Upgrading the Cisco ONS 15600 to Release 8.0

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) from Software Release 5.0.x, Software Release 6.x, or Software Release 7.x to Software Release 8.0, using the Timing and Shelf Controller (TSC) card. The ONS 15600 supports errorless upgrades.

Contents

This document contains the following information:

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. This data will be useful during and after the upgrade.

Caution Before beginning an upgrade of an ONS 15600 from Software R5.x, contact the Cisco Technical Assistance Center (TAC) for system verification. See the "Obtaining Documentation and Submitting a Service Request" section on page 25 for Cisco TAC contact information. This step is not necessary if you are upgrading from Software R6.0 or later.

Caution Read each procedure before you begin the upgrade.

Caution Software R8.0 does not support upgrade from SONET Software R1.1.x or Software R1.3.x, to Software R8.0.

Note Software R8.0 supports parallel upgrades for multiple nodes in a network. In a parallel upgrade you can still activate only 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 Non Trouble Procedures (NTPs). An NTP will, in most cases, refer to one or more related Detail Level Procedures (DLP).

Each NTP contains a list of steps designed to accomplish a specific task. Follow the steps until the task is complete. For a craftsperson requiring more detailed instructions, the NTP might refer to the steps in the DLP. Some steps might require that equipment indications be checked for verification.

The following NTPs are contained in this document:

1. NTP-U219 Prepare for the Release 8.0 Upgrade, page 3—This procedure contains critical information and tasks that you must read and complete before beginning the upgrade process.

2. NTP-U220 Back Up the Software Database, page 5—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-U221 Upgrade to ONS 15600 Release 8.0, page 6—You must complete this entire procedure to complete the upgrade.
4. NTP-U222 Restore the Previous Software Load and Database, page 17—Complete this procedure if you need to return to the previous software load.
5. "NTP-U223 Upgrade to ONS 15600 Release 8.0 Using TL1" procedure on page 19—Complete this procedure to install the ONS 15600 software using Transaction Language 1 (TL1).

NTP-U219 Prepare for the Release 8.0 Upgrade

Purpose	This procedure steps you through the critical information checks and tasks you must complete before beginning an upgrade.
Tools/Equipment	PC or UNIX workstation; Cisco ONS 15600 Software R8.0 (CD or soft copy)
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 Read the *Release Notes for Cisco ONS 15600 Release 8.0*.

Step 2 Using the CTC software, log into the node that you will upgrade. For detailed instructions, refer to the *Cisco ONS 15600 Procedure Guide*.

Step 3 Complete the "DLP-U328 Verify CTC Workstation Requirements" task on page 4.

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).

Note If you have multiple IP addresses on your workstation, you should remove them; you cannot run Software R8.0 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 If the TSC in Slot 5 is active, select the slot, and right-click to display a menu. Click **Soft reset Card**. The reset takes a few minutes, and resets the TSC card in Slot 10 as the active TSC.

Step 7 Complete the "NTP-U220 Back Up the Software Database" procedure on page 5.

Stop. You have completed this procedure.

DLP-U328 Verify CTC Workstation Requirements

Purpose	This task verifies that all PC or UNIX workstation hardware and software requirements are met.
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 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 Java Runtime Environment (JRE) JRE 5.0 and Java Plug-in 5.0 are both installed.

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 To install JRE 5.0, the Java Policy file, or the Software R8.0 online help, refer to the installation instructions in the *Cisco ONS 15600 Procedure Guide*.

Step 6 Return to your originating procedure (NTP).

NTP-U220 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-U219 Prepare for the Release 8.0 Upgrade, page 3
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of the workstation)
Security Level	Superuser

Note (BLSR nodes only) The database must be backed up prior to locking the Bidirectional Line Switched Ring (BLSR).

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 CTC node view, click the **Maintenance** tab and then click the **Software** button.

Step 3 Verify that the correct working and protect versions of the software are installed.

Step 4 In CTC node view, click the **Maintenance** tab and then click the **Database** button.

Step 5 Click **Backup**.

Step 6 Click the **Save** button to save the database on the workstation's hard drive or on network storage. Use an appropriate file name with the file extension.db. (Cisco recommends that you use the IP address of the node and the date, for example 10101281920611O7.db.)

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** and the **Performance** check boxes in order to choose these database items in addition to provisioning information.

Note Provisioning is a default component of the backup file, and is dimmed.

Step 9 In the Database Backup dialog box, click **OK**.

Step 10 A message indicates the status of the backup. When the backup is complete, click the **OK** button to close the message dialog box.

Step 11 Repeat Steps 1 through 10 for each node in the network.

Step 12 (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	
Data Communications Channel (DCC) 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 TSC **Note** 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-U221 Upgrade to ONS 15600 Release 8.0

Purpose	This procedure upgrades your software to Software R8.0.
Tools/Equipment	PC or UNIX workstation; Cisco ONS 15600 Software R8.0 (CD or soft copy)
Prerequisite Procedures	NTP-U220 Back Up the Software Database, page 5 (BLSR nodes only) The database must be backed up prior to locking the BLSR.
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of the workstation)
Security Level	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 R8.0 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 the Cancel button 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-U329 Perform a BLSR Lockout" task on page 8.

Warning **The BLSR lockout must be completed for all nodes in all rings for which the ONS 15600 is provisioned. The database must be backed up prior to locking the BLSR.**

Step 4 Back up the database. See "NTP-U220 Back Up the Software Database" procedure on page 5 for details.

Step 5 Complete the "DLP-U330 Download the ONS 15600 Release 8.0 Software" task on page 9.

Step 6 Complete the "DLP-U331 Activate the ONS 15600 Release 8.0 Software Load" task on page 11.

Step 7 (As needed) Complete the "DLP-U332 Delete Cached JAR Files" task on page 13.

Note The "DLP-U332 Delete Cached JAR Files" task on page 13 is provided in case you have trouble logging back into a node after the activation. This task is not generally necessary.

Step 8 Reconnect to the node using CTC. The new CTC applet for Software R8.0 uploads.

Step 9 During CTC login, complete the "DLP-U333 Install the Public-Key Security Certificate" task on page 14.

Step 10 Complete the "DLP-U334 Accept the New Load" task on page 15.

Note After you have accepted the Software R8.0 build on both Working and Protect TSC cards, you cannot revert to the pre-upgrade software without downloading the pre-upgrade software version again and restoring the appropriate database.

Step 11 Repeat Steps 6 through 10 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.

Step 12 Complete the "DLP-U335 Remove the BLSR Lockout" task on page 15 for all BLSR nodes in the network.

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 (wait 5 minutes from the time when the SYSBOOT alarm is raised). The database must be backed up prior to locking the BLSR.

Step 13 (Optional) If you wish to ensure that a software revert to the previous software release will no longer be possible, complete the "DLP-U330 Download the ONS 15600 Release 8.0 Software" task on page 9.

Step 14 Complete the "DLP-U336 Set the Date and Time" task on page 16 for any nodes that are not using Simple Network Time Protocol (SNTP).

Step 15 Complete the "DLP-U334 Accept the New Load" task on page 15 to accept the load.

Step 16 As needed, upgrade any spare TSC cards by installing the spare in the standby slot of a Software R8.0 node.

Caution 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 17 To back up the Software R8.0 database for the Working software load, see "NTP-U220 Back Up the Software Database" procedure on page 5 in order to preserve the database for the R8.0 software.

Stop. You have completed this procedure.

DLP-U329 Perform a BLSR Lockout

Purpose	If you have a BLSR provisioned, before beginning the upgrade you must perform a span lockout at each node in the ring. The database must be backed up prior to locking the BLSR.
Tools/Equipment	PC or UNIX workstation, Software R8.0 files
Prerequisite Procedures	NTP-U220 Back Up the Software Database, page 5 (BLSR nodes only) The database must be backed up prior to locking the ring.
Required/As Needed	Required for BLSR only
Onsite/Remote	Onsite or remote (but in the presence of the workstation)
Security Level	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. The database must be backed up prior to locking the BLSR.

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

Step 1 Back up the database. See "NTP-U220 Back Up the Software Database" procedure on page 5 for details.

Step 2 In node view, click the **Maintenance** tab, and click the **BLSR** button.

Step 3 For each of the BLSR trunk (span) cards (OC-48, OC-192), perform the following steps:

a. Next to the trunk card row, click the East Switch column to show the drop-down list.

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

c. Click **Apply**.

d. In the same row, click the West Switch column to show the drop-down list.

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

f. 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 4 Return to your originating procedure (NTP).

DLP-U330 Download the ONS 15600 Release 8.0 Software

Purpose	This task downloads the software to the ONS 15600 nodes.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-U220 Back Up the Software Database, page 5
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of the workstation)
Security Level	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 If CTC is not already running, start CTC.

Step 2 In CTC node view, click the **Alarms** tab.

Step 3 Verify that the alarm filter is not on. Click the **Filter** tool at the lower-left of the window.

Step 4 The Alarm Filter dialog box appears. Click to deselect any selections in the Show Severity section of the **General** tab.

Step 5 On the **Alarms** tab, check all nodes for existing alarms. Resolve any outstanding critical alarms before proceeding. If necessary, refer to the *Cisco ONS 15600 Troubleshooting Guide*.

Step 6 Verify that the TSC card in Slot 10 is the active card. If it is not, complete the following:

a. Right-click the TSC in Slot 5 and choose **Soft-reset Card**.

b. Click **Yes** in the confirmation dialog box.

c. Click **OK** in the Connection Lost dialog box.

Note The TSC card takes several minutes to reboot.

Step 7 If the display is not in node view, double-click the node icon to return to node view.

Step 8 Click the **Maintenance** tab and then click the **Software** button.

Step 9 Click **Download**. The Download Selection dialog box appears.

Step 10 Click the **Browse** button.

Step 11 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 12 Click the file with the PKG extension and click **Open**.

Step 13 In the Download Selection dialog box, verify that the node is selected. The TSC card in Slot 10 becomes highlighted.

Step 14 Click **OK**.

Step 15 Select the **History** tab to view the conditions:

1. Downloading (approximately 10 to 20 minutes)
2. System Upgrade in progress (approximately 3 to 5 minutes)

Step 16 Click the **Maintenance** tab, and click the **Software** button. When the Download Status column is empty, the software has finished loading.

Step 17 Verify that the Working Version field shows the pre-upgrade software version and that the Protect Version field shows R8.0. Click **OK**.

Step 18 Repeat Steps 1 through 17 for each node.

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

Step 19 Return to your originating procedure (NTP).

DLP-U331 Activate the ONS 15600 Release 8.0 Software Load

Purpose	This task activates Software R8.0 in each node in the network. Activating the software load downloads the software to the standby TSC[1].
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-U220 Back Up the Software Database, page 5 DLP-U330 Download the ONS 15600 Release 8.0 Software, page 9
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of the workstation)
Security Level	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 BLSR rings 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. After 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 If CTC is not already running, start CTC.

Step 2 In CTC node view, click the **Maintenance** tab and then click the **Software** button.

Step 3 Verify that the version in the Protect Version column is R8.0.

Step 4 Click the **Activate** button. The Activate dialog box appears with a warning message indicating that you should perform a database backup.

Step 5 Complete one of the following:

- If you have not backed up the database for the Working TSC B, click **No**. Complete the "NTP-U220 Back Up the Software Database" procedure on page 5. When you have completed the procedure, return to Step 4 in this task.
- If you have backed up the database for the Working TSC B, click **Yes** to proceed with the activation. The Download Status column shows:

  - A Qualifying message, indicating the percentage of qualification completed (approximately 1 to 2 minutes).
  - A Wait message, generated when the standby TSC card containing the upgrade software reboots. It signals to the active TSC card that it is ready to take over. When the active TSC receives this signal, it resets itself, and the standby TSC in Slot 5 takes over and transitions to the active software version. The pre-upgrade version of the TSC card is now the standby TSC.
  - An Acquiring message, indicating the percentage completed as the standby TSC acquires the active timing reference (approximately 10 to 15 minutes).

- Click **OK** when the Rebooting dialog box appears, indicating that the software is successfully activated. The node might take several minutes to reboot.

Step 6 A Connection Lost dialog box appears, indicating that the connection between the node and CTC is not currently active. Click **OK** in the Connection Lost dialog box.

Note CTC loses connection to the node while the node reboots and displays the network view. The node might take several minutes to reboot. A Minor loss of connection between the node and CTC alarm displays in the History tab. Next, a CTC and node incompatible alarm raises. Wait for node reactivation.

Step 7 In CTC, choose **File > Exit** to exit, or continue to Step 8 to delete the CTC cache.

Step 8 In CTC Launcher 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-U332 Delete Cached JAR Files" task on page 13.

Step 9 Close your browser.

Step 10 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**, then click **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 Software R8.0 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. Click **Cisco Transport Controller**, **Java Runtime Environment 5.0**, and (optionally) **CTC JAR files**. Deselect any other preselected options.

f. Click **Next**. A confirmation dialog 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 11 Reopen your browser, using the IP address from Step 1.

Step 12 Return to your originating procedure (NTP).

DLP-U332 Delete Cached JAR Files

Purpose	This task deletes previously cached files from your browser and hard drive.
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	None

Step 1 Delete cache files from your browser directory.

In Netscape:

a. Choose **Edit > Preferences,** click the **Advanced tab** and then click the **Cache** button.

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** and then click the **General** tab.

b. Click **Delete Files**.

c. Click 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 the Windows **Start** menu, choose **Control Panel > System** and click the **Advanced** tab.

b. Click the **Environment Variables** button. The resulting dialog box 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. Click to 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-U333 Install the Public-Key Security Certificate

Purpose	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.
Tools/Equipment	None
Prerequisite Procedures	DLP-U331 Activate the ONS 15600 Release 8.0 Software Load, page 11
Required/As Needed	Required
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 15600.
- Deny—Denies permission to install the certificate. If you choose this option, you cannot log into the ONS 15600.
- 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-U334 Accept the New Load

Purpose	This task upgrades the standby TSC.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	DLP-U331 Activate the ONS 15600 Release 8.0 Software Load, page 11
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of the workstation)
Security Level	Superuser

Step 1 In node view, click the **Maintenance** tab and then click the **Software** button.

Step 2 Click the **Accept** button. The process takes approximately 2 to 5 minutes.

Note You can reject the new software load by clicking the Cancel button. The Cancel button resets the active TSC card in Slot 5. The TSC card in Slot 10 then becomes the active TSC, using the pre-upgrade software version.

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:

a. Click **Info**.

b. 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.

c. 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.

d. Click **OK**.

Step 4 Return to your originating procedure (NTP).

DLP-U335 Remove the BLSR Lockout

Purpose	Release the span lockouts on all BLSR nodes. Complete this task after the new software load is activated on all nodes.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	DLP-U331 Activate the ONS 15600 Release 8.0 Software Load, page 11
Required/As Needed	Required for BLSR
Onsite/Remote	Onsite or remote (but in the presence of the workstation)
Security Level	Superuser

Step 1 If CTC is not already running, start CTC.

Step 2 In CTC node view, click the **Maintenance** tab, and click the **BLSR** button.

Step 3 For each of the BLSR trunk (span) cards (OC-48, or OC-192), perform the following steps:

a. Next to the trunk card row, click the West Switch column to show the drop-down list.

b. From the drop-down menu, select **Lockout Protect**.

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.

a. In the same row, click the East Switch column to show the drop-down list.

b. From the drop-down menu, click **Lockout Protect**.

Step 4 Repeat this task as many times as necessary to remove all BLSR span lockouts on the upgrade nodes.

Step 5 Return to your originating procedure (NTP).

DLP-U336 Set the Date and Time

Purpose	This task resets 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 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** tab, and click the **General** button.

Step 2 Set the correct date and time, then click the **Apply** button.

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

Step 4 Return to your originating procedure (NTP).

NTP-U222 Restore the Previous Software Load and Database

Purpose	This procedure returns the node to the software and database provisioning you had before you activated Software R8.0.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-U219 Prepare for the Release 8.0 Upgrade, page 3 NTP-U220 Back Up the Software Database, page 5 NTP-U221 Upgrade to ONS 15600 Release 8.0, page 6
Required/As Needed	As needed
Onsite/Remote	Onsite or remote (but in the presence of the workstation)
Security Level	Superuser

Note If both the Working and Protect TSC cards are loaded with Software 8.0, you cannot revert to a previous software version.

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 R8.0 software, you should have backed up the existing database at all nodes in the network (using the "NTP-U220 Back Up the Software Database" procedure on page 5). Cisco recommends that you record or export all critical information to your hard drive.

Caution Downgrades are service affecting.

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 Using CTC, 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.

Step 2 Back up the database. See "NTP-U220 Back Up the Software Database" procedure on page 5 for details.

Note To perform a downgrade from Software R8.0, the pre-upgrade software must have been working at the time you activated to Software R8.0 on that node. Also, a supported reversion 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 3 (BLSR nodes only) Complete the "DLP-U329 Perform a BLSR Lockout" task on page 8.

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

Step 4 For software reversion to a previous version only, complete the "DLP-U330 Download the ONS 15600 Release 8.0 Software" task on page 9.

Step 5 For a software reversion and/or a database restore click **Revert**. The Database Restore dialog box appears.

Step 6 Click the **Browse** button.

Note To restore the database only, without reverting the software version, select the database that you backed up prior to the BLSR lockout. To restore the database for a reverted software version, select the database for the reverted version.

Step 7 In the Open dialog box, navigate to a local PC directory or network directory where the database file is stored and click the **Open** button.

Step 8 If alarms and performance were backed up, check the **Alarms** and **Performance** check boxes in the Database Restore dialog box.

Step 9 Click **OK**.

Step 10 Click **Yes** in the confirmation dialog box.

Step 11 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 12 Complete the "DLP-U335 Remove the BLSR Lockout" task on page 15 for all BLSR nodes in the network.

Step 13 Complete the "DLP-U334 Accept the New Load" task on page 15.

Step 14 Repeat Steps 1 through 13 for any other nodes you want to downgrade.

Stop. You have completed this procedure.

NTP-U223 Upgrade to ONS 15600 Release 8.0 Using TL1

Purpose	This procedure upgrades the software to Software R8.0 using TL1, rather than CTC.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-U219 Prepare for the Release 8.0 Upgrade, page 3 NTP-U220 Back Up the Software Database, page 5
Required/As Needed	Optional
Onsite/Remote	Onsite or remote (but in the presence of the workstation)
Security Level	Superuser

Note This procedure assumes that you are upgrading using Release 6.x TL1 syntax. TL1 commands issued prior to software activation to ONS 15600 Software R8.0 will vary in syntax depending on the ONS 15600 release that you are 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
- APPLY
- CANC
- COPY-RFILE
- REPT EVT FXFR
- OPR-PROTNSW-<OCN_TYPE>
- RTRV-COND-ALL
- RTRV-ALM-ALL

Note To perform a Software R8.0 download using TL1, you must first have an FTP server or a terminal emulation program like HyperTerminal running on your workstation.

Note In the following conditions, the download (COPY-RFILE) command is different when downloading software to a gateway network element (GNE) or an end network element (ENE):

- - FTP is being used.
- - The server is set up with a login and password of FTPUSER1 and FTPUSERPASSWORD1.
- - The FTP server has an IP address of 10.1.1.1.
- - The FTP server is running on the standard FTP port.
- - The software package is called “15600-03xx-A04K-1405.pkg

The GNE and ENE commands are as follows:

- When downloading software to a GNE, use a command similar to:

```
COPY-RFILE:NODENAME:RFILE-PKG:CTAG::TYPE=SWDL,
SRC="ftp://FTPUSER1:FTPUSERPASSWORD1@10.1.1.1/15600-03xx-A04K-1405.pkg";
```

- When downloading Software to an ENE, use a command similar to:

```
COPY-RFILE:NODENAME:RFILE-PKG:CTAG::TYPE=SWDL,
SRC="ftp://FTPUSER1:FTPUSERPASSWORD1@10.111.11.1:2361@90.90.90.90/15600-03xx-A04K-1405
.pkg";
```

The ":2361" after the FTP server IP address 10.111.11.1 denotes port 2361 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 package resides between the last IP address and the PKG file in the command line. An example is shown here.

```
COPY:NODENAME:RFILE-PKG:CTAG::TYPE=SWDL,
SRC="ftp://FTPUSER1:FTPUSERPASSWORD1@10.1.1.1:2361@90.90.90.90/CISCO/SOFTWARE/15600-03
xx-A04K-1405.pkg";
```

Step 1 To use TL1 commands, set up an FTP session or use HyperTerminal or a similar terminal emulation package to establish a session with the ONS 15600 node.

Step 2 Type the IP address for the node, using port 3083 or 2361.

The terminal emulation interface will display a Warning message and a command prompt (usually >). You will issue TL1 commands at this prompt.

Step 3 Type the **ACT-USER** (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 (optional).
- <UID> is the Operations Support System (OSS) profile username (required).
- <CTAG> is the correlation tag that correlates command and response messages (optional).
- <PID> is the password identifier (required).

For example, in the TL1 command:

```
ACT-USER::CISCO99:100::PASSWORD;
```

ACT-USER is the activation command, CISCO99 is the user ID, 100 is the correlation tag (used to correlate commands to command responses), and PASSWORD is the password associated with the user ID.

A response message containing the CTAG that you specified indicates the completion status of the command.

Step 4 Select the IP address for the node, using port 3083 or 2361.

Step 5 Type the **COPY-RFILE** command in the TL1 window or, if using HyperTerminal, Select **Transfer** > **Receive File**, and use the associated dialog box to click on a file to receive. 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 TSC cards.

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

where:

- <TID> is the target identifier (optional).
- <SRC> is the source AID (required).
- <CTAG> is the correlation tag that correlates command and response messages (optional).
- <TYPE> is the file transfer protocol (required).
- <SRC1> specifies the source of the file to be transferred (required).
- <DEST> is the destination of the file to be transferred (required).
- <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 (required).
- <FTTD> is the URL format (required).

Step 6 Repeat Step 5 for all nodes to be upgraded.

Step 7 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 software download. REPT EVT FXFR also reports any failure during the software upgrade, including invalid package, invalid path, invalid user ID/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 8 Complete NTP-U219 Prepare for the Release 8.0 Upgrade, page 3 for each node to be upgraded.

Step 9 Complete NTP-U220 Back Up the Software Database, page 5 for each node to be upgraded.

Step 10 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:

- <TID> is the target identifier (optional).
- <AID> is the Access IDentifier (indicating the facility in the node to which the switch request is directed).
- <CTAG> is the message correlation tag, used to correlate messages and responses.
- <SC> is the switch command that is to be initiated on the paths.
- <SWITCHTYPE> is the 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 time slots during the lockout.

Note Certain BLSR-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 11 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:

- <TID> is the target identifier (optional).
- <AID> is the Access IDentifier (indicating the facility in the node to which the switch request is directed).
- <CTAG> is the message correlation tag, used to correlate messages and responses.

Step 12 Verify that there are no outstanding alarms or conditions on each node using the following commands:

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

where:

- <TID> is the target identifier (optional).
- <AID> is the Access IDentifier (indicating the facility in the node to which the switch request is directed).
- <CTAG> is the message correlation tag, used to correlate messages and responses.
- <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:

- <TID> is the target identifier (optional).
- <AID> is the Access IDentifier (indicating the facility in the node to which the switch request is directed).
- <CTAG> is the message correlation tag, used to correlate messages and responses.
- <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 remotely, wait five minutes for the controller cards to complete the reboot.

Step 13 Starting at the node farthest 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 message correlation tag, used to correlate messages and responses.
- <MEM_SW_TYPE> indicates a memory switch action during the software upgrade. The possible values are:
  - MEM_SW_TYPE is ACT to activate.
  - MEM_SW_TYPE is CANC to cancel the activation.

If the command is successful, the appropriate flash is selected and the TSC card reboots.

The following occurs:

- When the standby TSC card containing the upgrade software reboots (this can take up to 5 minutes).
- After the reboot is completed, the standby TSC is now running the R8.0 software upgrade. The active TSC in Slot 10 is running the version of software prior to the installation of the R8.0 software.

- The standby TSC acquires the active timing reference, which will take up to 15 minutes to accomplish. Then the active TSC in Slot 10 reboots, and the card in Slot 5 becomes active, using software R8.0 as the Working copy. When the TSC card in Slot 10 resets, it is in standby mode, and is running the pre-upgrade version of the software.
- All remaining cards in the shelf will reset simultaneously, raising a SYSBOOT alarm while activation is in progress. When all cards have reset, this alarm clears.
- After the common control cards have finished resetting and all alarms are cleared, you can proceed to the next step.

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 14 Perform Step 13 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 You might have to log in (Step 1 and Step 3) to each node again to activate the software (Step 13).

Step 15 After all nodes have been activated, log in using CTC (Step 1 and Step 3) and verify there are no outstanding alarms.

Step 16 Remove all BLSR lockouts using the following TL1 command:

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

where:

- <TID> is the target identifier (optional).
- <AID> is the Access IDentifier (indicating the facility in the node to which the switch request is directed).
- <CTAG> is the message correlation tag, used to correlate messages and responses.
- <DIRECTION> 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 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, ONS-15310 MA 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 8.2*
  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 and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

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