Upgrading Cisco ONS 15454 SDH Release 3.3 to Release 3.4 Using the TCC-I Card

This document explains how to upgrade the Cisco ONS 15454 SDH Cisco Transport Controller (CTC) software from Software R3.3 to Software R3.4 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 Procedures in this chapter 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 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 wish 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.

- Section 1.1 Prepare for Release 3.3 to Release 3.4 Upgrade, page 2—Review this critical information and complete these critical procedures before beginning the upgrade process.
- Section 1.2 Back Up the Database, page 4—Complete the database backup to ensure that you have preserved your node and network provisioning in the event that you need to restore them.
- Section 1.1 Upgrade the Software, page 6—Complete these procedures to upgrade the software. You must complete the entire procedure before the upgrade is finished.
- Section 1.2 Revert to Previous Load, page 13—Complete this procedure only if you need to return to the software load you were running before activating the Release 3.4 software.

Cisco Systems

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

1.1 Prepare for Release 3.3 to Release 3.4 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 Release 3.4 software.
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite or remote

Step 1 Read the *Release Notes for Cisco ONS 15454 SDH Release 3.4*.

Step 2 Complete the "Verify the CTC PC or UNIX Workstation" procedure on page 2.

Step 3 Complete the "Verify IP Addresses" procedure on page 3.

Step 4 Complete the "Verify LAN Connections" procedure on page 3.

Step 5 Complete the "Verify Common Control Cards" procedure on page 4.

Step 6 When you have completed the procedures for this section, proceed with the "1.2 Back Up the Database" section on page 4.

Verify the CTC PC or UNIX Workstation

Purpose	Before upgrading the software to CTC Release 3.4, 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)

Step 1 Ensure that your Windows or UNIX workstation is either 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

Step 2 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 Service Pack 2 or higher

Step 3 Ensure that you have Java Policy and Java Runtime Environment (JRE), Release 1.3.1_02. (JRE 1.3.1.02 is included on the ONS 15454 SDH software CD.)

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 4 After you have verified that your PC or workstation meets CTC Release 3.4 requirements, proceed to the "Verify IP Addresses" procedure on page 3.

Verify IP Addresses

Purpose	Use this procedure to ensure that there are no IP address conflicts with CTC.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	"Verify the CTC PC or UNIX Workstation" procedure on page 2
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of a PC or UNIX workstation)

Step 1 Disable all other Ethernet devices (such as a dial-up adapter) on a PC or workstation that runs CTC.

Step 2 If you have multiple IP addresses on your PC or workstation, you should remove them; you cannot install CTC Release 3.4 if multiple IP addresses are configured.

Step 3 You have completed the IP address check procedure. Now perform the "Verify LAN Connections" procedure on page 3.

Verify LAN Connections

Purpose	Use this procedure to ensure that LAN connections are correct.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	"Verify IP Addresses" procedure on page 3
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of a PC or UNIX workstation)

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 Installation and Operations Guide, Release 3.4* for LAN-connection suggestions.

Step 2 After verifying that your LAN is properly configured, proceed to the "Verify Common Control Cards" procedure on page 4.

Verify Common Control Cards

Purpose	You must now use CTC to check 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	"Verify LAN Connections" procedure on page 3
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of a PC or UNIX workstation)

Step 1 Log into a node.

Step 2 Ensure that Slots 7, 8, 10, and 11 have cards installed. Release 3.x does not support simplex operation.

Step 3 Repeat Steps 1 and 2 at every node in the network.

Step 4 You have completed the verification of duplex common control cards. Proceed to the "1.2 Back Up the Database" procedure on page 4.

1.2 Back Up the Database

Purpose	Use this procedure to preserve all configuration data for your network before performing the upgrade.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	"1.1 Prepare for Release 3.3 to Release 3.4 Upgrade" section on page 2
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of a PC or UNIX workstation)

Step 1 Complete the "Back Up the Software" procedure on page 4.

Step 2 Complete the "Perform a Manual Backup" procedure on page 5.

Step 3 After you have backed up the database, proceed to the "1.1 Upgrade the Software" section on page 6.

Back Up the Software

Purpose	Before upgrading from Release 3.3 to Release 3.4 software, you must back up the current database for all nodes in the network.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	"1.1 Prepare for Release 3.3 to Release 3.4 Upgrade" section on page 2
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of a PC or UNIX workstation)

Step 1 Log into CTC.

Step 2 From the node 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, for example 1010120192.db).

Step 5 Click **Save**. A message appears indicating that the backup is complete.

Step 6 Click **OK**.

Step 7 Repeat Steps 1 to 6 for each node in the network.

Step 8 You have completed the software backup. Proceed to the "Perform a Manual Backup" procedure on page 5.

Perform a Manual Backup

Purpose	Cisco recommends that you manually log critical information by either writing it down or by printing screens where applicable. This procedure is optional after you have backed up the database.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	"Back Up the Software" procedure on page 4
Required/As Needed	Recommended
Onsite/Remote	Onsite or remote (but in the presence of a PC or UNIX workstation)

Step 1 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 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[1], SNCP[2], etc.); print screens as needed.	

Table 1 Manually Recorded Data (continued)

Item	Record data here (if applicable)
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. MS-SPRing = multiplex section-shared protection ring
2. SNCP = subnetwork connection protection

Step 2 After you have backed up all databases and recorded all necessary information using the checklist, you can begin the "1.1 Upgrade the Software" procedure on page 6.

1.1 Upgrade the Software

Purpose	Use this procedure to upgrade your CTC software. To upgrade the 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	"1.2 Back Up the Database" procedure on page 4
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of a PC or UNIX workstation)

Step 1 Insert the Release 3.4 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 60 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 Complete the "Download the Release 3.4 Software" procedure on page 7 (all nodes).

Step 3 Complete the "Perform an MS-SPRing Lockout" procedure on page 8 (MS-SPRing nodes only).

Step 4 Complete the "Activate the New Load" procedure on page 9 (all nodes).

Step 5 Complete the "Delete Cached JAR Files" procedure on page 10.

Step 6 Complete the "Remove the MS-SPRing Lockout" procedure on page 11 (MS-SPRing nodes only).

Step 7 Complete the "Set the Date and Time" procedure on page 12 (any nodes not using Simple Network Time Protocol [SNTP]).

Step 8 Complete the "Upgrade Spare TCC-I Cards" procedure on page 13 (as needed for upgrading spare TCC-I cards).

Step 9 Complete the "Download the Release 3.4 Software" procedure on page 7.

Download the Release 3.4 Software

Purpose	Use this procedure to download the Release 3.4 software to the ONS 15454 SDH nodes prior to activation.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	"1.2 Back Up the Database" section on page 4
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of a PC or UNIX workstation)

Note There are two flash RAMs on the TCC-I card. 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 Check all nodes in the ring 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 2 From the CTC network view, click the **Maintenance** > **Software** tabs.

Step 3 Click **Download**. The Download Selection dialog box appears.

Step 4 Browse to locate the software files on the ONS 15454 SDH System Software CD (or on your hard drive, if you are working from a local copy).

Step 5 Open the Cisco15454SDH folder.

Step 6 Select the file with the .pkg extension and click **Open**.

Step 7 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 3 nodes at once.

Step 8 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.

Step 9 After you have successfully downloaded the CTC Release 3.4 software to each node you are upgrading, perform the "Perform an MS-SPRing Lockout" procedure on page 8. If none of your nodes participate in an MS-SPRing, you can skip the MS-SPRing lockout and begin the "Activate the New Load" procedure on page 9.

Perform an MS-SPRing Lockout

Purpose	If any of the nodes you are upgrading are in an MS-SPRing configuration, you must perform a span lockout at each node in the ring before activating the software for Release 3.4. Perform this procedure to issue a span lockout on an MS-SPRing using CTC Release 3.3.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	"Download the Release 3.4 Software" procedure on page 7
Required/As Needed	Required for MS-SPRing
Onsite/Remote	Onsite or remote (but in the presence of a PC or UNIX workstation)

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 Click the **Maintenance** > **Ring** tabs.

Step 2 For each of the MS-SPRing trunk cards (STM-4, STM-16, STM-64), go to the row in the table for that card and perform the following steps:

- **a.** Click the **East Switch** column to show the pull-down menu.
- **b.** From the menu options, choose **Span Lockout**.
- **c.** Click the **West Switch** column to show the pull-down menu.
- **d.** From the menu options, choose **Span Lockout**.
- **e.** Click **Apply** to activate the command.

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

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

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

Step 4 You have completed the MS-SPRing lockout. You must now perform the "Activate the New Load" procedure on page 9.

Activate the New Load

Purpose	Use this procedure to log into and activate each node in the network.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	Perform the "Download the Release 3.4 Software" procedure on page 7. "Perform an MS-SPRing Lockout" procedure on page 8 first if any of the nodes you are upgrading are in an MS-SPRing configuration.
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of a PC or UNIX workstation)

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.

Step 1 Log into a node.

Step 2 Record the IP address of that node.

Step 3 Verify that the node has no new alarms. If alarms exist, clear them before proceeding.

Step 4 From the CTC node view, click the **Maintenance** > **Software** tabs.

Step 5 Verify that the protect version is 3.4.

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** to begin the node rebooting process.

Step 9 After activating the node, wait until the software upgrade reboot finishes at that node before continuing. A system reboot (SYSBOOT) alarm is raised while activation is in progress. After all cards have reset, this alarm clears.

Each card in the node reboots, beginning with the standby TCC-I. After the standby TCC-I is fully activated and fully rebooted, it becomes the active TCC-I and the other TCC-I reboots. When the TCC-I cards are finished, the XC10G in Slot 8 reboots, and then the XC10G in Slot 10 reboots. Next, the Ethernet cards reset all at once, then the line cards boot consecutively from left to right. The whole process can take up to 30 minutes, depending on how many cards are installed. This 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. Expect Ethernet traffic to remain down from the time the TCC-I cards switch to the time all Ethernet cards have finished resetting. 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.)

Note Steps 10 to 12 are only necessary after upgrading the first node. For the remaining nodes, you will still be disconnected and moved to the network view during the node reboot, but after the reboot is complete, CTC will restore connectivity to the node.

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

Step 11 Follow all steps in the "Delete Cached JAR Files" procedure on page 10, then continue here with Step 12.

Step 12 Reconnect to CTC using the IP address from Step 2. (If the IP address is still in the browser location bar, you can simply hold down the **Shift** key and click the browser **Reload** or **Refresh** button.) The new CTC applet for Release 3.4 uploads. Because CTC Release 3.4 is backwardly compatible with CTC Release 3.3, the network view is visible while you are upgrading.

Note Only activate one node at a time.

Step 13 Perform Steps 1 to 9 for each of the remaining nodes. The activation must be performed for every node that is running CTC Software R3.3. Allow each node to finish (all alarms cleared for 10 minutes) before activating the next node.

Step 14 You have completed the activation procedure when you have activated all nodes with CTC Software R3.4. If you performed an MS-SPRing lockout before you began activation, you must now perform the "Remove the MS-SPRing Lockout" procedure on page 16, then go to the "Set the Date and Time" procedure on page 12.

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	Steps 1 to 10 of the "Activate the New Load" procedure on page 9
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of a PC or UNIX workstation)

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 variable "TEMP." The value associated with this variable is the path to your temporary directory where jar files are stored.

d. Open the temporary directory located in the path you just looked up.

e. Choose **View > Details**.

f. Select and delete all files with "jar" in either the name or type field.

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

Step 5 After deleting cached jar files, you should return to the referring procedure (either the "Activate the New Load" procedure on page 9, or the "Revert to Protect Load" procedure on page 15) and continue with the steps there.

Remove the MS-SPRing Lockout

Purpose	Release the span lockouts on all MS-SPRing nodes after the new software load is activated on all nodes. This procedure restores an MS-SPRing using Software R3.4.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	"Delete Cached JAR Files" procedure on page 10; Steps 1 to 13 of the "Activate the New Load" procedure on page 9
Required/As Needed	Required for MS-SPRing
Onsite/Remote	Onsite or remote (but in the presence of a PC or UNIX workstation)

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

Step 2 For each of the MS-SPRing trunk cards (STM-4, STM-16, or STM-64), go to the row in the table for that card and perform the following steps:

a. 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 after 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 You might need to accept a new ring map to clear Default K byte or Node ID mismatch alarms.

a. From the **Provisioning** > **MS-SPRing** tabs, click the **Ring Map** button.

b. If a new ring map exists, click **Accept**.

Step 4 When all MS-SPRing span lockouts are released, you have completed this procedure. Go to the "Set the Date and Time" procedure on page 12.

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	If required, perform the "Remove the MS-SPRing Lockout" procedure on page 11; then "Delete Cached JAR Files" procedure on page 10 and "Activate the New Load" procedure on page 9
Required/As Needed	As needed
Onsite/Remote	Onsite or remote (but in the presence of a PC or UNIX workstation)

Note If you are using SNTP, you do not need this procedure and can go to the "Upgrade Spare TCC-I Cards" procedure on page 13.

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 When all nodes have the correct date and time settings, go to the "Upgrade Spare TCC-I Cards" procedure on page 13.

Upgrade Spare TCC-I Cards

Purpose	Perform this procedure to upgrade all spare TCC-I cards to CTC Software R3.4. The provisioning database will also be copied to the spare TCC-I cards.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	"Remove the MS-SPRing Lockout" procedure on page 11 if required; otherwise, "Activate the New Load" procedure on page 9 and "Delete Cached JAR Files" procedure on page 10
Required/As Needed	Required for all spare TCC-I cards
Onsite/Remote	Onsite or remote (but in the presence of a PC or UNIX workstation)

Step 1 To upgrade a spare TCC-I, place it in the standby slot of a node running Software R3.4. The card upgrades automatically from the active TCC-I.

The standby TCC-I copies one or both software releases from the active TCC-I, as needed. Each software copy takes about 15 minutes, and the TCC-I resets after each copy. Thus, for a TCC-I that has no matching software with the active TCC-I, you should expect to see two TCC-I resets, lasting about 30 minutes total.

Note During the TCC-I upgrade, the LEDs on the upgrading card flash alternately between **Fail** and **Standby**.

Step 2 After you have upgraded all of your spare TCC-I cards, you have completed the software upgrade.

1.2 Revert to Previous Load

Purpose	Use this procedure to return to the exact software and database provisioning you had before you activated Software R3.4.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	"1.1 Prepare for Release 3.3 to Release 3.4 Upgrade" section on page 2, "1.2 Back Up the Database" section on page 4, and "1.1 Upgrade the Software" section on page 6 (up to and including the "Activate the New Load" procedure on page 9, and the "Remove the MS-SPRing Lockout" procedure on page 16, if applicable)
Required/As Needed	As needed
Onsite/Remote	Onsite or remote (but in the presence of a PC or UNIX workstation)

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 from Software R3.3 to Software R3.4, you should have backed up the existing database at all nodes in the network. (This is part of the "1.2 Back Up the Database" procedure on page 4.) 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 Complete the "Perform an MS-SPRing Lockout" procedure on page 14 (MS-SPRing only).

Step 2 Complete the "Revert to Protect Load" procedure on page 15.

Step 3 Complete the "Remove the MS-SPRing Lockout" procedure on page 16 (MS-SPRing only).

Note The "Manually Restore the Database" procedure on page 16 is provided for reference only. Do not complete this procedure unless an attempt to revert has failed.

Step 4 After you have completed the necessary steps above, the revert is complete.

Perform an MS-SPRing Lockout

Purpose	If you have an MS-SPRing provisioned, before beginning the revert you must perform a span lockout at each node. Perform this procedure to issue a span lockout on an MS-SPRing using CTC Software R3.4.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	"1.1 Prepare for Release 3.3 to Release 3.4 Upgrade" section on page 2; "1.2 Back Up the Database" section on page 4; "1.1 Upgrade the Software" section on page 6 (up to and including the "Activate the New Load" procedure on page 9, and the "Perform an MS-SPRing Lockout" procedure on page 8)
Required/As Needed	Required for MS-SPRing only
Onsite/Remote	Onsite or remote (but in the presence of a PC or UNIX workstation)

Step 1 If you have an MS-SPRing provisioned, before beginning the revert you must perform a span lockout at each node. Follow the "Perform an MS-SPRing Lockout" procedure on page 8 to perform a span lockout on an MS-SPRing using CTC Software R3.4.

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

Step 2 After you have performed the MS-SPRing lockout on all MS-SPRing nodes, perform the "Revert to Protect Load" procedure on page 15.

Revert to Protect Load

Purpose	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	"1.1 Prepare for Release 3.3 to Release 3.4 Upgrade" section on page 2; "1.2 Back Up the Database" section on page 4; "1.1 Upgrade the Software" section on page 6 (up to and including the "Activate the New Load" procedure on page 9, and the "Remove the MS-SPRing Lockout" procedure on page 16, if applicable); "Perform an MS-SPRing Lockout" procedure on page 8 (if required)
Required/As Needed	Required for revert
Onsite/Remote	Onsite or remote (but in the presence of a PC or UNIX workstation)

Note To perform a supported (non-service-affecting) revert from Software R3.4, the release you wish to revert to must have been working at the time you activated CTC Software R3.4 on that node. A supported revert automatically restores the node configuration to its state 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 3.3 (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.

Caution A traffic interruption of less than 60 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 After reverting the node, wait until the software revert finishes at that node before continuing.

Note Be patient. 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 for Software R3.3 to your PC or 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 "Delete Cached JAR Files" procedure on page 10.

Step 9 Remove any MS-SPRing lockout using the "Remove the MS-SPRing Lockout" procedure on page 11.

Remove the MS-SPRing Lockout

Purpose	To restore MS-SPRing protection, you must clear the span lockouts on all MS-SPRing nodes after reverting the software load and restoring the database on all nodes. Use the following procedure to restore an MS-SPRing using Software R3.x.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	"Perform an MS-SPRing Lockout" procedure on page 8, and "Revert to Protect Load" procedure on page 15
Required/As Needed	Required for MS-SPRing
Onsite/Remote	Onsite or remote (but in the presence of a PC or UNIX workstation)

Step 1 To restore MS-SPRing protection, you must clear the span lockouts on all MS-SPRing nodes after reverting the software load and restoring the database on all nodes. Complete the "Remove the MS-SPRing Lockout" procedure on page 11 to restore an MS-SPRing using Software R3.x.

Step 2 You have now completed the software revert procedure. All nodes should be provisioned as they were before the last activation; however, in case of trouble, Cisco provides the "Manually Restore the Database" procedure on page 16 to retrieve your databases.

Manually Restore the Database

Purpose	The revert procedure should have restored your Software R3.x database completely; however, as a precaution, Cisco includes here the steps to restore the pre-upgrade database manually. **Caution** Do not perform these steps unless the software revert failed.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	"Revert to Protect Load" procedure on page 15, and "Remove the MS-SPRing Lockout" procedure on page 11 (if required)
Required/As Needed	As needed
Onsite/Remote	Onsite or remote (but in the presence of a PC or UNIX workstation)

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

Caution A traffic interruption of less than 60 ms on each circuit is possible during the activation procedure, with Ethernet traffic disruption possibly lasting up to several minutes on each circuit.

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

Step 2 Click **Backup**. 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.

You have now completed the manual database backup.

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