# Upgrading the Cisco ONS 15454, ONS 15600, ONS 15310-MA, and ONS 15310-CL to Release 9.2.3.1

This document explains how to upgrade Cisco ONS 15454, ONS 15600, ONS 15310-MA, or ONS 15310-CL Cisco Transport Controller (CTC) software to Release 9.2.3.1.

## Contents

This document contains the following information:



## Before You Begin

Before you begin, 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.


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

The following releases can be upgraded to R9.2.3.1:

*Table 1 Upgrade Paths*

| Platform | Releases |
|---|---|
| 15310-CL | 9.1.0 |
| 15310-MA | 8.5.4 |
| 15600 (SONET and SDH) | 9.2.1 |
| 15454 SONET | 8.5.4, 9.2.1.5 |
| 15454 SDH | 9.2.1.5 |

If you wish to upgrade from an earlier software release than those supported, you must contact the Cisco Technical Assistance Center (Cisco TAC).

**Note** Read the procedures in this document before you begin the upgrade.

**Note** R9.2.3.1 supports parallel upgrades for multiple nodes in a network. In a parallel upgrade, you can 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 (wait five minutes from the time the SYSBOOT alarm is raised).

**Caution** When managing end-to-end circuits participating in an ML-Series resilient packet ring (RPR) across multiple nodes involved in a parallel upgrade, all nodes participating in these circuits must have completed the activation before the end-to-end traffic resumes.

# Document Procedures

Procedures in this document must be performed sequentially unless noted otherwise. Ensure that the procedure is completed for each node in a given network. If you are new to upgrading the software, make a printed copy of this document and use it as a checklist.

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

The DLP (task) supplies additional task details to support the NTP. The DLP lists numbered steps that lead you through completion of a task. Some steps mandate that equipment indications be checked for verification. When the proper response is not obtained, a trouble clearing reference is provided.

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

1. NTP-U487 Preparing to Upgrade to a New Release, page 3—This section contains critical information and tasks that you must read and complete before beginning the upgrade process.
2. NTP-U429 Back Up the Software Database, page 3—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-U518 Upgrade the Cisco ONS Software, page 5—You must complete this entire procedure before the upgrade is finished.
4. NTP-U431 Install Public-Key Security Certificate, page 11—You must complete this procedure to be able to run R9.2.3.1.
5. NTP-U432 Revert to Previous Software Load and Database, page 11—Complete this procedure only if you need to return to the software load you were running before activating Software R9.2.3.1.
6. NTP-U519 Upgrade to the ONS Software Using TL1, page 14—Complete this procedure only if you want to install software R9.2.3.1 using Transaction Language 1 (TL1).

# NTP-U487 Preparing to Upgrade to a New Release

| | |
|---|---|
| **Purpose** | This procedure provides critical information checks and tasks you must complete before starting an upgrade to Release 9.2.3.1. |
| **Tools/Equipment** | Nodes to upgrade<br>PC or UNIX workstation<br>Software R9.2.3.1 |
| **Prerequisite Procedures** | None |
| **Required/As Needed** | Required |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Superuser |

**Step 1** Read the release notes for *Cisco ONS 15454, ONS 15600, ONS 15310-MA, ONS 15310-CL, Release 9.2.3.1*.

**Step 2** Log into the node that you want to upgrade. For detailed instructions, refer to the procedure guide.

**Step 3** Verify the workstation hardware and software requirements.

**Step 4** When you have completed the tasks in this section, proceed with the "NTP-U429 Back Up the Software Database" procedure on page 3.

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

# NTP-U429 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-U487 Preparing to Upgrade to a New Release, page 3 |
| **Required/As Needed** | Required |
| **Onsite/Remote** | Onsite or remote (but in the presence of the workstation) |
| **Security Level** | Maintenance or higher; or Superuser, if performing optional Step 2 |

**Step 1** Log into CTC. For detailed instructions, refer to the the procedure guide. If you have already logged in, continue with Step 2.

**Step 2** (Optional) Cisco recommends that you manually log critical information by either writing it down or printing screens where applicable. Use the following table to determine the information you should log; complete the table (or your own version) for every node in the network.

***Table 2 Manually Recorded Data***

| Item | Record Applicable Data Here |
|---|---|
| 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; print the **Inventor**y window. | |
| Inventory; copy the screen contents of the **Inventory** window. Press **PrintScreen**. | |
| Network information; copy the network information from the **Provisioning** tab in the network view. Press **PrintScreen**. | |
| Current configuration (linear, etc.); copy the configuration as needed. | |
| List all protection groups in the system; copy the protection group window from the **Maintenance** tab, in the network view. Press **PrintScreen**. | |
| List alarms; copy the screen contents of the **Alarm** window. Press **PrintScreen**. | |

**Step 3** In CTC node view, click the Maintenance tab and then click the **Database** button.

**Step 4** Click the **Backup** button. A Database Backup dialog box appears.

**Step 5** In the Database Backup dialog box, click the **Browse** button, then navigate to a directory and type or select a database name using the IP address of the node to upgrade (such as 10101882010107.db).

**Step 6** In the Database Backup dialog box, click the **OK** button. If you are overwriting an existing file, click **Yes** in the confirmation dialog box.

**Step 7** A message indicates the status of the backup. When the backup is complete, click the **OK** button to close the message dialog box.

**Step 8** Repeat Steps 1 through 7 for each node in the network.

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

# NTP-U518 Upgrade the Cisco ONS Software

| | |
|---|---|
| **Purpose** | This procedure upgrades your CTC software to R9.2.3.1. |
| **Tools/Equipment** | PC or UNIX workstation |
| **Prerequisite Procedures** | NTP-U429 Back Up the Software Database, page 3 |
| **Required/As Needed** | Required |
| **Onsite/Remote** | Onsite or remote (but in the presence of the workstation) |
| **Security Level** | Superuser |

**Note** After upgrading to R9.2.3.1, the date and time in CTC is reset.

**Step 1** Insert the software R9.2.3.1 CD into the workstation CD-ROM (or otherwise obtain 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.

**Caution** When managing end-to-end circuits participating in a CL-Series resilient packet ring (RPR) across multiple nodes involved in a parallel upgrade, all nodes participating in these circuits must have completed the activation before the end-to-end traffic resumes.

**Step 2** Complete the "DLP-U586 Download the ONS Software" task on page 6 for all nodes (or groups of eight or less nodes) you are upgrading.

**Step 3** Complete the "DLP-U587 Activate the New ONS Software" task on page 7 for all nodes you are upgrading.

**Note** You can 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 (wait for five minutes from the time the SYSBOOT alarm is raised).

**Step 4** (Optional) If you wish to ensure that a software revert to a previous software release be no longer possible, complete the "DLP-U586 Download the ONS Software" task on page 6 for all nodes, or groups of nodes you are upgrading a second time.

**Caution** Downloading R9.2.3.1 a second time following activation prevents reversion to the previous software version.

**Step 5** Complete the "DLP-U460 Set the Date and Time" task on page 10 (any nodes not using Simple Network Time Protocol).

**Step 6** If you need to return to the software and database you had before activating software R9.2.3.1, proceed with the "NTP-U432 Revert to Previous Software Load and Database" procedure on page 11.

**Step 7** To preserve the database of R9.2.3.1, back up the database for the working software load. See "NTP-U429 Back Up the Software Database" procedure on page 3.

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

# DLP-U586 Download the ONS Software

| | |
|---|---|
| **Purpose** | This task downloads software R9.2.3.1 to the nodes prior to activation. |
| **Tools/Equipment** | PC or UNIX workstation |
| **Prerequisite Procedures** | NTP-U429 Back Up the Software Database, page 3 |
| **Required/As Needed** | Required |
| **Onsite/Remote** | Onsite or remote (but in the presence of the workstation) |
| **Security Level** | Superuser or Maintenance |

**Note** The 15310-CTX-CL/CTX2500/ TCC2/TCC2P/TSC card has two flash RAMs. An upgrade downloads the software to the backup RAM on the 15310-CTX-CL/CTX2500/ TCC2/TCC2P/TSC card. 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, using the IP address of the node.

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

**Step 3** Verify that the alarm filter is not on.

a. Click the **Filter** button at the lower-left of the window.

   The Alarm Filter dialog box appears.

b. Click to select any check box that is not selected in the Show Severity section of the **General** tab.

**Step 4** On the Alarms tab, check all nodes for existing alarms. Resolve any outstanding critical alarms before proceeding. If necessary, refer to the troubleshooting guide.

**Note** During the software download process, the SWFTDWN alarm is raised twice, once on standby and again on active, to indicate that the software download is taking place. The alarm is normal and clears when the download is complete.

**Step 5** Return to node view and click the **Maintenance** tab and then click the **Software** button.

**Step 6** Click the **Download** button.

The Download Selection dialog box appears.

**Step 7** Click the **Browse** button to locate and select the software upgrade package files (file with the PKG extension).

**Step 8** Click the **Open** button.

**Step 9** In the list of compatible nodes, click the check boxes for all nodes for software download.

**Note** Cisco advises that you limit concurrent software downloads on a Section data communications channel (SDCC) to eight nodes at once, using the central node to complete the download. If you attempt more than eight concurrent software downloads at once, the downloads in excess of eight will be placed in a queue.

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

**Note** The software download process per node happens in 10 minutes, and can go up to 30 minutes per node.

**Step 11** Return to your originating procedure (NTP).

# DLP-U587 Activate the New ONS Software

| | |
|---|---|
| **Purpose** | This task activates software R9.2.3.1 in each node in the network. |
| **Tools/Equipment** | PC or UNIX workstation |
| **Prerequisite Procedures** | DLP-U586 Download the ONS Software, page 6 |
| **Required/As Needed** | Required |
| **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, using the IP address of the ONS node.

**Step 2** Record the IP address of the node. The IP address is on the upper left corner of the CTC window.

**Step 3** In node view, click the **Alarms** tab.

**Step 4** Verify that the alarm filter is not on.

a. Click the **Filter** button at the lower-left of the window.

   The Alarm Filter dialog box appears.

b. 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 troubleshooting guide.

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

**Step 6** Click the **Maintenance** tab and then click the **Software** button.

**Step 7** Verify that the software version in the Protect Version column is software R9.2.3.1 (the release you are upgrading to).

**Step 8** Click the **Activate** button. The Activate dialog box appears with a warning message.

**Step 9** Click **Yes** to proceed with the activation. The Activation Successful message appears when the software is successfully activated. Click **OK** in the message dialog box.

**Note** When you click **Yes**, CTC loses connection to the node and displays the network view.

**Step 10** After activating the node, the software upgrade reboot occurs as follows:

- Each card in the node resets, beginning with the expansion card. The ONS 15310-CTX-CL card will then reset and come back up.
- When the ONS 15310-CTX-CL is finished, the Ethernet card comes back up, followed by reset of the electrical and optical ports.
- A system reboot (SYSBOOT) alarm is raised while activation is in progress (following the ONS 15310-CTX-CL and cross connect card resets). When all cards have reset, this alarm clears. The complete activation process can take up to 30 minutes, depending on how many cards are installed.
- The process can take up to 8 minutes, This process is service affecting, so Cisco recommends that you activate the new load during a maintenance window. Expect Ethernet traffic to remain down from the time the expansion card resets, until all cards have finished resetting and come back up (this will take 3 to 8 minutes).

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.)

**Caution** The upgrade process is service affecting, so Cisco recommends that you activate the new load during a maintenance window. Ethernet traffic might remain down from the time the ONS 15310-CTX-CL cards switch to the time all Ethernet cards have finished resetting.

**Step 11** In CTC, choose **File > Exit**.

**Step 12** In your browser window, click the **Delete CTC Cache** button. A confirmation dialog box appears.

**Step 13** Click the **Yes** button to confirm.

**Note** You must ensure that CTC is closed before clicking the Delete CTC Cache button. CTC behavior becomes unreliable if this button is clicked when the software is still running. Ensure that the cached files from your browser's directory are deleted, or from the TEMP directory in your Microsoft Windows workstation. If you have trouble reconnecting to CTC, complete the "DLP-U459 Delete Cached JAR Files" task on page 9.

**Step 14** Close your browser and then reopen it.

**Note** Step 15 is necessary only after upgrading the first node in a network, because cached files only need to be removed from your workstation once. For the remaining nodes, you will still be disconnected and removed to the network view during the node reboot, but after the reboot is complete, CTC restores connectivity to the node.

**Step 15** (Optional) Run the Cache Loader pre-caching utility, which can improve your speed logging back into CTC after an upgrade. Perform the following steps to run the Cache Loader.

**a.** Load the software R9.2.3.1 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 appears.

c. Click the **Next** button. The setup options dialog box appears.

d. Choose **Custom**, and click the **Next** button. The Custom Options dialog box appears.

e. Select **Cisco Transport Controller** and **CTC JAR Files** (deselect any other preselected options), then click the **Next** button. A confirmation dialog box appears.

f. Click the **Next** button again. The CTC Cache Loader pre-caches the JAR files to your workstation, displaying a progress status dialog box.

g. When the utility finishes, click **OK**, and then, in the wizard, click the **Finish** button.

**Step 16** Reconnect to CTC using the IP address from Step 2. The new CTC applet for Software R9.2.3.1 uploads. During this login, enter your Superuser user ID and password.

**Step 17** Return to your originating procedure (NTP).

# DLP-U459 Delete Cached JAR Files

| | |
|---|---|
| **Purpose** | This task manually deletes cached JAR files from your browser and hard drive. When you upgrade or revert to a different CTC software load, you must reload CTC to your browser. Before you can reload CTC, you must ensure that previously cached files are cleared from your browser and hard drive. |
| **Tools/Equipment** | PC or UNIX workstation |
| **Prerequisite Procedures** | None |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote (but in the presence of the workstation) |
| **Security Level** | Maintenance or higher |

**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 the **Clear Memory Cache** button, and click **OK**.

c. Click **Clear Disk Cache**, and click **OK** twice.

In Microsoft Internet Explorer:

a. Choose **Tools > Internet Options**. The Internet Options dialog box appears.

b. Click the **General** tab, and then click the **Delete Files** button.

c. Click the **Delete all offline content** check box.

d. Click **OK** twice.

**Step 2** Close your browser.

**Note** 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 **Control Panel > System** and then click the **Advanced** tab.

b. Click the **Environment Variables** button. The resulting display will show a list of user variables and a list of system variables.

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

d. Open the TEMP directory located in the discovered path.

e. Select **View > Details**.

f. 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-U460 Set the Date and Time

| | |
|---|---|
| **Purpose** | If you are not using SNTP, the upgrade procedure can cause the date/time setting to change. Perform this task to reset the date and time at each node. |
| **Tools/Equipment** | PC or UNIX workstation |
| **Prerequisite Procedures** | None |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote (but in the presence of the workstation) |
| **Security Level** | Superuser |

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

**Step 1** In CTC node view, click the **Provisioning** tab and then click the **General** button.

**Step 2** Set the correct date and time, then click the **Apply** button. Repeat Steps 1 and 2 for each remaining node.

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

# NTP-U431 Install Public-Key Security Certificate

| | |
|---|---|
| **Purpose** | This procedure installs the ITU Recommendation X.509 public-key security certificate. The public-key certificate is required to run Software R4.1 and later. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | This procedure is performed when logging into CTC. You cannot perform it at any other time. |
| **Required/As Needed** | This procedure is required to run ONS software. |
| **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. Once the session ends, the certificate gets deleted. This dialog box appears the next time you log into the node.
- Deny—Denies permission to install the certificate. If you choose this option, you cannot log into the node.
- Grant always—Installs the public-key certificate and does not delete it after the session is over. Cisco recommends this option.
- View Certificate—Allows you to view the public-key security certificate.

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

**Step 3** If you need to return to the software and database you had before activating software R9.2.3.1, proceed with the "NTP-U432 Revert to Previous Software Load and Database" procedure on page 11.

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

# NTP-U432 Revert to Previous Software Load and Database

| | |
|---|---|
| **Purpose** | This procedure restores the software and database provisioning you had before you activated software R9.2.3.1. |
| **Tools/Equipment** | PC or UNIX workstation |
| **Prerequisite Procedures** | NTP-U487 Preparing to Upgrade to a New Release, page 3<br>NTP-U429 Back Up the Software Database, page 3<br>NTP-U518 Upgrade the Cisco ONS Software, page 5 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote (but in the presence of the workstation) |
| **Security Level** | Superuser |

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

**Note** Before you upgraded to software R9.2.3.1, you should have backed up the existing database at all nodes in the network (this is part of the "NTP-U429 Back Up the Software Database" procedure on page 3). Cisco recommends that you record or export all critical information to your hard drive. If you need to revert to the backup database, use the following tasks, in order.

**Step 1** Log into the node. For detailed instructions, refer to the procedure guide. If you are already logged in, continue with Step 2.

**Step 2** Complete the "DLP-U461 Revert to Protect Load" task on page 12.

**Note** Do not perform "DLP-U462 Manually Restore the Database" task on page 13 unless the software revert failed.

**Step 3** If the software reversion to your previous release failed to restore the database, complete the "DLP-U462 Manually Restore the Database" task on page 13.

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

# DLP-U461 Revert to Protect Load

| | |
|---|---|
| **Purpose** | This task reverts to the software you were running prior to the last activation and restores your database to the provisioning prior to the activation. |
| **Tools/Equipment** | PC or UNIX workstation |
| **Prerequisite Procedures** | NTP-U487 Preparing to Upgrade to a New Release, page 3<br>NTP-U429 Back Up the Software Database, page 3<br>NTP-U518 Upgrade the Cisco ONS Software, page 5 |
| **Required/As Needed** | Required for revert |
| **Onsite/Remote** | Onsite or remote (but in the presence of the workstation) |
| **Security Level** | Superuser |

**Note** To perform a supported (non-service-affecting) reversion from software R9.2.3.1, the release you want to revert to must have been working at the time you activated to software R9.2.3.1 on that node. Also, a supported reversion automatically restores the node configuration at the time of the previous activation. Thus, any configuration changes made after activation are lost when you revert the software. The exception to this is when you have downloaded software R9.2.3.1 a second time, to ensure that no actual reversion to a previous load can take place. In the latter case, reversion occurs, but traffic is not affected and there are no changes to the database.

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

**Step 2** Verify that the protect software displays the release you upgraded from.

**Step 3** Click the **Revert** button. Reversion activates the protect software and restores the database from the previous load. A dialog box asks you to confirm the choice.

**Step 4** Click **Yes**. This begins the reversion. CTC drops the connection to the node and takes you to the network view, displaying a confirmation dialog box.

**Step 5** Click **OK** and wait until the software reversion finishes before continuing.

**Note** The system reboot might take up to 4 minutes to complete.

**Step 6** Wait one minute before reverting another node.

**Step 7** After reverting all the nodes in the network, close and restart your Netscape or Internet Explorer browser and log into the last node that was reverted. This uploads the appropriate CTC applet to your workstation.

**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, see the "DLP-U459 Delete Cached JAR Files" task on page 9.

**Step 8** Return to your originating procedure (NTP).

# DLP-U462 Manually Restore the Database

| | |
|---|---|
| **Purpose** | This task manually restores the database. If you were unable to perform a revert successfully and need to restore the database, perform this task. |
| **Tools/Equipment** | PC or UNIX workstation |
| **Prerequisite Procedures** | DLP-U461 Revert to Protect Load, page 12 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote (but in the presence of the workstation) |
| **Security Level** | Superuser |

**Caution** Do not perform these steps unless the software reversion failed.

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

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

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

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

The database is restored and the 15310-CTX-CL card reboots.

**Step 4** When the 15310-CTX-CL card has rebooted, log into CTC and verify that the database is restored.

Wait one minute before restoring the next node.

You have now completed the manual database restore.

**Note** When the complete database is restored, the node does not report an event regarding the IP change; the node reboots and configures the new IP from the database. If the IP address being restored is not in the CTC network IP addressing scheme, you might lose visibility of the node. To resolve this, you must launch CTC with the IP mentioned in the table against the database backup. Refer to Table 1 "Manually Recorded Data" in the "NTP-U429 Back Up the Software Database" procedure on page 3 for more information.

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

# NTP-U519 Upgrade to the ONS Software Using TL1

| | |
|---|---|
| **Purpose** | This procedure upgrades the software to software R9.2.3.1 using TL1 rather than CTC. |
| **Tools/Equipment** | PC or UNIX workstation |
| **Prerequisite Procedures** | NTP-U487 Preparing to Upgrade to a New Release, page 3<br>NTP-U429 Back Up the Software Database, page 3 |
| **Required/As Needed** | Optional |
| **Onsite/Remote** | Onsite or remote (but in the presence of the workstation) |
| **Security Level** | Superuser |

**Note** This procedure assumes you are upgrading using Release 6.x TL1 syntax. TL1 commands issued prior to software activation to software R9.2.3.1 will vary in syntax depending on the 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 release when issuing the following commands:

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

**Note** To perform an R9.2.3.1 software download using TL1, you must first have an FTP server or a terminal emulation program like HyperTerminal running on your workstation.

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

- FTP is being used.
- Server is set up with a login and password of FTPUSER1 and FTPUSERPASSWORD1.
- FTP server has an IP address of 10.1.1.1.
- FTP server is running on the standard FTP port.
- Software package is called “15310-03xx-A04K-1405.pkg, “15310ma-03xx-A04K-1405.pkg”, “15600-0xxx-xxxx-xxxx.pkg, “15600SDH-0xxx-xxxx-xxxx.pkg”, “15454-03xx-A04K-1405.pkg”, or “15454SDH-0xxx-xxxx-xxxx.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/*.pkg";
```

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

```
COPY-RFILE:NODENAME:RFILE-PKG:CTAG::TYPE=SWDL,
SRC="ftp://FTPUSER1:FTPUSERPASSWORD1@10.111.11.1:21@90.90.90.90/*.pkg";
```

  The ":21" after the FTP server IP address 10.111.11.1 denotes port 21 on the server.

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

  An example is shown here.

```
COPY-RFILE:NODENAME:RFILE-PKG:CTAG::TYPE=SWDL,
SRC="ftp://FTPUSER1:FTPUSERPASSWORD1@10.1.1.1:21@90.90.90.90/CISCO/SOFTWARE/*.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 node.

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

The terminal emulation interface appears with a Warning message and a command prompt (usually >). TL1 commands can be executed 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 OSS profile user ID (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 userid, 100 is the correlation tag (used to correlate commands to command responses), and PASSWORD is the password associated with the userid.

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

**Step 4** Type the COPY-RFILE command in the TL1 window or, if using HyperTerminal, Select **Transfer** > **Receive File**, and use the associated dialog box to select 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 ONS 15310-CTX-CL cards.

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

where:

- <TID> is the target identifier (optional).
- <AID> identifies the facility in the node to which the switch request is directed.
- <CTAG> is the correlation tag that correlates command and response messages (optional).
- <xfertype> 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 5** Repeat Step 4 for all nodes to be upgraded.

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

The format of the message is:

```
REPT EVT FXFR

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

where:

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

**Step 7** Complete NTP-U487 Preparing to Upgrade to a New Release, page 3 for each node to be upgraded.

**Step 8** Complete NTP-U429 Back Up the Software Database, page 3 for each node to be upgraded.

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

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

where:

- <TID> is the target identifier (optional).
- <AID> identifies the facility in the node to which the switch request is directed
- <CTAG> is the correlation tag that correlates command and response messages (optional).
- <SC> is the switch command that is to be initiated on the paths.
- <SWITCHTYPE> BLSR switch type.

- <DIRN> is the direction of transmission in which switching is to be made and is relative to the SONET line or path identified by the AID. The default value is RCV and should be changed to BTH.

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

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

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

where:

- <TID> is the target identifier (optional).
- <AID> indicates the entity in the node and must not be null.
- <CTAG> is the correlation tag that correlates command and response messages (optional).

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

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

where:

- <TID> is the target identifier (optional).
- <AID> indicates the entity in the node and must not be null.
- <CTAG> is the correlation tag that correlates command and response messages (optional).
- <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> indicates the entity in the node and must not be null.
- <CTAG> is the correlation tag that correlates command and response messages (optional).
- <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 activate only 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 12** 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 correlation tag that correlates command and response messages.
- <MEM_SW_TYPE> indicates a memory switch action during the software upgrade; MEM_SW_TYPE is ACT for activate.

If the command is successful, the appropriate flash is selected and the ONS 15310-CTX-CL/CTX2500/ TCC2/TCC2P/TSC card reboots.

The following occurs:

- Each card in the node reboots, beginning with the standby ONS 15310-CTX-CL/CTX2500/ TCC2/TCC2P/TSC card. When the standby ONS 15310-CTX-CL/CTX2500/ TCC2/TCC2P/TSC comes back up, it signals to the active ONS 15310-CTX-CL/CTX2500/ TCC2/TCC2P/TSC that it is ready to take over. When the active ONS 15310-CTX-CL/CTX2500/ TCC2/TCC2P/TSC receives this signal, it resets itself, and the standby ONS 15310-CTX-CL/CTX2500/ TCC2/TCC2P/TSC takes over and transitions to active. The originally active ONS 15310-CTX-CL/CTX2500/ TCC2/TCC2P/TSC then comes back up as the standby ONS 15310-CTX-CL/CTX2500/ TCC2/TCC2P/TSC .
- Next, the E-Series Ethernet cards reset simultaneously.
- Any cards in Y-cable protection groups boot next, one at a time (protect card first), in order of first creation (refer to the CTC protection group list for order of first creation).
- Next, the traffic cards, G-Series Ethernet cards, CE-Series Ethernet cards, and ML-Series Ethernet cards boot consecutively, in ascending order of slot number, first standby, then working, for each card pair, with the exception that E1-42 protect cards will always be reset before any of their peer working cards.
- A system reboot (SYSBOOT) alarm is raised while activation is in progress (following the ONS 15310-CTX-CL and cross-connect card resets). When all cards have reset, this alarm clears. The complete activation process can take up to 30 minutes, depending on how many cards are installed.

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

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

**Note** Note You might have to log in (Step 1 and Step 3) to each node again to activate the software (Step 12).

**Step 14** After all nodes have been activated, log in using CTC or Telnet (Step 1and Step 3) and verify there are no outstanding alarms.

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

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

where:

- <TID> is the target identifier (optional).
- <AID> indicates the entity in the node and must not be null.
- <CTAG> is the correlation tag that correlates command and response messages (optional).
- <DIRN> is the direction of transmission (transmit or receive). The possible values are RCV—receive direction only (default), TRMT—transmit direction only, or 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

- *Release notes for Cisco ONS 15454, ONS 15600, ONS 15310-MA, ONS 15310-CL, Release 9.2.3.1*

# Obtaining Optical Networking Information

This section contains information that is specific to optical networking products. For information that pertains to all of Cisco, refer to the Obtaining Documentation and Submitting a Service Request section.

## 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 15454 system. It also includes translations of the safety warnings that appear in the ONS 15454 system documentation.

## 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.

# 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.