



Upgrading the Cisco ONS 15454 SDH to Release 7.0.1(MSTP Only)

This document explains how to upgrade Cisco ONS 15454 SDH Cisco Transport Controller (CTC) software from Release 5.0.2, 5.0.3, 5.0.6, 6.0.1, 6.2, or 7.0 to Release 7.0.1, using the Advanced Timing, Communications, and Control (TCC2) or Advanced Timing, Communications, and Control Plus (TCC2P) card. Release 7.0.1 is an MSTP only release, the procedure described in this document should be used only for MSTP upgrade.



Note

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



Note

Release 7.0.1 supports MSTP configurations only. For SONET or SDH configured nodes, upgrade to Release 7.0, or its most current maintenance release.

Contents

- [Before You Begin, page 2](#)
- [NTP-U145 Prepare for Upgrade to Release 7.0.1, page 3](#)
- [NTP-U146 Back Up the Software Database, page 5](#)
- [NTP-U147 Upgrade to Release 7.0.1, page 7](#)
- [NTP-U148 Install Public-Key Security Certificate, page 12](#)
- [NTP-U149 Revert to Previous Software Load and Database, page 13](#)
- [Related Documentation, page 16](#)
- [Obtaining Documentation, page 16](#)
- [Documentation Feedback, page 17](#)
- [Cisco Product Security Overview, page 17](#)
- [Obtaining Technical Assistance, page 18](#)



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

© 2007 Cisco Systems, Inc. All rights reserved.

- [Obtaining Additional Publications and Information, page 20](#)

Before You Begin

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


Caution

Read all procedures before you begin the upgrade.


Caution

This upgrade is supported only for Software Releases 5.0.2, 5.0.3, 5.0.6, 6.0.1, 6.2, and 7.0. If you wish to upgrade from a different software release from those supported, you must contact Cisco Technical Assistance Center (Cisco TAC). For more information, see the [“Obtaining Technical Assistance” section on page 18](#).


Note

Release 7.0.1 supports parallel upgrades for multiple nodes in a network. In a parallel upgrade you can still only activate one node at a time; however, you can begin activation of the next node as soon as the controller cards for the current node have rebooted successfully.

Errorless Upgrades and Exceptions

Upgrades for DWDM configurations are expected to be errorless with the following exception:

The MXP_MR_2.5 and MXPP_MR_2.5 cards will automatically download a new FPGA during a software upgrade from a pre-7.0 release to the Release 7.0.x. For cards with no Y cable protection, the data path will incur a traffic hit of up to 10 seconds (typically less). Y cable protected cards with FibreChannel (FC) payloads will incur an FC link reinitialization as traffic switches away from the card downloading the new FPGA. Y cable protected cards with GE payloads are not expected to incur a traffic hit.


Note

For FC_MR-4 card, hitless software upgrades are not possible with an activation from Software R5.0 to Software R6.0 or higher in enhanced card mode. This is because the FPGA must be upgraded to support differential delay in enhanced mode. Upgrades are still hitless with the line rate mode.

Document Procedures

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

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

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

1. [NTP-U145 Prepare for Upgrade to Release 7.0.1, page 3](#)—This section contains critical information and tasks that you must read and complete before beginning the upgrade process.
2. [NTP-U146 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-U147 Upgrade to Release 7.0.1, page 7](#)—You must complete this entire procedure before the upgrade is finished.
4. [NTP-U148 Install Public-Key Security Certificate, page 12](#)—You must complete this procedure to be able to run ONS 15454 SDH Software R7.0.1.
5. [NTP-U149 Revert to Previous Software Load and Database, page 13](#)—Complete this procedure only if you need to return to the software load you were running before activating the Release 7.0.1 software.

NTP-U145 Prepare for Upgrade to Release 7.0.1

Purpose	This procedure provides the critical information checks and tasks you must complete before beginning an upgrade.
Tools/Equipment	ONS 15454 SDHs to upgrade PC or UNIX workstation Cisco ONS 15454 SDH Release 7.0.1 software
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser

-
- Step 1** Read the *Release Notes for Cisco ONS 15454 SDH Release 7.0.1*.
- Step 2** Log into the node that you will upgrade. For detailed instructions, refer to the *Cisco ONS 15454 SDH Procedure Guide* or the *Cisco ONS 15454 DWDM Procedure Guide*.
- Step 3** Complete the “[DLP-U223 Verify CTC Workstation Requirements](#)” task on page 4.
- Step 4** If you have multiple ONS 15454 SDH nodes configured in the same IP subnet, ensure that only one is connected to a router. Otherwise, the remaining nodes might be unreachable. Refer to the *Cisco ONS 15454 SDH Reference Manual* or the *Cisco ONS 15454 DWDM Procedure Guide* for LAN-connection suggestions.
- Step 5** Complete the “[DLP-U224 Verify Common Control Cards](#)” task on page 5.
- Step 6** When you have completed the tasks for this section, proceed with the “[NTP-U146 Back Up the Software Database](#)” procedure on page 5.

Stop. You have completed this procedure.

DLP-U223 Verify CTC Workstation Requirements

Purpose	This task verifies all PC or UNIX workstation hardware and software requirements. Perform this task before upgrading the workstation to run CTC Software R7.0.1.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of the workstation)
Security Level	Superuser

- Step 1** Ensure that your workstation is either one of the following:
- IBM-compatible PC with a Pentium III/700 or faster processor, CD-ROM drive, a minimum of 384 MB RAM and 190 MB of available hard drive space, running Windows 98, Windows NT 4.0 (with Service Pack 6a), Windows 2000 Professional (with Service Pack 3), or Windows XP Professional (with Service Pack 1)
 - UNIX workstation with Solaris Versions 8 or 9, on an UltraSPARC or faster processor, with a minimum of 384 MB RAM and a minimum of 190 MB of available hard drive space
- Step 2** Ensure that your web browser software is one of the following:
- Netscape Navigator 7.x or higher on Windows
 - Internet Explorer 6.x or higher on Windows
 - Mozilla 1.7 or higher on Solaris



Note Cisco recommends you use either Internet Explorer 6.x or Netscape 7.x on Windows workstations running Release 7.0.1. However, if you upgrade to Netscape 7 or JRE 1.4.2 and you still need to launch CTC directly from nodes running software prior to Release 4.6, you must first run the pre-caching utility supplied in the setup program on the software CD. Run the pre-caching utility during the activation in this case.

- Step 3** Verify that the Java Version installed on your computer is:
- Java Runtime Environment (JRE) 1.4.2 or JRE 5.0, and Java Plug-in 1.4.2 or Java Plug-in 5.0



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



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



Note To install JRE 1.4.2, the Java Policy file, or the Release 7.0.1 online help, refer to the installation instructions in the *Cisco ONS 15454 SDH Procedure Guide* or the *Cisco ONS 15454 DWDM Procedure Guide*.

Step 4 Return to your originating procedure (NTP).

DLP-U224 Verify Common Control Cards

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



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



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

- Step 1** Ensure that the cards are installed. The TCC2 or TCC2P cards are in Slots 7 and 11. Software R7.0.1 does not support simplex operation.
- Step 2** Repeat Step 1 at every node in the network.
- Step 3** Return to your originating procedure (NTP).

NTP-U146 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-U145 Prepare for Upgrade to Release 7.0.1, page 3
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of the workstation)
Security Level	Maintenance user or higher

- Step 1** Log into CTC. For detailed instructions, refer to the *Cisco ONS 15454 SDH Procedure Guide* or the *Cisco ONS 15454 DWDM Procedure Guide*. If you are already logged in, continue with [Step 2](#).
- Step 2** In the node (default) view, click the **Maintenance > Database** tabs.
- Step 3** Click **Backup**.
- Step 4** Save the database on the workstation's hard drive or on network storage. Use an appropriate file name with the file extension .db. (We recommend that you use the IP address of the node and the date, for example 1010120192061103.db.)
- Step 5** Click **Save**. A message appears indicating that the backup is complete.
- Step 6** Click **OK**.
- Step 7** Repeat Steps 1 through 6 for each node in the network.
- Step 8** (Optional) Cisco recommends that you manually log critical information by either writing it down or printing screens where applicable. Use the following table to determine the information you should log; complete the table (or your own version) for every node in the network.

Table 1 Manually Recorded Data

Item	Record Data Here (If Applicable)
IP address of the node.	
Node name.	
Timing settings.	
DCC ¹ connections; list all optical ports that have DCCs activated.	
User IDs; list all, including at least one Superuser.	
Inventory; do a print screen from the Inventory window.	
Active TCC2/TCC2P.	Slot 7 or Slot 11 (circle one)
Network information; do a print screen from the Provisioning tab in the network view.	
List all protection groups in the system; do a print screen from the Protection group window.	
List alarms; do a print screen from the Alarm window.	
List circuits; do a print screen from the Circuit window.	

1. DCC = data communications channel

Stop. You have completed this procedure.

NTP-U147 Upgrade to Release 7.0.1

Purpose	This procedure upgrades your CTC software to Software R7.0.1.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-U146 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

Step 1 Insert the Release 7.0.1 software CD into the workstation CD-ROM (or otherwise acquire access to the software) to begin the upgrade process.



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



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

Step 2 Complete the “[DLP-U225 Download Release 7.0.1 Software](#)” task on page 8 for all nodes, or groups of nodes you are upgrading.

Step 3 Complete the “[DLP-U227 Activate the New Load](#)” task on page 9 for all nodes you are upgrading.



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

Step 4 If necessary, complete the “[DLP-U228 Delete Cached JAR Files](#)” task on page 11.

Step 5 (Optional) If you wish to ensure that a software revert to the previous software release will no longer be possible, complete the “[DLP-U225 Download Release 7.0.1 Software](#)” task on page 8 for all nodes, or groups of nodes you are upgrading a second time.

Step 6 Complete the “[DLP-U66 Set the Date and Time](#)” task on page 12 (any nodes not using Simple Network Time Protocol [SNTP]).

Step 7 As needed, upgrade any spare TCC2 or TCC2P cards by installing the spare in the standby slot of a Release 7.0.1 node.



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

Step 8 If you need to return to the software and database you had before activating Software R7.0.1, proceed with the “[NTP-U149 Revert to Previous Software Load and Database](#)” procedure on page 13.

Step 9 To back up the Release 7.01 database for the Working software load, see , see “[NTP-U146 Back Up the Software Database, page 5](#) in order to preserve the database for the Release 7.01 software

Stop. You have completed this procedure.

DLP-U225 Download Release 7.0.1 Software

Purpose	This task downloads Software R7.0.1 to the ONS 15454 SDH nodes prior to activation.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-U146 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	Maintenance user or higher



Note

The TCC2/TCC2P card has two flash RAMs. An upgrade downloads the software to the backup RAM on both the standby and active TCC2/TCC2P cards. The download task does not affect traffic because the active software continues to run at the primary RAM location; therefore, you can download the software at any time.

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

Step 2 Verify that the alarm filter is not on:

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

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

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



Note

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

Step 4 Return to node view and click the **Maintenance > Software** tabs.

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

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

Step 7 Open the Cisco15454 SDH folder.

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

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



Note

Cisco advises that you limit concurrent software downloads on an optical service channel (OSC) to eight nodes at once, using the central node to complete the download.



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

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



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

Step 11 Return to your originating procedure (NTP).

DLP-U227 Activate the New Load

Purpose	This task activates Software R7.0.1 in each node in the network.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	DLP-U225 Download Release 7.0.1 Software, page 8
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of the workstation)
Security Level	Superuser



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



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

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

Step 2 Verify that the alarm filter is not on:

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

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

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

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

Step 5 Verify that the protect version is 7.0.1.

Step 6 Click **Activate**. The **Activate** dialog box appears with a warning message.

Step 7 Click **Yes** to proceed with the activation. The Activation Successful message appears when the software is successfully activated.

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

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

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

- Each card in the node reboots, beginning with the standby TCC2 or TCC2P card. When the standby TCC2/TCC2P comes back up, it signals to the active TCC2/TCC2P that it is ready to take over. When the active TCC2/TCC2P receives this signal, it resets itself, and the standby TCC2/TCC2P takes over and transitions to active. The originally active TCC2/TCC2P then comes back up as the standby TCC2/TCC2P.
- 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).
- A system reboot (SYSBOOT) alarm is raised while activation is in progress (following the TCC2/TCC2P and cross connect card resets). When all cards have reset, this alarm clears. The complete activation process can take up to 30 minutes, depending on how many cards are installed.

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

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

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



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



Note It might also be necessary to delete cached files from your browser's directory, or from the temp directory on your MS Windows workstation. If you have trouble reconnecting to CTC, complete the "[DLP-U228 Delete Cached JAR Files](#)" task on page 11.

Step 12 Close your browser and then reopen it.

Step 13 Reconnect to CTC using the IP address from [Step 1](#). The new CTC applet for Software R7.0.1 uploads. During this logon, type the user name CISCO15. A password is not required.



Note Steps 10 through 13 are necessary only after upgrading the first node in a network because cached files need to be removed from your workstation only once. For the remaining nodes, you will still be disconnected and removed to the network view during the node reboot, but after the reboot is complete, CTC restores connectivity to the node.

Step 14 Return to your originating procedure (NTP).

DLP-U228 Delete Cached JAR Files

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

Step 1 Delete cache files from your browser directory.

In Netscape:

- a. Choose **Edit > Preferences > Advanced > Cache**.
- b. Click **Clear Memory Cache**.
- c. Click **OK**.
- d. Click **Clear Disk Cache**.
- e. Click **OK** twice.

In Microsoft Internet Explorer:

- a. Choose **Tools > Internet Options > General**.
- b. Choose **Delete Files**.
- c. Select the **Delete all offline content** check box.
- d. Click **OK** twice.

Step 2 Close your browser.



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

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

- a. In your Windows start menu, choose **Settings > Control Panel > System > Advanced**.
- b. Click **Environment Variables**. This shows you a list of user variables and a list of system variables.
- c. In the list of user variables, look for the TEMP variable. The value associated with this variable is the path to your temporary directory where JAR files are stored.
- d. Open the TEMP directory located in the discovered path.
- e. Select **View > Details**.
- f. Select and delete all files with “jar” in the Name or Type field.

- Step 4** Reopen your browser. You should now be able to connect to CTC.
- Step 5** Return to your originating procedure (NTP).

DLP-U66 Set the Date and Time

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



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

- Step 1** In CTC node view, click the **Provisioning > General** tabs.
- Step 2** Set the correct date and time, then click **Apply**.
- Step 3** Repeat Steps 1 and 2 for each remaining node.
- Step 4** Return to your originating procedure (NTP).

NTP-U148 Install Public-Key Security Certificate

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

- Step 1** Log into CTC.
- Step 2** If the Java Plug-in Security Warning dialog box appears, choose one of the following options:
- Grant This Session—Installs the public-key certificate to your PC only for the current session. After the session is ended, the certificate is deleted. This dialog box will appear the next time you log into the ONS 15454 SDH.

- Deny—Denies permission to install the certificate. If you choose this option, you cannot log into the ONS 15454 SDH.
- Grant always—Installs the public-key certificate and does not delete it after the session is over. Cisco recommends this option.
- View Certificate—Allows you to view the public-key security certificate.

After you complete the security certificate dialog boxes, the web browser displays information about your Java and system environments. If this is the first login, a CTC downloading message appears while CTC files are downloaded to your computer. The first time you connect to an ONS 15454 SDH, 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 R7.0.1, proceed with the “[NTP-U149 Revert to Previous Software Load and Database](#)” procedure on page 13.

Stop. You have completed this procedure.

NTP-U149 Revert to Previous Software Load and Database

Purpose	This procedure returns you to the software and database provisioning you had before you activated Software R7.0.1.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-U145 Prepare for Upgrade to Release 7.0.1, page 3 NTP-U146 Back Up the Software Database, page 5 NTP-U147 Upgrade to Release 7.0.1, page 7
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 R7.0.1, you should have backed up the existing database at all nodes in the network (this is part of the “[NTP-U146 Back Up the Software Database](#)” procedure on page 5). Cisco recommends that you record or export all critical information to your hard drive. If you need to revert to the backup database, use the following tasks, in order.



Caution

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



Note

TCC2P cards act as TCC2 cards in Releases prior to Release 6.0.

-
- Step 1** Log into the node. For detailed instructions, refer to the *Cisco ONS 15454 SDH Procedure Guide*, or *Cisco ONS 15454 DWDM Procedure Guide*. If you are already logged in, continue with Step 2.
- Step 2** Complete the “[DLP-U230 Revert to Protect Load](#)” task on page 14.
- Step 3** If the software revert to your previous release failed, complete the “[DLP-U231 Manually Restore the Database](#)” task on page 15.

Stop. You have completed this procedure.

DLP-U230 Revert to Protect Load

Purpose	This task reverts to the software you were running prior to the last activation.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-U145 Prepare for Upgrade to Release 7.0.1 , page 3 NTP-U146 Back Up the Software Database , page 5 NTP-U147 Upgrade to Release 7.0.1 , page 7
Required/As Needed	Required for revert
Onsite/Remote	Onsite or remote (but in the presence of the workstation)
Security Level	Superuser



Note

To perform a supported (non-service-affecting) revert from Software R7.0.1, the release you want to revert to must have been working at the time you activated to Software R7.0.1 on that node. Also, a supported revert automatically restores the node configuration at the time of the previous activation. Thus, any configuration changes made after activation will be lost when you revert the software. The exception to this is when you have downloaded Release 7.0.1 a second time, to ensure that no actual revert to a previous load can take place. In this latter case, the revert will occur, but will not be traffic affecting and will not change your database.



Note

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

-
- Step 1** From the node view, click the **Maintenance > Software** tabs.
- Step 2** Verify that the protect software displays the release you upgraded from.
- Step 3** Click **Revert**. Revert activates the protect software and restores the database from the previous load. A dialog box asks you to confirm the choice.
- Step 4** Click **OK**. This begins the revert and drops the connection to the node.
- Step 5** Wait until the software revert finishes before continuing.



Note

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

Step 6 Restart your Netscape or Internet Explorer browser.

Step 7 Wait one minute before restoring another node.



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

Step 8 Perform the “[DLP-U228 Delete Cached JAR Files](#)” task on page 11.

Step 9 After reverting all of the nodes in the network, restart the browser and log back into the last node that was reverted. This uploads the appropriate CTC applet to your workstation.

Step 10 Return to your originating procedure (NTP).

DLP-U231 Manually Restore the Database

Purpose	This task manually restores the database. Use this task if you were unable to perform a revert successfully and need to restore the database.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	DLP-U230 Revert to Protect Load , page 14
Required/As Needed	As needed
Onsite/Remote	Onsite or remote (but in the presence of the workstation)
Security Level	Superuser



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



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

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

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

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

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

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

Wait one minute before restoring the next node.

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

Step 5 You have now completed the manual database restore.

Step 6 Return to your originating procedure (NTP).

Related Documentation

Use this document in conjunction with the following publications:

- *Cisco ONS 15454 SDH Procedure Guide*
Provides installation, turn up, test, and maintenance procedures for SONET networks
- *Cisco ONS 15454 SDH Reference Manual*
Provides technical reference information for SONET cards, nodes, and networks
- *Cisco ONS 15454 SDH Troubleshooting Guide*
Lists alarms, errors, and transient conditions and provides alarm and general troubleshooting procedures
- *Cisco ONS 15454 DWDM Procedure Guide*
Provides installation, turn up, test, and maintenance procedures for DWDM networks
- *Cisco ONS 15454 DWDM Reference Manual*
Provides technical reference information for DWDM cards, nodes, and networks
- *Cisco ONS 15454 DWDM Troubleshooting Guide*
Lists alarms, errors, and transient conditions and provides alarm and general troubleshooting procedures
- *Release Notes for Cisco ONS 15454 SDH Release 7.0.1*
Provides caveats, closed issues, and new feature and functionality information

Obtaining Documentation

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

Cisco.com

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

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

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

Product Documentation DVD

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

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

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

Cisco Optical Networking Product Documentation CD-ROM

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

Ordering Documentation

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

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

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

Documentation Feedback

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

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

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

We appreciate your comments.

Cisco Product Security Overview

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

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

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

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

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

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

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

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

Reporting Security Problems in Cisco Products

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

- For Emergencies only—security-alert@cisco.com

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

- For Nonemergencies—psirt@cisco.com

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

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



Tip

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

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

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

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

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

Obtaining Technical Assistance

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

Cisco Technical Support & Documentation Website

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

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

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

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



Note

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

Submitting a Service Request

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

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

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

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

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

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

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

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

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

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

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

<http://www.ciscopress.com>

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

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

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

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

or view the digital edition at this URL:

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

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:
<http://www.cisco.com/ipj>
- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:
<http://www.cisco.com/en/US/products/index.html>
- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:
<http://www.cisco.com/discuss/networking>
- World-class networking training is available from Cisco. You can view current offerings at this URL:
<http://www.cisco.com/en/US/learning/index.html>

This document is to be used in conjunction with the documents listed in the [“Related Documentation”](#) section.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

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

© 2007 Cisco Systems, Inc. All rights reserved.