a convenience to those wishing to perform a revert after an upgrade. If you have performed all necessary procedures up to this point, you have finished the software upgrade.

Note Before you upgraded to Software R6.2, you should have backed up the existing database at all nodes in the network (this is part of the "NTP-U128 Back Up the Software Database" procedure on page 8). 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 tasks, in order.

Caution If you have converted a node to secure, dual-IP mode, the database information is overwritten with this configuration and you cannot revert it to single-IP repeater mode.

Note TCC2P cards act as TCC2 cards in Releases prior to Release 5.0.

Step 1 Log into the node. For detailed instructions, refer to the *Cisco ONS 15454 Procedure Guide*, or *Cisco ONS 15454 DWDM Installation and Operations Guide*. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-U202 Perform a BLSR Lockout" task on page 12 (BLSR only).

Step 3 Complete the "DLP-U205 Revert to Protect Load" task on page 20.

Step 4 Complete the "DLP-U204 Remove the BLSR Lockout" task on page 17 (BLSR only).

Step 5 If the software revert to your previous release failed, complete the "DLP-U171 Manually Restore the Database" task on page 21.

Stop. You have completed this procedure.

DLP-U205 Revert to Protect Load

Purpose	This task reverts to the software you were running prior to the last activation.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-U127 Prepare for Upgrade to Release 6.2, page 5 NTP-U128 Back Up the Software Database, page 8 NTP-U129 Upgrade to Release 6.2, page 9 DLP-U202 Perform a BLSR Lockout, page 12
Required/As Needed	Required for revert
Onsite/Remote	Onsite or remote (but in the presence of the workstation)
Security Level	Superuser

Note To perform a supported (non-service-affecting) revert from Software R6.2, the release you want to revert to must have been working at the time you activated to Software R6.2 on that node. Also, a supported revert automatically restores the node configuration at the time of the previous activation. Thus, any configuration changes made after activation will be lost when you revert the software. The exception to this is when you have downloaded Release 6.2 a second time, to ensure that no actual revert to a previous load can take place. In this latter case, the revert will occur, but will not be traffic affecting and will not change your database.

Note Ensure that all cards that are part of a protection group (1+1, 1:1, or 1:N) are active on the working card of that protection group and that no protection switches are occurring. In other words, ensure that the protect cards are in standby before proceeding. Move your mouse cursor over a card in node view to see its active or standby status.

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

Step 2 Verify that the protect software displays 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 Wait until the software revert finishes before continuing.

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

Step 6 Close your Netscape or Internet Explorer browser.

Step 7 Wait one minute before restoring another node.

Note After you upgrade to JRE 1.4.2, you cannot log into an ONS 15454, ONS 15454 SDH, or ONS 15327 node until you reconfigure the Java Plug-in to use JRE 1.3.1. If you are reverting to a release that uses JRE 1.3.1_02 and you retained JRE 1.3.1_02 during the upgrade, you do not need to do anything.

Step 8 Perform the "DLP-U102 Delete Cached JAR Files" task on page 16.

Step 9 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 to your workstation.

Step 10 Return to your originating procedure (NTP).

DLP-U171 Manually Restore the Database

Purpose	This task manually restores the database. Use this task if you were unable to perform a revert successfully and need to restore the database.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	DLP-U205 Revert to Protect Load, page 20 DLP-U204 Remove the BLSR Lockout, page 17 (if required)
Required/As Needed	As needed
Onsite/Remote	Onsite or remote (but in the presence of the workstation)
Security Level	Superuser

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

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

Step 1 In the CTC node view, click the **Maintenance** > **Database** tabs.

Step 2 Click **Restore**. The Open dialog box appears.

Step 3 Select the previously saved file and choose **Open**.

The database is restored and the TCC2/TCC2P cards reboot.

Step 4 When the TCC2/TCC2P cards have finished rebooting, log back into CTC and verify that the database is restored.

Wait one minute before restoring the next node.

Repeat Steps 1 to 4 for each node in the network.

Step 5 You have now completed the manual database restore.

Step 6 Return to your originating procedure (NTP).

NTP-U131 Upgrade the TCC+ Card to the TCC2/TCC2P Card

Purpose	This procedure upgrades the TCC+ card to the TCC2/TCC2P card. The TCC2/TCC2P card supports ONS 15454 Software R4.x and forward. The TCC+ card is compatible with ONS 15454 Software R4.0 and R4.1.x, as well as earlier software versions.
Tools/Equipment	Two SONET TCC2 or TCC2P cards
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Maintenance or higher

Note Downgrade procedures from TCC/TCC2P2 cards to TCC+ cards are not supported. Contact Cisco TAC for more information. See the "Obtaining Technical Assistance" section on page 31 for contact information.

Step 1 Log into CTC. For detailed instructions, refer to the *Cisco ONS 15454 Procedure Guide*. If you are already logged in, continue with Step 2.

Step 2 Verify that the LAN wires on the backplane are installed properly. The TCC2/TCC2P card does not autodetect miswired LAN connections. If a LAN connection is miswired, a LAN Connection Polarity Reversed condition appears. For information on installing LAN wires, refer to the *Cisco ONS 15454 Procedure Guide*.

Step 3 Verify that the node you are upgrading has ONS 15454 Software R4.x installed. The software version is displayed in the upper left corner of the window.

Step 4 Complete the "NTP-U128 Back Up the Software Database" procedure on page 8 before beginning the upgrade.

Step 5 Physically replace the standby TCC+ card on the ONS 15454 with a TCC2/TCC2P card.

- **a.** Check the LED on the faceplate. The ACT/STBY LED on the faceplate of the TCC+/TCC2/TCC2P card indicates whether the card is in active or standby mode. A green ACT/STBY LED indicates an active card and an amber light indicates a standby card.
- **b.** Open the standby TCC+ card ejectors.
- **c.** Slide the card out of the slot. This raises the IMPROPRMVL alarm, which clears when the upgrade is complete.
- **d.** Open the ejectors on the TCC2/TCC2P card to be installed.
- **e.** Slide the TCC2/TCC2P card into the slot along the guide rails.
- **f.** Close the ejectors.
- **g.** In CTC node view, Ldg (loading) appears on the newly installed TCC2/TCC2P card.

Note The MEA (card mismatch) alarm appears because CTC recognizes a mismatch between TCC card types. Disregard this alarm; it clears by the end of the procedure.

Note It takes approximately 10 minutes for the active TCC+ card to transfer the system software and database to the newly installed TCC2/TCC2P card. During this operation, the LEDs on the TCC2/TCC2P card flash Fail and then the active/standby LED flashes. When the transfer completes, the TCC2/TCC2P card reboots and goes into standby mode after approximately three minutes. Do not remove the card from the shelf during a database transfer.

Caution If your active TCC+ card resets during the upgrade before the new TCC2/TCC2P card is in full standby mode, remove the new TCC2/TCC2P card immediately.

Step 6 When the newly installed TCC2/TCC2P card is in standby, right-click the active TCC+ card in CTC.

Step 7 From the pull-down menu, click **Reset Card**.

Wait for the TCC+ card to reboot. The ONS 15454 switches the standby TCC2/TCC2P card to active mode. The TCC+ card verifies that it has the same database as the TCC2/TCC2P card and then switches to standby.

Step 8 Verify that the remaining TCC+ card is now in standby mode (the ACT/STBY LED changes to amber).

Step 9 Physically replace the remaining TCC+ card with the second TCC2/TCC2P card.

a. Open the TCC+ card ejectors.

b. Slide the card out of the slot. This raises the IMPROPRMVL alarm, which clears when the upgrade is complete.

c. Open the ejectors on the TCC2/TCC2P card.

d. Slide the TCC2/TCC2P card into the slot along the guide rails.

e. Close the ejectors.

The ONS 15454 boots up the second TCC2/TCC2P card. The second TCC2/TCC2P card must also copy the database. Do not remove the card from the shelf during a database transfer.

Tip When a newly installed TCC2/TCC2P card has a different version of the ONS 15454 software installed from the version running on the active TCC2/TCC2P card, the newly installed TCC2/TCC2P card automatically copies the software version running on the active TCC2/TCC2P card. You do not need to do anything in this situation. However, the loading TCC2/TCC2P card does not boot up in the normal manner. When the card is first inserted, the red FAIL LED stays on for a short period. The FAIL LED then blinks normally and all LEDs go dark. After loading the new software for approximately 10 minutes, the TCC2/TCC2P card becomes the standby card and the amber LED is illuminated.

Step 10 If power-related alarms occur after the second TCC2/TCC2P card is installed, check the voltage on the backplane. Refer to the *Cisco ONS 15454 Troubleshooting Guide* for information on clearing alarms.

Stop. You have completed this procedure.

NTP-U132 Upgrade to Release 6.2 Using TL1

Purpose	This procedure upgrades the Software R6.2 software using TL1 rather than CTC.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-U127 Prepare for Upgrade to Release 6.2, page 5 NTP-U128 Back Up the Software Database, page 8
Required/As Needed	Optional
Onsite/Remote	Onsite or remote (but in the presence of the workstation)
Security Level	Superuser

Note This procedure assumes you are upgrading using Release 5.x or 6.0.x TL1 syntax. TL1 commands issued prior to software activation to Release 6.2 will vary in syntax depending on the release you are actually upgrading from. To ensure that your syntax for each command is correct, use the TL1 syntax supplied in the *Cisco ONS SONET TL1 Command Guide* for your particular release when issuing the following commands:

- ACT-USER
- COPY-RFILE
- REPT EVT FXFR
- OPR-PROTNSW-<OCN_TYPE>
- RTRV-COND-ALL
- RTRV-ALM-ALL

Note To perform a download using TL1, you must first have an FTP server running on your workstation in order to establish the required FTP session. For example, if your FTP server is set up with a login and password of FTPUSER1 and FTPUSERPASSWORD1, and if the FTP server has an IP address of 10.1.1.1 and is running on the standard FTP port, where the software package is called "15454-03xx-A04K-1405.pkg," the command, which is different depending on if you are downloading software to a GNE or ENE, follows:

- Downloading software to a GNE

```
COPY-RFILE:NODENAME:RFILE-PKG:CTAG::TYPE=SWDL,
SRC="ftp://FTPUSER1:FTPUSERPASSWORD1@10.1.1.1/15454-03xx-A04K-1405.pkg";
```

- Downloading Software To An ENE

```
COPY-RFILE:NODENAME:RFILE-PKG:CTAG::TYPE=SWDL,
SRC="ftp://FTPUSER1:FTPUSERPASSWORD1@10.1.1.1:21@90.90.90.90/15454-03xx-A04K-1405.pkg";
```

The ":21" after the FTP server IP address denotes port 21 on the server.

The software *.pkg file in the preceding example is located in the home directory of the FTP server. If the software *.pkg file is not in the home directory on the FTP server, insert the directory path where the software *.pkg resides between the last IP address and the *.pkg file in the command line. An example is shown here.

```
COPY-RFILE:NODENAME:RFILE-PKG:CTAG::TYPE=SWDL,
SRC="ftp://FTPUSER1:FTPUSERPASSWORD1@10.1.1.1:21@90.90.90.90/CISCO/SOFTWARE/15454-03xx-A04
K-1405.pkg";
```

Step 1 Open a Telnet session to the ONS 15454 GNE using port 3083 or 2361.

Step 2 Type the **Activate User** command in the TL1 request window to open a TL1 session:

```
ACT-USER:[<TID>]:<uid>:<CTAG>[::<pid>];
```

where:

- <TID> is the target identifier.
- <UID> is the OSS profile name (username).
- <CTAG> is the correlation tag that correlates command and response messages.
- <PID> is the password identifier (password).

Step 3 Repeat Step 2 for each node to be upgraded.

Step 4 Type the **COPY-RFILE** command in the TL1 window. The **COPY-RFILE** command downloads a new software package from the location specified by the FTP URL into the inactive Flash partition residing on either of the TCC2/TCC2P cards.

```
COPY-RFILE:[<TID>]:<src>:<CTAG>::TYPE=<xfertype>,[SRC=<src1>],[DEST=<dest>],[OVWRT=<ovwrt>
],[FTTD=<fttd>];
```

where:

- <TID> is the target identifier.
- <SRC> is the source AID.
- <CTAG> is the correlation tag that correlates command and response messages.
- <XFERTYPE> is the file transfer protocol.
- <SRC1> specifies the source of the file to be transferred. Only the FTP URL is supported.
- <DEST> is the destination of the file to be transferred.
- <OVWRT> is overwrite. If <OVWRT> is yes, then files should be overwritten. If <OVWRT> is no, then file transfers will fail if the file already exists at the destination.
- <FTTD> is the URL format.

Step 5 Repeat Step 4 for all nodes to be upgraded.

Step 6 Look for the **REPT EVT FXFR** message in the TL1 window. REPT EVT FXFR is an autonomous message used to report the start, completion, and completed percentage status of the FTP software download. REPT EVT FXFR also reports any failure during the software upgrade, including invalid package, invalid path, invalid userid/password, and loss of network connection. The format of the message is:

```
REPT EVT FXFR

   SID DATE TIME
A  ATAG REPT EVT FXFR
   "<FILENAME>,<FXFR_STATUS>,[<FXFR_RSLT>],[<BYTES_XFRD>]"
;
```

where:

- <FILENAME> indicates the transferred file path name and is a string.
- <FXFR_STATUS> indicates the file transferred status: Start, IP (in progress), or COMPLD.
- <FXFR_RSLT> indicates the file transferred result: success or failure. FXFR_RSLT is optional (the FXFR_RSLT is only sent when the FXFR_STATUS is COMPLD).

- <BYTES_XFRD> indicates the percentage transfer complete and is optional (the BYTES_XFRD is only sent when the FXFR_STATUS is IP or COMPLD).

Step 7 Complete NTP-U127 Prepare for Upgrade to Release 6.2, page 5 for each node to be upgraded.

Step 8 Complete NTP-U128 Back Up the Software Database, page 8 for each node to be upgraded.

Step 9 Lock out each BLSR span on each node being upgraded using the following command.

```
OPR-PROTNSW-<OCN_TYPE>:[<TID>]:<AID>:<CTAG>::<SC>,[<SWITCHTYPE>][:<DIRN>];
```

where:

- <AID> identifies the facility in the NE to which the switch request is directed.
- <SC> is the switch command that is to be initiated on the paths
- <SWITCHTYPE> BLSR switch type.
- <DIRN> is the direction of transmission in which switching is to be made and is relative to the SONET line or path identified by the AID. The default value is RCV and should be changed to BTH.

Note Some nodes might have more than one BLSR. If this is the case, all BLSR spans on all nodes being upgraded need to be locked out. Nodes that are not being upgraded do not need to have the BLSR spans locked out. You must be aware of each span that is part of a BLSR to make sure all necessary spans are locked out.

Note BLSR lockouts must remain in place until the upgrade is complete for all nodes.

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

Note Certain BLSR or MSSP-related alarms might be raised following activation of the first node in the ring. The following alarms, if raised, are normal, and should not cause concern. They clear upon completion of the upgrade, after all nodes have been activated: BLSR-OOSYNC (MN); RING-MISMATCH (MJ); APSCDFLTK (MN); BLSR-RESYNC (NA).

Step 10 Verify that all necessary BLSR spans on each node being upgraded have been locked out using the following command:

```
RTRV-PROTNSW-<OCN_TYPE>:[<TID>]:<AID>:<CTAG>[::::];
```

where:

<AID> indicates the entity in the NE. <AID> must not be null.

Step 11 Verify that there are no outstanding alarms or conditions on each node using the following commands:.

```
RTRV-COND-ALL:[<TID>]:[<AID>]:<CTAG>::[<TYPEREQ>][,,,];
```

where:

- <TYPEREQ> is the type of condition to be retrieved. A null value is equivalent to ALL.

```
RTRV-ALM-ALL:[<TID>]:[<AID>]:<CTAG>::[<NTFCNCDE>],[<CONDITION>],[<SRVEFF>][,,,];
```

where:

- <NTFCNCDE> is a notification code. A null value is equivalent to ALL.
- <CONDITION> is the type of alarm condition. A null value is equivalent to ALL.
- <SRVEFF> is the effect on service caused by the alarm condition. A null value is equivalent to ALL.

Resolve all issues before proceeding.

Note You can only activate one node at a time; however, in a parallel upgrade you can begin activation of the next node as soon as the controller cards for the current node have rebooted successfully. If you wish to perform a parallel upgrade, wait five minutes for the controller cards to complete the reboot.

Step 12 Starting at the node furthest from the GNE type the APPLY command to activate the system software.

```
APPLY:[<TID>]::<CTAG>[::<MEM_SW_TYPE>];
```

where:

- <TID> is the target identifier.
- <CTAG> is the correlation tag that correlates command and response messages.
- <MEM_SW_TYPE> indicates a memory switch action during the software upgrade. MEM_SW_TYPE is ACT for activate.

If the command is successful, the appropriate flash is selected and the TCC2/TCC2P card reboots.

The following occurs:

- Each card in the node reboots, beginning with the standby TCC2 or TCC2P card. When the standby TCC2/TCC2P comes back up, it signals to the active TCC2/TCC2P that it is ready to take over. When the active TCC2/TCC2P receives this signal, it resets itself, and the standby TCC2/TCC2P takes over and transitions to active. The originally active TCC2/TCC2P then comes back up as the standby TCC2/TCC2P.
- While the second TCC2/TCC2P is rebooting, the cross-connect card (SONET/SDH only) in Slot 8 reboots, and then the cross-connect card (SONET/SDH only) in Slot 10 reboots.
- Next, the E-series Ethernet cards reset simultaneously.
- Any cards in Y-cable protection groups boot next, one at a time (protect card first), in order of first creation (refer to the CTC protection group list for order of first creation).
- Next, the traffic cards, G-series Ethernet cards, CE-series Ethernet cards, and ML-series Ethernet cards boot consecutively, in ascending order of slot number, first standby, then working, for each card pair, with the exception that E1-42 protect cards will always be reset before any of their peer working cards.
- A system reboot (SYSBOOT) alarm is raised while activation is in progress (following the TCC2/TCC2P and cross connect card resets). When all cards have reset, this alarm clears. The complete activation process can take up to 30 minutes, depending on how many cards are installed.

After the common control cards finish resetting and all associated alarms clear, you can safely proceed to the next step. (If you are upgrading remotely and cannot see the nodes, wait for 5 minutes for the process to complete, then check to ensure that related alarms have cleared before proceeding.)

Step 13 Perform Step 12 for each node that will be upgraded, moving from the furthest node from the GNE toward the GNE itself, which should be activated last.

Note Note You might have to log in (Step 1 and Step 2) to each node again to activate the software (Step 12).

Step 14 After all nodes have been activated, log in using CTC or Telnet (Step 1 and Step 2) and verify there are no outstanding alarms.

Step 15 Remove all BLSR lockouts using the following TL1 command:

```
RLS-PROTNSW-<OCN_TYPE>:[<TID>]:<AID>:<CTAG>[::<DIRECTION>];
```
where:

<AID> identifies the facility in the NE to which the switch request is directed.

<DIRN> is the direction of transmission (transmit or receive). The possible values are:

- RCV—receive direction only (default)
- TRMT—transmit direction only
- BTH—both transmit and receive directions

For example:

```
RLS-PROTNSW-OC48:PETALUMA:FAC-6-1:209::BTH;
```

Stop. You have completed this procedure.

Related Documentation

Use this document in conjunction with the following publications:

- *Cisco ONS 15454 Procedure Guide*
  Provides installation, turn up, test, and maintenance procedures
- *Cisco ONS 15454 Reference Manual*
  Provides technical reference information for SONET/SDH cards, nodes, and networks
- *Cisco ONS 15454 DWDM Installation and Operations Guide*
  Provides technical reference information for DWDM cards, nodes, and networks
- *Cisco ONS 15454 Troubleshooting Guide*
  Provides a list of SONET alarms and troubleshooting procedures, general troubleshooting information, and hardware replacement procedures
- *Cisco ONS SONET TL1 Command Guide*
  Provides a full TL1 command and autonomous message set including parameters, AIDs, conditions and modifiers for the Cisco ONS 15454, ONS 15327, ONS 15600 and ONS 15310-CL systems.
- *Cisco ONS SONET TL1 Reference Guide*
  Provides general information, procedures, and errors for TL1 in the Cisco ONS 15454, ONS 15327, ONS 15600 and ONS 15310-CL systems
- *Ethernet Card Software Feature and Configuration G uide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*, Release 6.2
  Provides software features for all Ethernet cards and configuration information for Cisco IOS on ML-Series cards.
- *Release Notes for Cisco ONS 15454 Release 6.2*
  Provides caveats, closed issues, and new feature and functionality information

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

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

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

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

Cisco Optical Networking Product Documentation CD-ROM

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

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

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

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

Documentation Feedback

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

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

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

- Nonemergencies—psirt@cisco.com

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

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

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

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

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

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

Obtaining Technical Assistance

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

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

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

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

Printed in the USA on recycled paper containing 10% postconsumer waste.