

# Upgrading the Cisco ONS 15600 to Release 7.2

October 2007



**Note**

The terms "Unidirectional Path Switched Ring" and "UPSR" may appear in Cisco literature. These terms do not refer to using Cisco ONS 15xxx products in a unidirectional path switched ring configuration. Rather, these terms, as well as "Path Protected Mesh Network" and "PPMN," refer generally to Cisco's path protection feature, which may be used in any topological network configuration. Cisco does not recommend using its path protection feature in any particular topological network configuration.

This document explains how to upgrade the Cisco ONS 15600 Cisco Transport Controller (CTC) software from Release 5.0.x, 6.x, or 7.0.x to Release 7.2.x, or from Release 7.2.x to a later maintenance release of 7.2.x, using the Timing and Shelf Controller (TSC) card. The ONS 15600 supports errorless upgrades.

## Contents

- [Before You Begin, page 2](#)
- [NTP-U186 Prepare for the Release 7.2 Upgrade, page 3](#)
- [NTP-U187 Back Up the Software Database, page 4](#)
- [NTP-U188 Upgrade to Release 7.2, page 6](#)
- [NTP-U189 Restore the Previous Software Load and Database, page 16](#)
- [Related Documentation, page 17](#)
- [Where to Find Safety and Warning Information, page 18](#)
- [Obtaining Documentation, page 18](#)
- [Documentation Feedback, page 19](#)
- [Cisco Product Security Overview, page 19](#)
- [Obtaining Technical Assistance, page 20](#)
- [Obtaining Additional Publications and Information, page 22](#)



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

© 2007 Cisco Systems, Inc. All rights reserved.

# Before You Begin

Before beginning, write down the following information about your site: date, street address, site phone number, and dial-up number. This data will be useful during and after the upgrade.


**Caution**

Before beginning an upgrade of an ONS 15600 from Release 5.x to Release 7.2 contact the Cisco TAC for system verification. See the [“Obtaining Technical Assistance” section on page 20](#) for TAC contact information. This step is not necessary if you are upgrading from Release 6.0 or later.


**Caution**

Read each procedure before you begin the upgrade.


**Caution**

This document supports upgrades from Release 5.0.x, 6.x, or 7.0.x to 7.2.x, or from Release 7.2.x to a later maintenance release of 7.2.x. You cannot upgrade from Releases 1.1.x or 1.3.x, to 7.2.


**Note**

Release 7.2 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.


**Note**

Perform the procedures in this document in consecutive order unless otherwise noted. In general, you are not done with a procedure until you have completed it for each node that 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 15600, you might want to check off each procedure on your printed copy of this document as you complete it.

This section lists the document procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

Each non-trouble procedure (NTP) is a list of steps designed to accomplish a specific task. Follow the steps until the task is complete. For a crafts person requiring more detailed instructions, refer to the Detailed Level Procedure (DLP) specified in the procedure steps.

The detailed level procedure (DLP) supplies additional task details to support the NTP. The DLP lists numbered steps that lead the crafts person 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.

The following NTPs are in this document:

1. [NTP-U186 Prepare for the Release 7.2 Upgrade, page 3](#)—This procedure contains critical information and tasks that you must read and complete before beginning the upgrade process.
2. [NTP-U187 Back Up the Software Database, page 4](#)—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-U188 Upgrade to Release 7.2, page 6](#)—You must complete this entire procedure to complete the upgrade.
4. [NTP-U189 Restore the Previous Software Load and Database, page 16](#)—Complete this procedure if you need to return to Software R5.x.

## NTP-U186 Prepare for the Release 7.2 Upgrade

<b>Purpose</b>	This procedure steps you through the critical information checks and tasks you must complete before beginning an upgrade.
<b>Tools/Equipment</b>	PC or UNIX workstation; Cisco ONS 15600 Software Release 7.2 (CD or soft copy)
<b>Prerequisite Procedures</b>	None
<b>Required/As Needed</b>	Required
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Superuser

- 
- Step 1** Read the *Release Notes for Cisco ONS 15600 Release 7.2*.
- Step 2** Log into the node that you will upgrade. For detailed instructions, refer to the *Cisco ONS 15600 Procedure Guide*.
- Step 3** Complete the “[DLP-U280 Verify CTC Workstation Requirements](#)” task on page 3.
- Step 4** Disable all other Ethernet devices (such as a dial-up adapter) on the workstation that runs CTC. For instructions, contact the Cisco Technical Assistance Center (TAC).
- If you have multiple IP addresses on your workstation, you should remove them; you cannot run Software R7.2 if multiple IP addresses are configured.
- Step 5** Verify that TSC cards are installed in Slots 5 and 10 and that the TSC in Slot 10 is active.
- Step 6** Complete the “[NTP-U187 Back Up the Software Database](#)” task on page 4.
- Stop. You have completed this procedure.**
- 

## DLP-U280 Verify CTC Workstation Requirements

<b>Purpose</b>	This task verifies that all PC or UNIX workstation hardware and software requirements are met.
<b>Tools/Equipment</b>	PC or UNIX workstation
<b>Prerequisite Procedures</b>	None
<b>Required/As Needed</b>	Required
<b>Onsite/Remote</b>	Onsite or remote (but in the presence of the workstation)
<b>Security Level</b>	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 on Windows
- Internet Explorer 6.x or higher on Windows
- Mozilla 1.7 or higher on Solaris

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

- Java Runtime Environment (JRE) 1.4.2 or JRE 5.0, and Java Plug-in 1.4.2 or Java Plug-in 5.0



**Tip**

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

**Step 4** Verify that 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.

**Step 5** Return to your originating procedure (NTP).

## NTP-U187 Back Up the Software Database

<b>Purpose</b>	This procedure preserves all configuration data for your network before performing the upgrade.
<b>Tools/Equipment</b>	PC or UNIX workstation
<b>Prerequisite Procedures</b>	<a href="#">NTP-U186 Prepare for the Release 7.2 Upgrade, page 3</a>
<b>Required/As Needed</b>	Required
<b>Onsite/Remote</b>	Onsite or remote (but in the presence of the workstation)
<b>Security Level</b>	Superuser



**Note**

To restore a software database, a backup file of that database must be available.

**Step 1** Log into CTC. For detailed instructions, refer to the *Cisco ONS 15600 Procedure Guide*. If you are already logged in, continue with Step 2.

**Step 2** In node view, click the **Maintenance > Database** tabs.

**Step 3** Click **Backup**.

**Step 4** In the Database backup dialog box, click **Browse**.

**Step 5** In the Save dialog box, navigate to a local PC directory or network directory and type a database name (such as database.db) in the File name field.

**Step 6** Click **Save**.

**Step 7** If you are overwriting an existing file, click **Yes** in the confirmation dialog box.

- Step 8** In the Database backup dialog box, check the **Alarms**, **Performance**, and/or **Audit** check boxes to choose these database items in addition to provisioning information.



**Note** Provisioning is a default component of the backup file.

- Step 9** Click **OK**.

- Step 10** Repeat Steps 1 through 9 for each node in the network.

- Step 11** (Optional) Cisco recommends that you manually log critical information by either writing it down or printing screens where applicable. Use [Table 1](#) to determine the information you should log; complete the table (or your own version) for every node in the network.

**Table 1** *Manually Logged Data*

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 TSC <b>Note</b> The TSC card in Slot 10 must be the active TSC card for an upgrade.	Slot 5 or Slot 10 (circle one)
SSXC preferred copy	Slot 6/7 or Slot 8/9 (circle one)
Network information; do a print screen from the Provisioning tab in the network view.	
Current configuration: path protection, 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.	

**Stop. You have completed this procedure.**

# NTP-U188 Upgrade to Release 7.2

<b>Purpose</b>	This procedure upgrades your software to Software R7.2.
<b>Tools/Equipment</b>	PC or UNIX workstation; Cisco ONS 15600 Software Release 7.2 (CD or soft copy)
<b>Prerequisite Procedures</b>	<a href="#">NTP-U187 Back Up the Software Database, page 4</a>
<b>Required/As Needed</b>	Required
<b>Onsite/Remote</b>	Onsite or remote (but in the presence of the workstation)
<b>Security Level</b>	Superuser


**Caution**

Executing an upgrade with a single TSC card is traffic affecting. Do not start an upgrade unless both TSC cards are present and alarm free.


**Note**

To upgrade the software successfully, read and perform each task that applies to your network in the proper order.


**Note**

The UPGRADE, SFTWDOWN, and SW-VER alarms are raised during the upgrade process. These alarms are normal and will clear when the download is complete.

**Step 1** Insert the Software R7.2 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** Log into the node that you want to upgrade. For detailed instructions, refer to the *Cisco ONS 15600 Procedure Guide*. If you are already logged in, continue with Step 3.

**Step 3** (BLSR nodes only) Complete the “[DLP-U281 Perform a BLSR Lockout](#)” task on page 7.


**Note**

The bidirectional line switched ring (BLSR) lockout must be completed for all nodes in all rings for which the ONS 15600 is provisioned.

**Step 4** Complete the “[DLP-U282 Download the Software](#)” task on page 8.




**Step 5** Complete the “[DLP-U283 Activate the New Load](#)” task on page 10.

**Step 6** (As needed) Complete the “[DLP-U253 Delete Cached JAR Files](#)” task on page 12.


**Note**

The “[DLP-U253 Delete Cached JAR Files](#)” task on page 12 is provided in case you have trouble logging back into a node after the activation. This task is not generally necessary.

**Step 7** Reconnect to the node using CTC. The new CTC applet for Software R7.2 uploads.

- Step 8** During the CTC login, complete the “[DLP-U284 Install the Public-Key Security Certificate](#)” task on [page 13](#).
- Step 9** Complete the “[DLP-U285 Accept the New Load](#)” task on [page 14](#).
-  **Note** After you have accepted the Software R7.2 build, you cannot revert to Software R5.x without downloading Software R5.x again and restoring the R5.x database.
- Step 10** Repeat Steps [5](#) through [9](#) for all nodes in the network that need to be upgraded. Allow each node to finish. All alarms should be cleared for 10 minutes before activating the next node.
-  **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 11** Complete the “[DLP-U286 Remove the BLSR Lockout](#)” task on [page 15](#) for all BLSR nodes in the network.
- Step 12** Complete the “[DLP-U94 Set the Date and Time](#)” task on [page 15](#) for any nodes that are not using Simple Network Time Protocol (SNTP).
- Step 13** As needed, upgrade any spare TSC cards by installing the spare in the standby slot of a Software R7.2 node.
-  **Note** When you insert a spare TSC card in the standby slot, a software mismatch is raised. The working software on the active TSC card is then copied to the standby TSC, causing the standby TSC card to reset. When the standby TSC card reset completes, the standby TSC is running the same software version as the active TSC card.
- Step 14** To back up the Release 7.2 database for the Working software load, see “[NTP-U187 Back Up the Software Database](#)” procedure on [page 4](#) in order to preserve the database for the Release 7.2 software. **Stop. You have completed this procedure.**

## DLP-U281 Perform a BLSR Lockout

<b>Purpose</b>	If you have a BLSR provisioned, before beginning the upgrade you must perform a span lockout at each node in the ring.
<b>Tools/Equipment</b>	PC or UNIX workstation, Software R7.2 files
<b>Prerequisite Procedures</b>	<a href="#">NTP-U187 Back Up the Software Database, page 4</a>
<b>Required/As Needed</b>	Required for BLSR only
<b>Onsite/Remote</b>	Onsite or remote (but in the presence of the workstation)
<b>Security Level</b>	Superuser



**Note** During 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 you must be sure to remove the lockout after you have 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-48, OC-192), perform the following steps:

- Next to the trunk card row, click the **East Switch** column to show the drop-down list.
- From the menu options, choose **Lockout Span**.
- Click **Apply**.
- In the same row, click the **West Switch** column to show the drop-down list.
- From the menu options, choose **Lockout Span**.
- Click **Apply**.

**Note**

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

**Note**

Certain BLSR or Multiservice Switching Platform (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.

- BLSROSYNC (MN)
- RING-MISMATCH (MJ)
- APSCDFLTK (MN)
- BLSR-RESYNC (NA)
- BLSR-SW-VER-MISM



**Step 3** Return to your originating procedure (NTP).

## DLP-U282 Download the Software

<b>Purpose</b>	This task downloads the software to the ONS 15600 nodes.
<b>Tools/Equipment</b>	PC or UNIX workstation
<b>Prerequisite Procedures</b>	<a href="#">NTP-U187 Back Up the Software Database, page 4</a>
<b>Required/As Needed</b>	Required
<b>Onsite/Remote</b>	Onsite or remote (but in the presence of the workstation)
<b>Security Level</b>	Superuser

**Note**

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.

- 
- Step 1** From the View menu, choose **Go To Network View**.
- Step 2** Verify that the alarm filter is not on:
- Click the **Alarms** tab.
  - Click the Filter tool at the lower-right side of the bottom toolbar.  
Alarm filtering is enabled if the tool is 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. If necessary, refer to the *Cisco ONS 15600 Troubleshooting Guide*.
- Step 4** From the View menu, choose **Go to Home View**.
- Step 5** Verify that the TSC card in Slot 10 is the active card. If it is not, complete the following:
- Right-click the TSC in Slot 5 and choose **Soft-reset Card**.
  - Click **Yes** in the confirmation dialog box.
  - Click **OK** in the Connection Lost dialog box.
-  **Note** The TSC card takes several minutes to reboot.
- 
- Step 6** Double-click the node icon to return to node view.
- Step 7** Click the **Maintenance > Software** tabs.
- Step 8** Click **Download**. The Download Selection dialog box appears.
- Step 9** Click **Browse**.
- Step 10** In the Open dialog box, navigate to the software package files on the ONS 15600 software CD or on your hard drive, if you are working from a local copy.
- Step 11** Select the file with the .pkg extension and click **Open**.
- Step 12** In the Download Selection dialog box, verify that the node is checked.
- Step 13** Click **OK**. The software begins downloading to the active TSC card. The Download Status column on the Maintenance > Software tab shows the percentages complete:
- Downloading (approximately 7 to 10 minutes)
  - Qualifying (approximately 1 to 2 minutes)
  - Copying to stby TSC (approximately 2 to 5 minutes)
- When the Download Status column is empty, the software has finished loading.
- Step 14** Verify the version:
- Click **Info**.
  - In the Current Software Info dialog box, verify that the TSC B Working field shows 5.x and the TSC B Protect field shows 7.2.
  - Click **OK**.
-  **Note** You can also verify the load information on the Maintenance > Software tab. The Working Version column shows the original software load and the Protect Version column shows the software load that you just downloaded.
- 
- Step 15** Repeat Steps 1 through 14 for each node.



**Note** The software download process can take 15 minutes or more per node.

**Step 16** Return to your originating procedure (NTP).

## DLP-U283 Activate the New Load

<b>Purpose</b>	This task activates Software R7.2 in each node in the network. Activating the software load downloads the software to the standby TSC <sup>1</sup> .
<b>Tools/Equipment</b>	PC or UNIX workstation
<b>Prerequisite Procedures</b>	<a href="#">NTP-U187 Back Up the Software Database, page 4</a> <a href="#">DLP-U282 Download the Software, page 8</a>
<b>Required/As Needed</b>	Required
<b>Onsite/Remote</b>	Onsite or remote (but in the presence of the workstation)
<b>Security Level</b>	Superuser

1. If you have downloaded the software into the protect side of the TSC card and want to activate (or revert) it at a later time, the Activate (or Revert) buttons may be grayed out. This occurs when the Cisco ONS 15600 node detects the software in the protect side of the TSC as invalid. In order to activate (or revert) the software, download the software to the TSC card once again.



**Note** Although the activate task is not service affecting, Cisco recommends that you activate the new load during a maintenance window.



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



**Note** For BLSRs only, a non-service affecting APS-CHAN-FAILURE alarm is raised on each of the nodes joined to an activating node in the ring during activation. Once the activation completes for that node, the alarms will clear.






**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.

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

**Step 2** Verify the version:

- a. Click **Info**.
- b. In the Current Software Info dialog box, verify that the TSC B Working shows R5.x and the TSC B Protect shows R7.2.
- c. Click **OK**.

- Step 3** Click **Activate**. The Activate dialog box appears with a warning message indicating that you should perform a database backup.
- Step 4** Complete one of the following:
- If you have not backed up the Software R5.x database, click **No**. Complete the “[NTP-U187 Back Up the Software Database](#)” procedure on page 4. When you have completed the procedure, return to Step 3 in this task.
  - If you have backed up the Software R5.x database, click **Yes** to proceed with the activation. The Download Status column shows:
    - The Qualifying percentage completed (approximately 1 to 2 minutes).
    - The status “Wait” while the standby TSC reboots (approximately 2 to 5 minutes). When the standby TSC completes the reboot, it is still in standby but is now running Software R7.2. The active TSC in Slot 10 is still active and is running Software R5.x.
    - The Acquiring percentage completed as the standby TSC acquires the active timing reference (approximately 10 to 15 minutes).
- Step 5** Click **OK** when the Rebooting message appears indicating that the software is successfully activated. The node reboot could take up to four minutes.
- Step 6** Click **OK** in the Connection Lost dialog box.
-  **Note** CTC loses connection to the node while the node reboots and displays the network view.
- Step 7** After activating the node, the software upgrade reboot occurs as follows.( The node will remain gray for the remainder of this task.)
- When the active TSC card in Slot 10 reboots, the TSC card in Slot 5 becomes active, using Software R7.2 as the working copy. When the TSC card in Slot 10 resets, it is in standby mode and is still running Software R5.x. All remaining cards in the shelf reset simultaneously.
  - A system reboot (SYSBOOT) alarm is raised briefly while activation is in progress. When all cards have reset, this alarm clears.
- 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 8** In CTC, choose **File > Exit**.
- Step 9** In your browser window, click the **Delete CTC Cache** button.
-  **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-U253 Delete Cached JAR Files](#)” task on page 12.
- Step 10** Close your browser.
- Step 11** Install the new JRE version and (optionally) run the Cache Loader pre-caching utility:



**Note** Cisco recommends you run the optional Cache Loader pre-caching utility during this step, prior to activating the node. This ensures that the new CTC JAR files download to your workstation as quickly as possible.

- a. In your Windows environment, choose **Start > Settings > Control Panel**, and click **Add/Remove Programs**.
- b. Scroll the list of programs until you see the Java 2 Runtime Environment, then click **Change/Remove**.
- c. Click **Yes** in the dialog box to proceed with removing the old JRE version.
- a. Load the Release 7.2 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 appears.
- e. Select **Cisco Transport Controller, Java Runtime Environment 1.4.2**, and (optionally) **CTC JAR files**. Deselect any other preselected options.
- f. Click **Next**. A confirmation box appears.
- g. Click **Next** again. The (optional) CTC Cache Loader pre-caches the JAR files to your workstation, displaying a progress status box, and installs the JRE.
- h. When the installation finishes, click **OK**, and then in the wizard, click **Finish**.

**Step 12** Reopen your browser.

**Step 13** Return to your originating procedure (NTP).

## DLP-U253 Delete Cached JAR Files

<b>Purpose</b>	This task deletes previously cached files from your browser and hard drive.
<b>Tools/Equipment</b>	PC or UNIX workstation
<b>Prerequisite Procedures</b>	None
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote (but in the presence of the workstation)
<b>Security Level</b>	None

**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.

You will not be able to 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** (Windows systems only) Delete cached files from your workstation.

- 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 path you just looked up.
- 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-U284 Install the Public-Key Security Certificate

<b>Purpose</b>	This task installs the ITU Recommendation X.509 public-key security certificate. The public-key certificate is required to run Software R5.0 or later.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-U283 Activate the New Load, page 10</a>
<b>Required/As Needed</b>	Required
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	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 SDH.
- **Deny**—Denies permission to install the certificate. If you choose this option, you cannot log into the ONS 15454 SDH.

- 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.

**Step 3** Return to your originating procedure (NTP).

---

## DLP-U285 Accept the New Load

<b>Purpose</b>	This task upgrades the standby TSC.
<b>Tools/Equipment</b>	PC or UNIX workstation
<b>Prerequisite Procedures</b>	<a href="#">DLP-U283 Activate the New Load, page 10</a>
<b>Required/As Needed</b>	Required
<b>Onsite/Remote</b>	Onsite or remote (but in the presence of the workstation)
<b>Security Level</b>	Superuser

---

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

**Step 2** Click **Accept**. This process takes approximately 2 to 5 minutes.



**Note** You can reject the new software load by clicking **Cancel**. The Cancel button resets the active TSC card in Slot 5. The TSC card in Slot 10 then becomes the active TSC using Software R7.x as the working copy. After the TSC card in Slot 5 resets, it becomes the standby TSC and begins using Software R7.x.

---



**Note** If the Cancel button is not active, the standby TSC has not finished acquiring the active timing reference. The acquire process can take approximately 10 to 15 minutes. When the acquire process completes, the Cancel button becomes active.

---

**Step 3** Verify the version:

- Click **Info**.
- In the Current Software Info dialog box, verify that the TSC B Working field shows the correct version. The TSC B Protect field should show the previous version.
- If the TSC B Working and TSC B Protect fields show “none,” click **OK** and click the **Info** button again after several minutes. Repeat until the TSC B software versions appear.
- Click **OK**.

**Step 4** Return to your originating procedure (NTP).

---

## DLP-U286 Remove the BLSR Lockout

<b>Purpose</b>	Release the span lockouts on all BLSR nodes. Complete this task after the new software load is activated on all nodes.
<b>Tools/Equipment</b>	PC or UNIX workstation
<b>Prerequisite Procedures</b>	<a href="#">DLP-U283 Activate the New Load, page 10</a>
<b>Required/As Needed</b>	Required for BLSR
<b>Onsite/Remote</b>	Onsite or remote (but in the presence of the workstation)
<b>Security Level</b>	Superuser

- 
- Step 1** In CTC node view, click the **Maintenance > BLSR** tabs.
- Step 2** For each of the BLSR trunk (span) cards (OC-48, or OC-192), perform the following steps:
- Next to the trunk card row, click the **West Switch** column to show the drop-down list.
  - Choose **Clear** from the list
  - 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.

- In the same row, click the **East Switch** column to show the drop-down list.
  - Choose **Clear** from the list.
  - 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-U94 Set the Date and Time

<b>Purpose</b>	This task resets the date and time at each node.
<b>Tools/Equipment</b>	PC or UNIX workstation
<b>Prerequisite Procedures</b>	None
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote (but in the presence of the workstation)
<b>Security Level</b>	Superuser



**Note** If you are not using SNTP, the upgrade procedure can cause the date and time setting to change. If you are using SNTP, you do not need to perform this task.

- 
- Step 1** In 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-U189 Restore the Previous Software Load and Database

<b>Purpose</b>	This procedure returns the node to the software and database provisioning you had before you activated Software R7.2.
<b>Tools/Equipment</b>	PC or UNIX workstation
<b>Prerequisite Procedures</b>	<a href="#">NTP-U186 Prepare for the Release 7.2 Upgrade, page 3</a> <a href="#">NTP-U187 Back Up the Software Database, page 4</a> <a href="#">NTP-U188 Upgrade to Release 7.2, page 6</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote (but in the presence of the workstation)
<b>Security Level</b>	Superuser



**Note**

The tasks to downgrade to a previous load are not a part of the upgrade. They are provided here as a convenience to those wishing to restore an earlier software load 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 Release 7.2 software, you should have backed up the existing database at all nodes in the network (using the “[NTP-U187 Back Up the Software Database](#)” procedure on page 4). Cisco recommends that you record or export all critical information to your hard drive.

---



**Caution**

Downgrades are service affecting.

---



**Caution**

If any IPIOs have been installed in an ASAP card after an upgrade to Release 7.2, you must delete them from the database, and then physically remove them from the node prior to reverting to a release that does not support the IPIO; then wait for CTC to update showing the card is removed before proceeding with the revert.

---



**Note**

A system-wide soft reset occurs after the database is restored. All line (I/O) and matrix (SSXC) cards automatically soft reset. Existing traffic can be affected, depending on the circuit provisioning map.

---

- Step 1** Log into the node. For detailed instructions, refer to the *Cisco ONS 15600 Procedure Guide*. If you are already logged in, continue with Step 2.

**Note**

To perform a downgrade from Software R7.2, Software R5.x or 6.x must have been working at the time you activated to Software R7.2 on that node. Also, a supported revert 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.

**Step 2** (BLSR nodes only) Complete the [“DLP-U281 Perform a BLSR Lockout” task on page 7](#).

**Note**

The BLSR lockout must be completed for all nodes in all rings for which the ONS 15600 is provisioned.

**Step 3** Complete the [“DLP-U282 Download the Software” task on page 8](#).

**Step 4** Click **Revert**. The Database Restore dialog box appears.

**Step 5** Click **Browse**.

**Step 6** In the Open dialog box, navigate to a local PC directory or network directory where the database file is stored and click **Open**.

**Step 7** If alarms and performance were backed up, check the **Alarms** and **Performance** check boxes in the Database Restore dialog box.

**Step 8** Click **OK**.

**Step 9** Click **Yes** in the confirmation dialog box.

**Step 10** Wait until the software download finishes. The Download Status column shows:

- The Qualifying percentage completed (approximately 1 to 2 minutes)
- The status “Wait” while the standby TSC reboots (approximately 2 to 5 minutes)
- The Acquiring percentage completed as the standby TSC acquires the active timing reference (approximately 10 to 15 minutes)

The ONS 15600 then reboots.

**Step 11** Complete the [“DLP-U286 Remove the BLSR Lockout” task on page 15](#) for all BLSR nodes in the network.

**Step 12** Complete the [“DLP-U285 Accept the New Load” task on page 14](#).

**Step 13** Repeat Steps 1 through 12 for any other nodes you want to downgrade.

**Stop. You have completed this procedure.**

## Related Documentation

Use this document in conjunction with the following publications:

- *Cisco ONS 15600 Procedure Guide*  
Provides installation, turn up, test, and maintenance procedures
- *Cisco ONS 15600 Reference Manual*  
Provides technical reference information for cards, nodes, and networks

- *Cisco ONS 15600 Troubleshooting Guide*  
Provides a list of 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, ONS 15310-CL, and ONS 15310-MA systems
- *Release Notes for Cisco ONS 15600 Release 7.2*  
Provides caveats, closed issues, and new feature and functionality information

## Where to Find Safety and Warning Information

For safety and warning information, refer to the *Cisco Optical Transport Products Safety and Compliance Information* document that accompanied the product. This publication describes the international agency compliance and safety information for the Cisco ONS 15600 systems. It also includes translations of the safety warnings that appear in the ONS 15600 system documentation.

## Obtaining Documentation

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

### Cisco.com

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

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

## Product Documentation DVD

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

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

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

## Cisco Optical Networking Product Documentation CD-ROM

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

## Ordering Documentation

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

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

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

## Documentation Feedback

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

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

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

We appreciate your comments.

## Cisco Product Security Overview

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

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

From this site, you will find information about how to:

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

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

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

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

[http://www.cisco.com/en/US/products/products\\_psirt\\_rss\\_feed.html](http://www.cisco.com/en/US/products/products_psirt_rss_feed.html)

## Reporting Security Problems in Cisco Products

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

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

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

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

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

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



### Tip

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

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

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

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

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

## Obtaining Technical Assistance

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

## Cisco Technical Support & Documentation Website

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

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

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

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

**Note**

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

## Submitting a Service Request

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

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

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

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

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

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

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

## Definitions of Service Request Severity

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

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

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

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

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

## Obtaining Additional Publications and Information

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

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

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

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

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

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

<http://www.ciscopress.com>

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

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

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

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

or view the digital edition at this URL:

<http://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.



Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

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

