



Upgrading Cisco ONS 15454 SDH Release 4.x to 4.6

This document explains how to upgrade Cisco ONS 15454 Cisco Transport Controller (CTC) software from Release 4.x to Release 4.6 using the TCC2 card.



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.

Contents

- [Before You Begin, page 2](#)
- [NTP-U62 Prepare for Release 4.x to Release 4.6 Upgrade, page 4](#)
- [NTP-U63 Back Up the Software R4.x Database, page 6](#)
- [NTP-U64 Upgrade Software R4.x to Software R4.6, page 7](#)
- [NTP-U65 Install Public-Key Security Certificate, page 14](#)
- [NTP-U66 Revert to Previous Software Load and Database, page 16](#)
- [Related Documentation, page 18](#)
- [Obtaining Documentation, page 19](#)
- [Documentation Feedback, page 20](#)
- [Obtaining Technical Assistance, page 20](#)
- [Obtaining Additional Publications and Information, page 21](#)



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

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

Before You Begin

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



Caution

Read all procedures before you begin the upgrade.



Caution

This upgrade is supported only for Software Releases 4.0.x, 4.1.x, and 4.5. If you wish to upgrade from an earlier software release, you must contact Cisco Technical Assistance Center (Cisco TAC). For more information, see the [“Obtaining Technical Assistance” section on page 20](#).

Errorless Upgrades and Exceptions

The following tables, organized by cross connect card type, define where errorless upgrades are expected for Release 4.6, and where exceptions can occur. Please review the table for your particular cross connect card type.



Note

In all cases, if traffic goes over a non-revertive path protection and is on the protect path all traffic will experience less than 60 ms hits.

XC10G

This table applies to nodes equipped with XC10G cards.

Table 0-1 XC10G

Card Type	Expected Traffic Effect
DS1	Errorless
DS3	Errorless
DS3E	Errorless
DS3XM	Errorless
EC1	Errorless
OCn	Errorless
E-series Ethernet	Traffic hits up to 5 minutes (approximately)
ML-series Ethernet	Traffic hits up to 3 minutes (approximately)
G-series Ethernet	Errorless

XCVXL

This table applies to nodes equipped with XCVXL cards.

Table 0-2 XCVXL

Card Type	Expected Traffic Effect
DS1	Errorless
DS3	Errorless
DS3E	Errorless
DS3XM	Errorless
EC1	Errorless
OCn	Errorless
E-series Ethernet	Traffic hits up to 5 minutes (approximately)
ML-series Ethernet	Traffic hits up to 3 minutes (approximately)
G-series Ethernet	Errorless

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 wish 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-U62 Prepare for Release 4.x to Release 4.6 Upgrade, page 4](#)—This section contains critical information and tasks that you must read and complete before beginning the upgrade process.
2. [NTP-U63 Back Up the Software R4.x Database, page 6](#)—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-U64 Upgrade Software R4.x to Software R4.6, page 7](#)—You must complete this entire procedure before the upgrade is finished.
4. [NTP-U65 Install Public-Key Security Certificate, page 14](#)—You must complete this procedure to be able to run ONS 15454 SDH Software R4.6.
5. [NTP-U66 Revert to Previous Software Load and Database, page 16](#)—Complete this procedure only if you need to return to the software load you were running before activating the Release 4.6 software.

NTP-U62 Prepare for Release 4.x to Release 4.6 Upgrade

Purpose	This procedure provides the critical information checks and tasks you must complete before beginning an upgrade.
Tools/Equipment	ONS 15454 SDH nodes to upgrade PC or UNIX workstation Cisco ONS 15454 SDH Release 4.6 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 4.6*.
- Step 2** Log into the node that you will upgrade. For detailed instructions, refer to the *Cisco ONS 15454 SDH Procedure Guide*.
- Step 3** Complete the “[DLP-U106 Verify CTC PC or UNIX 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* for LAN-connection suggestions.
- Step 5** Complete the “[DLP-U108 Verify Common Control Cards](#)” task on page 5.
- Step 6** When you have completed the tasks for this section, proceed with the “[NTP-U63 Back Up the Software R4.x Database](#)” procedure on page 6.
- Stop. You have completed this procedure.**
-

DLP-U106 Verify CTC PC or UNIX Workstation Requirements

Purpose	This task verifies all PC or UNIX workstation hardware and software requirements. Use this task before upgrading the workstation to run CTC Software R4.6.
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 higher processor, and a CD-ROM drive with a minimum of 256 MB RAM and 50 MB of available hard drive space running Windows 98, Windows NT 4.0, Windows 2000, or Windows XP
 - UNIX workstation running Solaris version 8 or 9, on an UltraSPARC or faster processor, with a minimum of 256 MB RAM and a minimum of 50 MB of available hard drive space

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

- Netscape Navigator 4.73 or higher (Netscape Navigator 7.0 is included on the ONS 15454 SDH software CD shipped with the node)
- Internet Explorer 4.0.x Service Pack 2 or higher



Note Cisco recommends you use either Internet Explorer 6.x or Netscape 7.x for Windows workstations running Release 4.6. However, Cisco does not recommend upgrading to Netscape 7 or JRE 1.4.2 if CTC still needs to be launched directly from nodes running software prior to Release 4.6.

Step 3 Verify the following:

- The Java Version installed on your computer is:
 - Java Runtime Environment (JRE) 1.4.2, and Java Plug-in 1.4.2 if you are using Netscape 7.x (also preferred for Internet Explorer 6.x)
 - JRE 1.3.1_02, and Java Plug-in 1.3.1 if you are using Netscape 4.7.x (also works with Internet Explorer 6.x)



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

- The Java Policy file is installed on your computer.



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



Note If you need to install either the JRE 1.4.2 or the Java Policy file, they are included on the ONS 15454 SDH software CD. For detailed installation instructions, refer to the *Cisco ONS 15454 SDH Procedure Guide*.

Step 4 Return to your originating procedure (NTP).

DLP-U108 Verify Common Control Cards

Purpose	This task verifies that two TCC2 cards and two XC-VXLs or two OSCMs (in DWDM configurations) 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

Dense wavelength division multiplexing (DWDM) nodes should have OSCM cards installed during the upgrade. If you plan to convert from dedicated DWDM support to Release 4.6 hybrid support, you must first complete the software upgrade for all DWDM nodes before attempting to install OSC-CSM and XC-VXL cards in your nodes. Release 4.5 does not support XC-VXL cards.

- Step 1** Ensure that the cards are installed. The TCC2 cards are in Slots 7 and 11 and the XC-VXL/OSCM cards are in Slots 8 and 10. Software R4.6 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-U63 Back Up the Software R4.x Database

Purpose	This procedure preserves all configuration data for your network before performing the upgrade.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-U62 Prepare for Release 4.x to Release 4.6 Upgrade, page 4
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of the workstation)
Security Level	Superuser

- Step 1** Log into CTC. For detailed instructions, refer to the *Cisco ONS 15454 SDH 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. (Cisco recommends 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 3 *Manually Recorded Data*

Item	Record Data Here (If Applicable)
IP address of the node.	
Node name.	
Timing settings.	

Table 3 Manually Recorded Data (continued)

Item	Record Data Here (If Applicable)
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.	Slot 7 or Slot 11 (circle one)
Active XC-VXL/OSCM.	Slot 8 or Slot 10 (circle one)
Network information; do a print screen from the Provisioning tab in the network view.	
Current configuration (MS-SPRing ² , linear, etc.); do print screens as needed.	
List all Protection groups in the system; do a print screen from the protection group window.	
List alarms; do a print screen from the Alarm window.	
List circuits; do a print screen from the Circuit window.	

1. DCC = data communications channel
2. MS-SPRing = multiplex section-shared protection ring

Stop. You have completed this procedure.

NTP-U64 Upgrade Software R4.x to Software R4.6

Purpose	This procedure upgrades your CTC software to Software R4.6.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-U63 Back Up the Software R4.x Database, page 6
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of the workstation)
Security Level	Superuser

Step 1 Insert the Release 4.6 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-U109 Download Release 4.6 Software](#)” task on page 8 for all nodes (or groups of eight or less nodes) you are upgrading.

Step 3 Complete the “[DLP-U110 Perform a Software R4.x MS-SPRing Lockout](#)” task on page 9 (MS-SPRing nodes only).

Step 4 Complete the “[DLP-U111 Activate the New Load](#)” task on page 10 for all nodes you are upgrading.



Note Only activate one node at a time.

Step 5 If necessary, complete the “[DLP-U112 Delete Cached JAR Files](#)” task on page 12.

Step 6 Complete the “[DLP-U113 Remove the MS-SPRing Lockout](#)” task on page 13 for all MS-SPRing nodes in the network.



Note Leave the MS-SPRing in the lockout state until you have finished reverting all nodes.

Step 7 Complete the “[DLP-U79 Set the Date and Time](#)” task on page 14 (any nodes not using Simple Network Time Protocol [SNTP]).

Step 8 As needed, upgrade any spare TCC2 cards by installing the spare in the standby slot of a Release 4.6 node.



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

Step 9 If you need to return to the software and database you had before activating Software R4.6, proceed with the “[NTP-U66 Revert to Previous Software Load and Database](#)” procedure on page 16.

Stop. You have completed this procedure.




DLP-U109 Download Release 4.6 Software

Purpose	This task downloads Software R4.6 to the ONS 15454 SDH nodes prior to activation.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-U63 Back Up the Software R4.x Database, page 6
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of the workstation)
Security Level	Superuser or Maintenance



Note The TCC2 card has two flash RAMs. An upgrade downloads the software to the backup RAM on both the backup and active TCC2 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:
- Click the **Alarms** tab.
 - Click the **Filter** tool at the lower-right side of the bottom toolbar. Alarm filtering is enabled if the tool is 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 Cisco15454SDH 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 SDCC to eight nodes at once, using the central node to complete the download.
- 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-U110 Perform a Software R4.x MS-SPRing Lockout

Purpose	This task performs an MS-SPRing lockout. If you have an MS-SPRing provisioned, you must use this task before beginning the upgrade.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-U63 Back Up the Software R4.x Database, page 6
Required/As Needed	Required for MS-SPRing only
Onsite/Remote	Onsite or remote (but in the presence of the workstation)
Security Level	Superuser



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

**Note**

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

Step 1 In node view, click the **Maintenance > MS-SPRing** tabs.

Step 2 For each of the MS-SPRing trunk (span) cards (STM-4, STM-16, or STM-64), perform the following steps:

- a. Next to the trunk card row, click the **East Switch** column to show the pull-down menu.
- b. From the menu options, choose **Lockout Span**.
- c. Click **Apply**.
- d. In the same row, click the **West Switch** column to show the pull-down menu.
- e. From the menu options, choose **Lockout Span**.
- f. Click **Apply**.

**Note**

Ignore any Default K alarms that occur on the protect VC4 timeslots during this lockout period.

**Note**

Certain MS-SPRing-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 will clear upon completion of the upgrade, after all nodes have been activated.

- MSSP-OOSYNC (MN)
- RING-MISMATCH (MJ)
- APSCDFLTK (MN)
- MSSP-RESYNC (NA)

Step 3 Return to your originating procedure (NTP).

DLP-U111 Activate the New Load

Purpose	This task activates Software R4.6 in each node in the network.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	DLP-U109 Download Release 4.6 Software, page 8 DLP-U110 Perform a Software R4.x MS-SPRing Lockout, page 9 (if required)
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of the workstation)
Security Level	Superuser

**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.

**Note**

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

- Step 1** 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 4.6.
- 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. Click **OK** in the message box.

**Note**

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

- Step 8** After activating the node, wait until the software upgrade reboot finishes at that node before continuing. The following occurs:
- Each card in the node reboots, beginning with the standby TCC2 card. When the standby TCC2 comes back up, it signals to the active TCC2 that it is ready to take over. When the active TCC2 receives this signal, it resets itself, and the standby TCC2 takes over and transitions to active. The originally active TCC2 then comes back up as the standby TCC2.
 - While the second TCC2 is rebooting, the cross-connect card (or OSCM card) in Slot 8 reboots, and then the cross-connect card (or OSCM card) in Slot 10 reboots.
 - Next, the Ethernet cards reset simultaneously; then the traffic cards boot consecutively from left to right.
 - A system reboot (SYSBOOT) alarm is raised while activation is in progress. When all cards have reset, this alarm clears. The activation process can take up to 30 minutes, depending on how many cards are installed.

When all the cards finish rebooting and all alarms clear, you can safely proceed to the next step. If you are upgrading remotely and cannot see the nodes, wait for 30 minutes for the process to complete, then check to ensure that all alarms have cleared before proceeding.

- Step 9** In CTC, choose **File > Exit**.

Step 10 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-U112 Delete Cached JAR Files” task on page 12](#).

Step 11 Reconnect to CTC using the IP address from [Step 1](#). The new CTC applet for Software R4.6 uploads. During this logon, type the user name CISCO15. A password is not required.



Note Steps 9 through 11 are only necessary 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 will restore connectivity to the node.

Step 12 Return to your originating procedure (NTP).

DLP-U112 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	As needed.
Onsite/Remote	Onsite or remote (but in the presence of the workstation)
Security Level	Superuser

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 path you just looked up.
- e. Select **View > Details**.
- f. Select and delete all files with “jar” in the Name or Type field.

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

Step 5 Return to your originating procedure (NTP).

DLP-U113 Remove the MS-SPRing Lockout

Purpose	This task releases the span lockouts on all MS-SPRing nodes after the new software load is activated on all nodes.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	DLP-U111 Activate the New Load, page 10
Required/As Needed	Required for MS-SPRing
Onsite/Remote	Onsite or remote (but in the presence of the workstation)
Security Level	Superuser

Step 1 In CTC node view, click the **Maintenance > MS-SPRing** tabs.

Step 2 For each of the MS-SPRing trunk (span) cards (STM-4, STM-16, or STM-64), perform the following steps:

- a. Next to the trunk card row, click the **West Switch** column to show the pull-down menu.
- b. From the menu options, choose **Clear**.
- c. Click **Apply** to activate the command.



Note When removing a lockout, be sure to apply your changes each time you choose the Clear option. If you try to select Clear for more than one lockout at a time, you risk traffic loss on the first ring switch.

- d. In the same row, click the **East Switch** column to show the pull-down menu.
 - e. From the menu options, choose **Clear**.
 - f. Click **Apply** to activate the command.
- Step 3** Repeat this task as many times as necessary to remove all MS-SPRing span lockouts on the upgrade nodes.
- Step 4** Return to your originating procedure (NTP).

DLP-U79 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-U65 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 SDH 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.
- Step 3** If the Login dialog box appears, you have completed this procedure. If the Change Java Policy File dialog box appears, complete this step. The Change Java Policy File dialog box appears if CTC finds a modified Java policy file .java.policy on your computer. In Software R4.0 and earlier, the Java policy file was modified to allow CTC software files to be downloaded to your computer. Choose one of the following options:
- **Yes**—Removes CTC-related entries from the modified Java policy file from your computer. Choose this option only if you will log into ONS 15454 SDH nodes running Software R4.1 or later.
 - **No**—Does not remove CTC-related entries from the modified Java policy file from your computer. Choose this option if you will log into ONS 15454 SDH nodes running Software R4.0 or earlier. If you choose No, this dialog box will appear every time you log into the node. If you do not want it to appear, check the **Do not show the message again** check box.

**Caution**

If you delete CTC-related files from the Java policy file, you cannot log into nodes running Software R4.0 and earlier. If you want to log into an ONS 15454 SDH node running an earlier release, insert the software CD for the release into your PC CD-ROM and run the CTC setup wizard to reinstall the Java policy file. In the CTC setup wizard, choose the custom installation option.

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, CTC downloading message appears while CTC files are downloaded to your computer. The first time you connect to an ONS 15454 SDH node, this process can take several minutes. After the download, the CTC Login dialog box appears.

- Step 4** If you need to return to the software and database you had before activating Software R4.6, proceed with the [“NTP-U66 Revert to Previous Software Load and Database” procedure on page 16](#).

Stop. You have completed this procedure.

NTP-U66 Revert to Previous Software Load and Database

Purpose	This procedure returns you to the software and database provisioning you had before you activated Software R4.6.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-U62 Prepare for Release 4.x to Release 4.6 Upgrade, page 4 NTP-U63 Back Up the Software R4.x Database, page 6 NTP-U64 Upgrade Software R4.x to Software R4.6, 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 R4.6, you should have backed up the existing database at all nodes in the network (this is part of the “[NTP-U63 Back Up the Software R4.x Database](#)” procedure on page 6). 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 *Cisco ONS 15454 SDH Procedure Guide*. If you are already logged in, continue with Step 2.
 - Step 2** Complete the “[DLP-U110 Perform a Software R4.x MS-SPRing Lockout](#)” task on page 9 (MS-SPRing only).
 - Step 3** Complete the “[DLP-U114 Revert to Protect Load](#)” task on page 17.
 - Step 4** Complete the “[DLP-U113 Remove the MS-SPRing Lockout](#)” task on page 13 (MS-SPRing only).
 - Step 5** If the software revert to your previous release failed, complete the “[DLP-U115 Manually Restore the Database](#)” task on page 18.

Stop. You have completed this procedure.

DLP-U114 Revert to Protect Load

Purpose	This task reverts to the software you were running prior to the last activation and to restore your database to the provisioning you had prior to the activation.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-U62 Prepare for Release 4.x to Release 4.6 Upgrade, page 4 NTP-U63 Back Up the Software R4.x Database, page 6 NTP-U64 Upgrade Software R4.x to Software R4.6, page 7 DLP-U110 Perform a Software R4.x MS-SPRing Lockout, page 9
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 R4.6, the release you want to revert to must have been working at the time you activated to Software R4.6 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.

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


Note

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

- Step 6** Close your Netscape or Internet Explorer browser.
- Step 7** Wait one minute before restoring another node.


Note

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

- Step 8** 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.


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-U112 Delete Cached JAR Files” task on page 12](#).

Step 9 Return to your originating procedure (NTP).

DLP-U115 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-U114 Revert to Protect Load, page 17 DLP-U113 Remove the MS-SPRing Lockout, page 13 (if required)
Required/As Needed	As needed
Onsite/Remote	Onsite or remote (but in the presence of the workstation)
Security Level	Superuser



Caution

Do not perform these steps unless the software revert failed.



Caution

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

- Step 1** In the CTC node view, click the **Maintenance > Database** tabs.
- Step 2** Click **Restore**. The Open dialog box appears.
- Step 3** Select the previously saved file and choose **Open**.
The database id restored and the TCC2 cards reboot.
- Step 4** When the TCC2 cards have rebooted, log back into CTC and verify that the database is restored.
Wait one minute before restoring the next node.
- Step 5** Repeat Steps 1 to 4 for each node in the network.
You have now completed the manual database backup.
- Step 6** Return to your originating procedure (NTP).
-

Related Documentation

Release-Specific Documents

- *Release Notes for the Cisco ONS 15454 SDH, Release 4.6*
- *Release Notes for the Cisco ONS 15327, Release 4.6*
- *Release Notes for the Cisco ONS 15454, Release 4.6*

Platform-Specific Documents

- *Cisco ONS 15454 SDH Procedure Guide, Release 4.6*
- *Cisco ONS 15454 SDH Reference Guide, Release 4.6*
- *Cisco ONS 15454 SDH Troubleshooting Guide, Release 4.6*

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 on the World Wide Web at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco websites can be accessed from this URL:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:
<http://www.cisco.com/en/US/partner/ordering/index.shtml>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Cisco Optical Networking Product Documentation CD-ROM

Optical networking-related documentation, including Cisco ONS 15454 SDH 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.

Documentation Feedback

You can submit e-mail comments about technical documentation to bug-doc@cisco.com.

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

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

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour-a-day, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance. If you do not hold a valid Cisco service contract, please contact your reseller.

Cisco TAC Website

The Cisco TAC website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year. The Cisco TAC website is located at this URL:

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

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

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

Opening a TAC Case

Using the online TAC Case Open Tool is the fastest way to open P3 and P4 cases. (P3 and P4 cases are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using the recommended resources, your case will be assigned to a Cisco TAC engineer. The online TAC Case Open Tool is located at this URL:

<http://www.cisco.com/tac/caseopen>

For P1 or P2 cases (P1 and P2 cases are those in which your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case 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 listing of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—Your network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Priority 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Priority 3 (P3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Priority 4 (P4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Go to this URL to visit the company store:
<http://www.cisco.com/go/marketplace/>
- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:
<http://cisco.com/univercd/cc/td/doc/pcat/>
- *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 online at this URL:
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:
<http://www.cisco.com/packet>
- *iQ Magazine* is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:
<http://www.cisco.com/go/iqmagazine>

- *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>
- Training—Cisco offers world-class networking training. Current offerings in network training are listed 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.

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site 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. (0304R)

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