Upgrading Cisco ONS 15454 SDH Release 3.x to Release 4.0.x Using the TCC-I 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.

This document explains how to upgrade the Cisco ONS 15454 SDH Cisco Transport Controller (CTC) software from Software Release 3.x to Software R4.0.x using the Timing, Communications, and Control–International (TCC-I) card.

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 each procedure before you begin the upgrade.

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

Each section begins with an overview procedure, followed by a detailed procedure for each step.

- NTP-U11 Prepare for Release 3.x to Release 4.0.x Upgrade, page 2—Review this critical information and complete these critical procedures before beginning the upgrade process.

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

- NTP-U12 Back Up the Software R3.x 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.
- NTP-U21 Upgrade Software R3.x to Software R4.0.x, page 6—Complete these procedures to upgrade the software. You must complete the entire procedure before the upgrade is finished.
- NTP-U15 Upgrade the TCC-I Card to the TCC2 Card, page 13—Complete this procedure to upgrade the TCC-I card to a TCC2 card.
- NTP-U14 Revert to Previous Software Load and Database, page 16—As needed, complete this procedure to return to the software load you were running before activating the R4.0.x software.
- After performing the procedures in this chapter, upgrade the XC10G cards with XCVXL cards, as necessary. For detailed instructions, refer to the *Cisco ONS 15454 SDH Procedure Guide*.

NTP-U11 Prepare for Release 3.x to Release 4.0.x Upgrade

Purpose	This procedure steps you through the critical information checks and procedures you must complete before beginning an upgrade.
Tools/Equipment	ONS 15454 SDH nodes to upgrade; PC or UNIX workstation; Cisco ONS 15454 SDH R4.0.x 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 4.0.x*.

Step 2 Log into the node that you will upgrade. For detailed instructions, refer to the *Cisco ONS SDH 15454 Procedure Guide*.

Step 3 Complete the "DLP-U17 Verify the CTC PC or UNIX Workstation" task on page 3.

Step 4 Disable all other Ethernet devices (such as a dial-up adapter) on a PC or workstation that runs CTC. For more information, refer to the Cisco Technical Assistance Center (TAC) web site at http://www.cisco.com/tac.

If you have multiple IP addresses on your PC or workstation, you should remove them; you cannot install R4.0.x if multiple IP addresses are configured.

Step 5 Complete the "DLP-U18 Verify the LAN Connections" task on page 4.

Step 6 Complete the "DLP-U19 Verify Common Control Cards" task on page 4.

Step 7 When you have completed the procedures for this section, proceed with the "NTP-U12 Back Up the Software R3.x Database" procedure on page 5.

Stop. You have completed this procedure.

DLP-U17 Verify the CTC PC or UNIX Workstation

Purpose	Before upgrading the software to R4.0.x, verify all PC or UNIX workstation hardware and software requirements.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of a PC or UNIX workstation)
Security Level	Superuser

Step 1 Ensure that your workstation is one of the following:

- IBM-compatible PC with a Pentium or higher processor, CD-ROM drive, and 128 MB RAM running Windows 95, Windows 98, Windows 2000, Windows NT (with service pack 4 or higher), or Windows XP
- UNIX workstation running Solaris 2.5.x or 2.6.x.

Check your web browser software version and use one of the following:

- Netscape Navigator 4.73 or higher (Netscape Navigator is included on the ONS 15454 SDH software CD shipped with the node)
- Netscape Communicator 4.61 or higher
- Internet Explorer 4.0.x Service Pack 2 or higher

Step 2 Verify the following:

- The Java Version installed on your computer is Java Runtime Environment (JRE) Release 1.3.1_02. You can check this on 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 If you need to install either the JRE 1.3.1_01 or the Java Policy file, they are included on the ONS 15454 SDH software CD. For detailed installation instructions, refer to the *Cisco ONS SDH 15454 Procedure Guide*.

Note If you must later revert to a release that can use a previous version of JRE, you will need to reinstall Java and delete the JAR files from your PC or workstation's system temp directory after reverting all of the nodes in the network. You can find the appropriate JRE version on the older Cisco software CD. If you are currently running a release that is also compatible with JRE 1.3.1_02, the extra steps are not necessary.

Step 3 Return to the "NTP-U11 Prepare for Release 3.x to Release 4.0.x Upgrade" procedure on page 2.

DLP-U18 Verify the LAN Connections

Purpose	Use this task to ensure that LAN connections are correct.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	DLP-U17 Verify the CTC PC or UNIX Workstation, page 3
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of a PC or UNIX workstation)
Security Level	Superuser

Step 1 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 2 Return to the "NTP-U11 Prepare for Release 3.x to Release 4.0.x Upgrade" procedure on page 2.

DLP-U19 Verify Common Control Cards

Purpose	This task checks for duplex common control cards. The node must have two TCC-I cards and two 10 Gigabit Cross-Connect (XC10G) cards.
Tools/Equipment	PC or UNIX workstation with CTC installed
Prerequisite Procedures	DLP-U17 Verify the CTC PC or UNIX Workstation, page 3 DLP-U18 Verify the LAN Connections, page 4
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of a PC or UNIX workstation)
Security Level	Superuser

Step 1 In CTC node (default) view, ensure that TCC-I cards are installed in Slots 7 and 11 and that the XC10G cross-connect cards are installed in Slots 8 and 10. Release 3.x does not support simplex operation.

Step 2 Repeat Step 1 at every node in the network.

Step 3 Return to the "NTP-U11 Prepare for Release 3.x to Release 4.0.x Upgrade" procedure on page 2.

NTP-U12 Back Up the Software R3.x Database

Purpose	Use this procedure to preserve all configuration data for each node in the network being upgraded.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-U11 Prepare for Release 3.x to Release 4.0.x Upgrade, page 2
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of a PC or UNIX workstation)
Security Level	Superuser

Step 1 Log into CTC. For detailed instructions, refer to the *Cisco ONS SDH 15454 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 a PC or workstation hard drive or on network storage. Use an appropriate file name with the file extension .db. (Cisco recommends using 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 by printing screens where applicable. Use Table 1 to determine the information you should log; complete the table (or your own version) for every node in the network.

Table 1 Manually 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 super user.)	
Inventory; do a print screen from the inventory window.	
Active TCC-I.	Slot 7 or Slot 11 (circle one)
Active XC10G.	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], SNCP[3], etc.); print screens as needed.	
List all protection groups in the system; do a print screen from the protection group window.	

Table 1 Manually Recorded Data (continued)

Item	Record Data Here (if Applicable)
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
3. SNCP = subnetwork connection protection

Step 9 After you have backed up the database, continue with the "NTP-U21 Upgrade Software R3.x to Software R4.0.x" procedure on page 6.

Stop. You have completed this procedure.

NTP-U21 Upgrade Software R3.x to Software R4.0.x

Purpose	Use this procedure to upgrade to R4.0.x software. To upgrade to R4.0.x software successfully, you must read and perform each procedure that applies to your network in the proper order.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-U12 Back Up the Software R3.x Database, page 5
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of a PC or UNIX workstation)
Security Level	Superuser

Step 1 Insert the Release 4.0.x software CD into a PC or workstation CD-ROM drive (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 A traffic interruption of less than 50 ms on each circuit is possible during the activation procedure, with Ethernet traffic disruption possibly lasting up to several minutes on each circuit.

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

Step 2 Log into the node that you want to upgrade. For detailed instructions, refer to the *Cisco ONS SDH 15454 Procedure Guide*. If you are already logged in, continue with Step 3.

Step 3 Verify that your PC is LAN connected to the node that you want to upgrade.

Step 4 As needed, complete the "DLP-U20 Download the Release 4.0.x Software" task on page 7.

If you are downloading software to each node in a ring from a central location, repeat "DLP-U20 Download the Release 4.0.x Software" task on page 7 at each node.

Step 5 Complete the "DLP-U21 Perform an MS-SPRing Lock Out" task on page 8 (MS-SPRing nodes only).

Step 6 Complete the "DLP-U29 Activate the New Load" task on page 9.

Note Only activate one node at a time.

Step 7 As needed, complete the "DLP-U23 Delete Cached JAR Files" task on page 11.

Step 8 Reconnect to CTC using the IP address from Step 6. The new CTC applet for R4.0.x uploads. During this logon, you will need to type the user name CISCO15. A password is not required.

Note Steps 7 and 8 are only necessary after upgrading the first node in a network because cached files only need to be removed from the workstation once. For the remaining nodes, you will still be disconnected and moved to the network view during the node reboot.

Step 9 Complete the "DLP-U24 Remove the Software R4.0.x MS-SPRing Lock Out" task on page 12 (MS-SPRing nodes only).

Step 10 Complete the "DLP-U25 Set the Date and Time" task on page 13 (any nodes not using Simple Network Time Protocol [SNTP]).

Step 11 If the nodes are in path protection configuration or BLSR, repeat Steps 2 through 10 for all nodes in the ring.

All nodes in a ring configuration must be upgraded to R4.0.x software. Mixed software versions in a ring are not supported.

Step 12 Continue with the "NTP-U15 Upgrade the TCC-I Card to the TCC2 Card" procedure on page 13.

Stop. You have completed this procedure.

DLP-U20 Download the Release 4.0.x Software

Purpose	Use this task to download the R4.0.x software to the ONS 15454 SDH nodes prior to activation.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-U12 Back Up the Software R3.x Database, page 5
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of a PC or UNIX workstation)
Security Level	Superuser

Note The TCC-I card has two flash RAMs. An upgrade downloads the software to the backup RAM on both the backup and active TCC-I cards. The download procedure 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 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 to three nodes at once.

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

Note The software download process can take 30 minutes or more per node. It is normal to see flashing LEDs on the TCC-I card. After the active TCC-I is downloaded, the download will automatically begin on the standby side. Normal LED behavior on the standby side is a flashing amber LED and flashing red FAIL.

Step 11 Return to the "NTP-U21 Upgrade Software R3.x to Software R4.0.x" procedure on page 6.

DLP-U21 Perform an MS-SPRing Lock Out

Purpose	You must perform a lock out at each node in the MS-SPRing before activating the software for R4.0.x.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-U12 Back Up the Software R3.x Database, page 5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote (but in the presence of a PC or UNIX workstation)
Security Level	Superuser

Note During the lockout, MS-SPRing spans are not protected. Be sure to remove the lockout after activating all nodes in the ring.

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

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

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

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

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

c. Click **Apply**.

d. Click the **West Switch** column to show the drop-down menu.

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

f. Click **Apply**.

Step 3 Repeat Step 2 at each node in the ring.

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

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

Step 4 Return to the "NTP-U21 Upgrade Software R3.x to Software R4.0.x" procedure on page 6.

DLP-U29 Activate the New Load

Purpose	Use this task to activate Software R4.0.x in each node in the network.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-U12 Back Up the Software R3.x Database, page 5 DLP-U21 Perform an MS-SPRing Lock Out, page 8 (if required) DLP-U20 Download the Release 4.0.x Software, page 7
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of a 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 will download to your PC or workstation as quickly as possible.

Note Make sure 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, make sure that the protect cards are in standby mode before proceeding. Move your mouse cursor over a card in node view to see its active or standby status.

Step 1 To ensure database synchronization, run the memAudit utility:

a. Close all active telnet connections to the ONS 15454.

b. Copy the memAudit.exe from the ONS 15454 software CD or the following Cisco.com web page to a folder on your hard drive or desktop:

http://www.cisco.com/cgi-bin/tablebuild.pl/ons15454

c. In the Windows or Solaris command window, change the prompt to the folder where the memAudit.exe is located.

d. At the prompt, type the following command:

```
memAudit <nodename or IP address>
```

Note Use the full memAudit command with the version numbers. In addition, optional parameters exist for the memAudit command. For more information about the memAudit utility, view the memAudit_readme.htm file on the CD or Cisco.com web page.

The command prompt window displays the following:

```
IP address DB:insync RESET:no:
```

Step 2 Note the IP address of the node. The IP address can either be on the LCD or on the upper left corner of the CTC window.

Step 3 Click the **Alarms** tab and verify that the node has no new alarms. If alarms exist, clear them before proceeding and make sure that the alarm filter is not active.

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

Step 5 Verify that the protect version is 4.0.x.

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.

Note CTC will lose connection to the node and will display the network view.

Step 8 Click **OK** to begin the node rebooting process. A rebooting window appears.

Step 9 After activating the node, wait until the software upgrade reboot finishes at that node before continuing.

During the reboot process, the following occurs:

- The standby TCC-I card reboots. After the standby TCC-I card is fully activated and rebooted, it becomes the active TCC-I card and the other TCC-I card reboots. The TCC-I cards and the XC10G cards in Slot 8 and Slot 10 reboot simultaneously.
- After the TCC-I and XC10G cards reboot, the Ethernet cards reset. G-Series cards reboot consecutively from left to right, and the E-Series cards reboot simultaneously.
- After the Ethernet cards have rebooted, the traffic (line) cards boot consecutively from left to right.

- A system reboot (SYSBOOT) alarm is raised while activation is in progress. After all cards have reset, this alarm clears.

The entire process can take up to 30 minutes, depending on how many cards are installed. After 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 30 minutes for the process to complete, then check to ensure that all alarms have cleared before proceeding.

Caution The upgrade process is service affecting, so Cisco recommends that you activate the new load during a maintenance window. Time-division multiplexing (TDM) traffic can endure an outage of up to 50 ms. Ethernet traffic may remain down from the time the TCC-I cards switch to the time all Ethernet cards have finished resetting.

Note It is normal after this activity for CTC to lose connection with the node and return to network view. The node icon representing the node you are upgrading will be gray. You will receive a "node software incompatible" alarm in network view.

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

Step 11 Return to the "NTP-U21 Upgrade Software R3.x to Software R4.0.x" procedure on page 6.

DLP-U23 Delete Cached JAR Files

Purpose	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	NTP-U12 Back Up the Software R3.x Database, page 5 DLP-U20 Download the Release 4.0.x Software, page 7 DLP-U21 Perform an MS-SPRing Lock Out, page 8 (as needed) DLP-U29 Activate the New Load, page 9
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 a PC or UNIX 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 are not able to delete cached JAR files from your hard drive until you close your browser. If you have other applications open that use JAR files, you must also close them.

Step 3 Delete cached files from your PC (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 and delete all files with "jar" in the Name or Type field.

Step 4 Return to the "NTP-U21 Upgrade Software R3.x to Software R4.0.x" procedure on page 6.

DLP-U24 Remove the Software R4.0.x MS-SPRing Lock Out

Purpose	Release the span lock outs on all MS-SPRing nodes after the new software load is activated on all nodes.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	DLP-U21 Perform an MS-SPRing Lock Out, page 8
Required/As Needed	Required for MS-SPRing
Onsite/Remote	Onsite or remote (but in the presence of a PC or UNIX 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 drop-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 drop-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 BLSR span lock outs on the upgrade nodes.

Step 4 Return to the "NTP-U21 Upgrade Software R3.x to Software R4.0.x" procedure on page 6.

DLP-U25 Set the Date and Time

Purpose	If you are not using SNTP, the upgrade procedure can cause the Date/Time setting to change. Perform this procedure 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 a PC or UNIX workstation)
Security Level	Superuser

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 the "NTP-U21 Upgrade Software R3.x to Software R4.0.x" procedure on page 6.

NTP-U15 Upgrade the TCC-I Card to the TCC2 Card

Purpose	This procedure upgrades the TCC-I card to the TCC2 card. The TCC2 card supports ONS 15454 SDH Software R4.0.x. The TCC-I card supports ONS 15454 SDH Software R3.4 and earlier. The TCC-I card can only be used with Software R4.0.x during the upgrade process.
Tools/Equipment	Two SDH TCC2 cards
Prerequisite Procedures	NTP-U21 Upgrade Software R3.x to Software R4.0.x, page 6
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Maintenance or higher

Note The TCC2 card does not carry any software other than Software R4.0.x. You will not be able to revert to a software release earlier than Software R4.0.x with TCC2 cards installed.

Note The TCC-I card can be used with Software R4.0.x only for TCC2 card upgrade purposes. For example, during a TCC2 card upgrade, some nodes on your network could have Software R4.0.x with TCC-I cards installed, while other nodes have Software R4.0.x with TCC2 cards installed. TCC-I cards running Software R4.0.x are not supported beyond the TCC2 upgrade process because performance issues such as switch times cannot be guaranteed.

Downgrade procedures from TCC2 cards to TCC-I cards are not supported. Contact Cisco Technical Assistance Center (TAC) for more information.

Step 1 Log into CTC. For more detailed instructions, refer to the *Cisco ONS SDH 15454 Procedure Guide*. If you are logged in, continue with Step 2.

Step 2 Verify that the LAN wires on the MIC-C/T/P are installed properly. The TCC2 does not autodetect miswired LAN connections. If a LAN connection is miswired, a "LAN Connection Polarity Reversed" condition appears. For information on backplane pinouts, refer to the *Cisco ONS SDH 15454 Reference Manual*.

Step 3 Verify that the node you are upgrading has ONS 15454 SDH Software R4.0.x installed. The software version is displayed in the upper left corner of the window.

Step 4 Complete the "NTP-U12 Back Up the Software R3.x Database" task on page 5.

Step 5 Physically replace the standby TCC-I card on the ONS 15454 SDH with a TCC2 card.

a. Check the LED on the faceplate. The ACT/STBY LED on the faceplate of the TCC-I or TCC2 card indicates whether the card is in active or standby mode. A green ACT/STBY LED indicates an active card and an amber light indicates a standby card.

b. Open the standby TCC-I card ejectors.

c. Slide the card out of the slot. This raises the IMPROPRMVL alarm which will clear when the upgrade is complete.

d. Open the ejectors on the TCC2 card to be installed.

e. Slide the TCC2 card into the slot along the guide rails.

f. Close the ejectors.

g. In CTC node view, Ldg (loading) appears on the recently installed TCC card.

Caution If your active TCC-I card resets during the upgrade before the new TCC2 card has come to a full standby mode, remove the new TCC2 card immediately.

Note The MEA (card mismatch) alarm appears because CTC recognizes a mismatch between TCC card types. Disregard this alarm; it clears by the end of the procedure.

Note It will take approximately 5 to 10 minutes for the active TCC-I card to transfer the database to the newly-installed TCC2 card. During this operation, the LEDs on the TCC2 flash Fail and then the active/standby LED flashes. When the transfer completes, the TCC2 card reboots and goes into standby mode after approximately 1 to 3 minutes. Do not remove the card from the shelf during a database transfer. The amount of time required for the transfer depends on the size of the database.

Step 6 When the newly installed TCC2 card is in standby, go to the active TCC-I card and right-click the card.

Note You cannot revert to a software release prior to Software R4.0.x after you switch the standby TCC2 card to the active TCC2 card.

Step 7 From the pull-down menu, click **Reset Card**.

Wait for the TCC-I card to reboot. The ONS 15454 SDH switches the standby TCC2 card to active mode. The TCC-I card verifies that it has the same database as the TCC2 card and then switches to standby.

Step 8 Verify that the remaining TCC-I card is now in standby mode (the ACT/STBY LED changes to amber).

Step 9 Physically replace the remaining TCC-I card with the second TCC2 card.

a. Open the TCC-I card ejectors.

b. Slide the card out of the slot. This raises the MEA alarm, which will clear when the upgrade is complete.

c. Open the ejectors on the TCC2 card.

d. Slide the TCC2 card into the slot along the guide rails.

e. Close the ejectors.

The ONS 15454 SDH boots up the second TCC2 card. The second TCC2 card must also copy the database, which can take approximately 10 minutes. Do not remove the card from the shelf during a database transfer.

Note When a newly installed TCC2 card has a different version of the ONS 15454 SDH software installed than the version running on the active TCC2, the newly installed TCC2 card automatically copies the software version running on the active TCC2. You do not need to do anything in this situation. However, the loading TCC2 card does not boot up in the normal manner. When the card is first inserted, the red FAIL LED stays on for a short period. The FAIL LED then blinks normally and all LEDs go dark. The FAIL LED and the ACT/STBY LED flash alternately every 30 to 45 seconds as the new software loads onto the new TCC2 card. After loading the new software for approximately 30 minutes, the TCC2 card becomes the standby card and the amber LED is illuminated.

Step 10 If power-related alarms occur after the second TCC2 card is installed, check the voltage.

Step 11 Perform this procedure again until all nodes on your network are running TCC2 cards with Software R4.0.x installed.

Stop. You have completed this procedure.

NTP-U14 Revert to Previous Software Load and Database

Purpose	Use this procedure to return to the software and database provisioning you had before you activated Software R4.0.x.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-U21 Upgrade Software R3.x to Software R4.0.x, page 6
Required/As Needed	As needed
Onsite/Remote	Onsite or remote (but in the presence of a PC or UNIX workstation)
Security Level	Superuser

Note To revert from Software R4.0.x to R3.4, TCC-I cards are required. You cannot perform this procedure if TCC2 cards are installed.

Note The procedures 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 R4.0.x, you should have backed up the existing database at all nodes in the network. (This is part of the "NTP-U12 Back Up the Software R3.x 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 procedures, in order.

Step 1 Log into the node. For detailed instructions, refer to the *Cisco ONS SDH 15454 Procedure Guide*. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-U21 Perform an MS-SPRing Lock Out" task on page 8 (MS-SPRing only).

Step 3 Complete the "DLP-U26 Revert to Protect Load" task on page 17.

Step 4 Complete the "DLP-U24 Remove the Software R4.0.x MS-SPRing Lock Out" task on page 12 (MS-SPRing only).

Step 5 If you need to revert to Software R3.x or the revert to a later release failed, complete the DLP-U27 Manually Restore the Database, page 18.

Stop. You have completed this procedure.

DLP-U26 Revert to Protect Load

Purpose	Use this task to revert to the software you were running prior to the last activation. This procedure also restores your database to the provisioning you had prior to the activation.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-U11 Prepare for Release 3.x to Release 4.0.x Upgrade, page 2 NTP-U12 Back Up the Software R3.x Database, page 5 NTP-U21 Upgrade Software R3.x to Software R4.0.x, page 6
Required/As Needed	Required for revert
Onsite/Remote	Onsite or remote (but in the presence of a PC or UNIX workstation)
Security Level	Superuser

Note To perform a supported (non-service-affecting) revert from Software R4.0.x, the release you want to revert to must have been working at the time you activated CTC Software R4.0.x 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 In node view, click the **Maintenance** > **Software** tabs.

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

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

Caution A traffic interruption of less than 50 ms on each circuit is possible during the activation procedure, with Ethernet traffic disruption possibly lasting up to several minutes on each circuit.

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.

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 cache files from your browser's directory or from the TEMP directory on your MS Windows PC. If you have trouble reconnecting to CTC, complete the "DLP-U23 Delete Cached JAR Files" task on page 11.

Step 9 Return to the "NTP-U14 Revert to Previous Software Load and Database" procedure on page 16.

DLP-U27 Manually Restore the Database

Purpose	Use this task to revert to Release 3.x or if you were unable to perform a revert using another software release.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	"DLP-U26 Revert to Protect Load" task on page 17, and "DLP-U24 Remove the Software R4.0.x MS-SPRing Lock Out" task on page 12 (if required)
Required/As Needed	As needed
Onsite/Remote	Onsite or remote (but in the presence of a PC or UNIX workstation)
Security Level	Superuser

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

Caution A traffic interruption of less than 50 ms on each circuit is possible during the activation procedure, with Ethernet traffic disruption possibly lasting up to several minutes on each circuit.

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

Step 1 In 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 TCC-I cards reboot.

Step 4 After the TCC-I cards have rebooted, log back into CTC and verify that the database is restored.

Step 5 Wait one minute before restoring the next node.

Step 6 Return to the "NTP-U14 Revert to Previous Software Load and Database" procedure on page 16.

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/univercd/home/home.htm

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

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).

Documentation Feedback

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

Cisco Technical Support Website

The Cisco Technical Support 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, 365 days a year at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support 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

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 automatically provides recommended solutions. If your issue is not resolved using the recommended resources, your service request will be assigned to a Cisco TAC 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 TAC 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)—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.

Severity 2 (S2)—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.

Severity 3 (S3)—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.

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.

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

  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 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

- *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

- 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 Cisco ONS 15454 SDH Release 4.0 documentation.

Printed in the USA on recycled paper containing 10% postconsumer waste.