



Upgrading the Cisco ONS 15454 SDH to Release 8.0

This document explains how to upgrade Cisco ONS 15454 SDH Cisco Transport Controller (CTC) software from Software Releases 5.0.x, 6.0.x, 6.1.x, 7.0 or 7.2 to Release 8.0.x, using the Advanced Timing, Communications, and Control (TCC2) or Advanced Timing, Communications, and Control Plus (TCC2P) card.



Note

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

Contents

This document contains the following information:

- [Before You Begin, page 2](#)
- [Errorless Upgrades and Exceptions, page 3](#)
- [XC-VXC-10G, page 3](#)
- [XC-VXL-10G/XC-VXL-2.5G, page 4](#)
- [XC10G, page 5](#)
- [Document Procedures, page 5](#)
- [NTP-U213 Prepare for Upgrade to ONS 15454 SDH Software Release 8.0, page 6](#)
- [DLP-U318 Verify CTC PC or UNIX Workstation Requirements, page 6](#)
- [DLP-U319 Verify Common Control Cards, page 8](#)
- [NTP-U214 Back Up the Software Database, page 8](#)
- [NTP-U215 Upgrade to ONS 15454 SDH Release 8.0, page 10](#)
- [DLP-U320 Download ONS 15454 SDH Release 8.0 Software, page 12](#)
- [DLP-U321 Perform an MS-SPRING Lockout, page 13](#)
- [DLP-U322 Activate the New ONS 15454 SDH Software Load, page 15](#)



Corporate Headquarters:

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

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

- [DLP-U323 Delete Cached JAR Files, page 19](#)
- [DLP-U324 Remove the MS-SPRing Lockout, page 20](#)
- [DLP-U325 Set the Date and Time, page 20](#)
- [NTP-U216 Install Public-Key Security Certificate, page 21](#)
- [NTP-U217 Revert to Previous Software Load and Database, page 22](#)
- [DLP-U326 Revert to Protect Load, page 23](#)
- [DLP-U327 Manually Restore the Database, page 24](#)
- [NTP-U218 Upgrade to ONS 15454 SDH Release 8.0 Using TL1, page 25](#)
- [Related Documentation, page 30](#)
- [Release-Specific Documents, page 30](#)
- [Platform-Specific Documents, page 30](#)
- [Obtaining Documentation, page 31](#)
- [Cisco.com, page 31](#)
- [Product Documentation DVD, page 31](#)
- [Cisco Optical Networking Product Documentation CD-ROM, page 31](#)
- [Ordering Documentation, page 32](#)
- [Reporting Security Problems in Cisco Products, page 33](#)
- [Obtaining Technical Assistance, page 33](#)
- [Cisco Technical Support & Documentation Website, page 33](#)
- [Obtaining Additional Publications and Information, page 35](#)

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 dialup number.



Caution

Read all procedures before you begin the upgrade.



Caution

This upgrade is supported only for Software upgrade from Software R5.0.x, Software R6.0.x, Software R6.1.x, Software R7.0, and Software R7.2 upgrading to Software R8.0.x. 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 33.



Note

Software R8.0 supports parallel upgrades for multiple nodes in a network. In a parallel upgrade you can still activate only one node at a time; however, you can begin activation of the next node as soon as the controller cards for the current node have rebooted successfully.

Errorless Upgrades and Exceptions

The following tables define where errorless upgrades are expected for R8.0, and where exceptions can occur. Please review [Table 1 on page 3](#), [Table 2 on page 4](#) or [Table 3 on page 5](#) for your particular cross-connect card type.



Caution

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



Caution

G-Series cards (G1000-4 and G1000) purchased prior to Software R7.2 incur a traffic hit of 2 to 3 minutes per card during activation, while a field-programmable gate array (FPGA) upgrade to the card takes place. Cards thus upgraded also incur the same traffic hit if the software is subsequently reverted, as the FPGA is downgraded in the case of such a revert.



Note

Upgrades for dense wavelength division multiplexing (DWDM) configurations are expected to be errorless with the following exception:

The MXP_MR_2.5 and MXPP_MR_2.5 cards automatically download a new FPGA image during a software upgrade from a software release prior to 7.0 to the Software R8.0. For cards with no Y-cable protection, the data path incurs a traffic hit of up to 10 seconds (typically less). Y-cable-protected cards with Fibre Channel (FC) payloads incur an FC link reinitialization as traffic switches away from the card downloading the new FPGA image. Y-cable-protected cards with Gigabit Ethernet (GE) payloads are not expected to incur a traffic hit.



Note

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

XC-VXC-10G

[Table 1](#) applies to nodes equipped with XC-VXC-10G cards.

Table 1 XC-VXC-10G

Card Type	Expected Traffic Effect
E1	Errorless
E3	Errorless
E1-42	Errorless
DS3I	Errorless
STMn (including STM64-XFP and STM1E)	Errorless
MRC-12	Errorless
ML-Series Ethernet	Traffic hits 3 to 8 minutes (approximately)

Table 1 XC-VXC-10G (Continued)

Card Type	Expected Traffic Effect
G-Series Ethernet	Errorless (except as noted)
E-Series and CE-Series Ethernet	Errorless

XC-VXL-10G/XC-VXL-2.5G

Table 2 applies to nodes equipped with XC-VXL-10G or XC-VXL-2.5G cards.

Table 2 XC-VXL-10G/XC-VXL-2.5G

Card Type	Expected Traffic Effect
E1	Errorless
E3	Errorless
E1-42	Errorless
DS3I	Errorless
STMn (including STM64-XFP and STM1E)	Errorless
MRC-12	Errorless
ML-Series Ethernet	Traffic hits 3 to 8 minutes (approximately)
G-Series Ethernet	Errorless (except as noted)
E-Series and CE-Series Ethernet	Errorless

XC10G

Table 3 applies to nodes equipped with XC10G cards.

Table 3 XC10G

Card Type	Expected Traffic Effect
E-1	Errorless
E-3	Errorless
STM1E	Errorless
FMEC-DS1/E1	Errorless
FMEC-E1	Errorless
OC-N (including MRC-12 and OC192-XFP)	Errorless
E-Series Ethernet	Traffic hits up to 5 minutes (approximately)
ML-Series Ethernet	Traffic hits 3 to 8 minutes (approximately)
G-Series Ethernet	Errorless (except as noted)

Document Procedures

Procedures in this document are to be performed in consecutive order unless otherwise noted. In general, you are not done with a procedure until you have completed it for each node you are upgrading, and you are not done with the upgrade until you have completed each procedure that applies to your network. If you are new to upgrading the ONS 15454 SDH, you might 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-U213 Prepare for Upgrade to ONS 15454 SDH Software Release 8.0, page 6](#)—This section contains critical information and tasks that you must read and complete before beginning the upgrade process.
2. [NTP-U214 Back Up the Software Database, page 8](#)—Complete the database backup to ensure that you have preserved your node and network provisioning in the event that you need to restore them.



Caution

You must back up the database when using a multiplex section-shared protection ring (MS-SPRing) configuration.

3. [NTP-U215 Upgrade to ONS 15454 SDH Release 8.0, page 10](#)—You must complete this entire procedure before the upgrade is finished.

4. [NTP-U216 Install Public-Key Security Certificate, page 21](#)—You must complete this procedure to be able to run ONS 15454 SDH Software R8.0.
5. [NTP-U217 Revert to Previous Software Load and Database, page 22](#)—Complete this procedure only if you need to return to the software load you were running before activating Software R8.0.
6. [NTP-U218 Upgrade to ONS 15454 SDH Release 8.0 Using TL1, page 25](#)—Complete this procedure only if you want to upgrade to Software R8.0 using Transaction Language (TL1).

NTP-U213 Prepare for Upgrade to ONS 15454 SDH Software Release 8.0

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 Software R8.0
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 8.0*.
- 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-U318 Verify CTC PC or UNIX Workstation Requirements](#)” task on page 6.
- Step 4** Complete the “[DLP-U319 Verify Common Control Cards](#)” task on page 8.
- Step 5** When you have completed the tasks for this section, proceed with the “[NTP-U214 Back Up the Software Database](#)” procedure on page 8.
- Stop. You have completed this procedure.**
-

DLP-U318 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 R8.0.
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 one of the following:
- IBM-compatible PC with a Pentium III/700 or faster processor, CD-ROM drive, a minimum of 384 MB RAM and 190 MB of available hard drive space, running Windows 98, Windows NT 4.0 (with Service Pack 6a), Windows 2000 Professional (with Service Pack 3), or Windows XP Professional (with Service Pack 1)
 - UNIX workstation with Solaris Versions 8 or 9, on an UltraSPARC or faster processor, with a minimum of 384 MB RAM and a minimum of 190 MB of available hard drive space

- Step 2** Ensure that your web browser software is one of the following:
- Netscape Navigator 7.x or higher on Windows
 - Internet Explorer 6.x or higher on Windows
 - Mozilla 1.7 or higher on Solaris



Note Cisco recommends you use either Internet Explorer 6.x or Netscape 7.x for Windows workstations running Software R8.0. However, if you upgrade to Netscape 7 or JRE 5.0 and you still need to launch CTC directly from nodes running software prior to R4.6, you must first run the pre-caching utility supplied in the setup program on the software CD. Run the pre-caching utility during the activation ([Step 16](#) on [page 17](#)) in this case.

- Step 3** Verify that the following are installed on your computer:
- - Java Runtime Environment (JRE) 5.0
 - - Java Plug-in 5.0
 - - Java Policy file



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



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



Note To install JRE 5.0, the Java Policy file, or the Software R8.0 online help, refer to the installation instructions in the *Cisco ONS 15454 SDH Procedure Guide*.

- Step 4** Return to your originating procedure (NTP).

DLP-U319 Verify Common Control Cards

Purpose	This task verifies that two TCC2 or TCC2P cards and two XC-VXL-10G, XC-VXL-2.5G, XC-VXC-10G, or XC-10G cards (SDH only) are installed at each node, as appropriate for your network configuration.
Tools/Equipment	PC or UNIX workstation with CTC installed
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of the workstation)
Security Level	Superuser


Note

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


Note

DWDM nodes need only TCC2/TCC2P cards installed during the upgrade.

- Step 1** Ensure that the cards are installed. The TCC2 or TCC2P cards are in Slots 7 and 11 and the XC-VXL-10G, XC-VXL-2.5G, XC-VXC-10G, or XC-10G cards (as needed for SDH operation) are in Slots 8 and 10. Software R8.0 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-U214 Back Up the Software Database

Purpose	This procedure preserves all configuration data for your network before performing the upgrade.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-U213 Prepare for Upgrade to ONS 15454 SDH Software Release 8.0, page 6
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of the workstation)
Security Level	Maintenance or higher; Superuser, if performing optional Step 10


Caution

You must back up the database when using an MS-SPRing configuration.

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

- Step 4** In the Database Backup dialog box, click the **Browse** button, then navigate to a local PC directory or network directory and type a database name (such as database15454SDH010107.db) in the File Name field.
- Step 5** In the Database Backup dialog box, click the **OK** button. If you are overwriting an existing file, click **Yes** in the confirmation dialog box.
- Step 6** In the Database Backup dialog box, check the **Alarms** and the **Performance** check boxes in order to choose these database items in addition to provisioning information.



Note The Provisioning selection in the Database Backup dialog box is a default component of the backup file, and this selection is dimmed.

- Step 7** Click the **Save** button to save the database on the workstation's hard drive or on a network storage location.
- Step 8** When the backup is complete, click **OK**.
- Step 9** Repeat Steps 1 through 8 for each node in the network.
- Step 10** (Optional) Cisco recommends that you manually log critical information by either writing it down or printing screens where applicable. Use Table 4 to determine the information you should log; complete the table (or your own version) for every node in the network.

Table 4 *Manually Recorded Data*

Item	Record Data Here
IP address of the node.	
Node name.	
Timing settings.	
DCC ¹ connections; list all optical ports that have DCCs activated.	
User IDs; list all, including at least one Superuser.	
Inventory; do a print screen from the Inventory window.	
Active TCC2/TCC2P.	Slot 7 or Slot 11 (circle one)
Active XC-VXL-10G, XC-VXL-2.5G, XC-10G, or XC-VXC-10G.	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, 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

Stop. You have completed this procedure.

NTP-U215 Upgrade to ONS 15454 SDH Release 8.0

Purpose	This procedure upgrades your CTC software to Software R8.0.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-U214 Back Up the Software Database, page 8
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of the workstation)
Security Level	Superuser


Caution

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


Caution

When managing end-to-end circuits participating in an ML-Series RPR ring across multiple nodes involved in a parallel upgrade, all nodes participating in these circuits must have completed the activation before the end-to-end traffic will resume.


Note

When a software upgrade from earlier to R8.0 to R8.0 is made, the optical threshold defaults of R8.0 are applied and all previously configured optical threshold defaults are lost. To view new default settings, go to card view and click **Provisioning > Defaults** pane. These settings apply to ADM-10G, MXP-2_5G-10E, MXP-2_5G-10G, MXP-MR-10DME, MXP-MR-2_5G, MXPP-MR-2_5G, TXP-MR-10E, TXP-MR-10G, TXP-MR-2_5G, TXPP-MR-2_5G, 10GE-XP, and GE-XP cards.

Step 1

Insert the Software R8.0 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 Java Setup Wizard. You can use the setup wizard to install components or click the **Cancel** button to continue with the upgrade.

Step 2

Complete the “[DLP-U320 Download ONS 15454 SDH Release 8.0 Software](#)” task on page 12 for all nodes (or groups of eight or less nodes) you are upgrading.


Caution

You must back up the database when using an MS-SPRing configuration.

Step 3

For MS-SPRing nodes only, complete the “[DLP-U321 Perform an MS-SPRing Lockout](#)” task on page 13.

Step 4

Complete the “[DLP-U322 Activate the New ONS 15454 SDH Software Load](#)” task on page 15 for all nodes you are upgrading.


Note

You can activate only one node at a time; however, you can begin activation of the next node as soon as the controller cards for the current node have rebooted successfully (wait 5 minutes from the time the SYSBOOT alarm is raised).

- Step 5** If necessary, complete the “[DLP-U323 Delete Cached JAR Files](#)” task on page 19 for all nodes, or groups of nodes you are upgrading a second time.

**Caution**

If you download Software R8.0 a second time following activation you can not revert to the previous software version.

- Step 6** (Optional) If you wish to ensure that a software revert to the previous software release is no longer be possible, complete the “[DLP-U320 Download ONS 15454 SDH Release 8.0 Software](#)” task on page 12 a second time.

- Step 7** Complete the “[DLP-U324 Remove the MS-SPRing Lockout](#)” task on page 20 for all MS-SPRing nodes in the network.

**Note**

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

- Step 8** For MS-SPRing nodes only, complete the “[DLP-U325 Set the Date and Time](#)” task on page 20 for any nodes not using Simple Network Time Protocol (SNTP).

- Step 9** As needed, upgrade any spare TCC2 or TCC2P cards by installing the spare in the standby slot of a Software R8.0 node.

**Note**

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

- Step 10** If you need to return to the software and database you had before activating Software R8.0, proceed with the “[NTP-U217 Revert to Previous Software Load and Database](#)” procedure on page 22.

**Note**

When you upgrade a TCC2 card to a TCC2P, the SFTWDOWN alarm can be raised and cleared more than once before the software download is complete. For example, when you remove the standby TCC2 card in Slot 11 and replace it with a TCC2P card, the SFTWDOWN alarm occurs within moments of this replacement. It can briefly clear and then occur again before the alarm is finally cleared at the end of the upgrade process

- Step 11** To back up the Software R8.0 database for the working software load, see “[NTP-U214 Back Up the Software Database](#)” procedure on page 8.

Stop. You have completed this procedure.

DLP-U320 Download ONS 15454 SDH Release 8.0 Software

Purpose	This task downloads Software R8.0 to the ONS 15454 SDH nodes prior to activation.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-U214 Back Up the Software Database, page 8
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of the workstation)
Security Level	Superuser or Maintenance


Note

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


Note

To download and upgrade the software using TL1, see the [“NTP-U218 Upgrade to ONS 15454 SDH Release 8.0 Using TL1” procedure on page 25](#).

-
- Step 1** From the CTC **View** menu, choose **Go to Network View**.
- Step 2** Verify that the alarm filter is not on. Click the **Filter** tool at the lower-left of the window.
- Step 3** The Alarm Filter dialog box appears. Click to deselect any selections in the Show Severity section of the General tab.
- Step 4** 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 is raised twice, once on standby and again on active, to indicate that the software download is taking place. The alarm is normal and clears when the download is complete.

-
- Step 5** From the CTC View menu, choose **Go to Home View** to go to the node view.
- Step 6** For nodes in single-shelf architecture mode, proceed to [Step 8](#). For nodes in multishelf mode (implemented using either MS-ISC cards or external Catalyst switches) running software R7.00 or earlier, do the following:
- Provision the active TCC/TCC2 cards in the node controller shelf and subtended shelf in slots 7 and before starting the upgrade process.
 - Make sure that all active TCC/TCC2 cards in the node controller and subtended shelf are in the same slot 11 (slot 7 is recommended). If they are, go to [Step 8](#).
- Step 7** Provision the node controller and subtended shelf in the same slot a switch-over of the active TCC/TCC2 card must be performed. Do the following:
- Right-click the currently active TCC/TCC2 card (Slot 11) and choose **Soft-reset Card**.
 - Click **Yes** in the confirmation dialog box.

- c. Click **OK** in the Connection Lost dialog box.
It might take a few minutes for CTC to establish connectivity
- d. Verify if the standby TCC/TCC2 (slot 7) is active.
- e. Repeat steps **a** to **d** as necessary.

Step 8 Return to node view and click the **Maintenance** tab, and then click the **Software** button.

Step 9 Click the **Download** button. The Download Selection dialog box appears.

Step 10 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 11 To open the Cisco15454SDH folder, select the file with the PKG extension and click the **Open** button.

Step 12 In the list of compatible nodes, click the check boxes for all nodes for software download.



Note Cisco advises that you limit concurrent software downloads to eight nodes at once, using the central node to complete the download.



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

Step 13 Click the **OK** button. 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 14 Return to your originating procedure (NTP).

DLP-U321 Perform an 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-U214 Back Up the Software Database, page 8
Required/As Needed	Required for MS-SPRing only
Onsite/Remote	Onsite or remote (but in the presence of the workstation)
Security Level	Maintenance



Note During activation, MS-SPRing spans are not protected. You must leave the MS-SPRing in the lockout state until all nodes in the ring are activated, and you must be sure to remove the lockout after activation.



Caution You must back up the database when using an MS-SPRing configuration.



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

Step 1 If CTC is not yet running, start CTC.

Step 2 In node view, click the **Maintenance** tab, then click the **MS-SPRing** button.

Step 3 For each of the MS-SPRing trunk (span) cards (STM-4, STM-16, STM-64, MRC-2.5G-12, MRC-12, STM64-XFP), 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 Protect**.
- c. Click **Apply**.
- d. In the same row, click the West Switch column to show the drop-down menu.
- e. From the menu options, choose **Lockout Protect**.
- f. Click **Apply**.



Note Ignore any Default K alarms that occur on the protect VC4 time slots 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 4 Return to your originating procedure (NTP).

DLP-U322 Activate the New ONS 15454 SDH Software Load

Purpose	This task activates Software R8.0 in each node in the network.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	DLP-U320 Download ONS 15454 SDH Release 8.0 Software, page 12 DLP-U321 Perform an MS-SPRing Lockout, page 13 (if required)
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of the workstation)
Security Level	Superuser



Caution

G-Series cards (G1000-4 and G1000) purchased prior to Software R7.2 will incur a traffic hit of 2 to 3 minutes per card during activation, while an FPGA upgrade to the card takes place, and will also incur the same traffic hit if the software is subsequently reverted, as the FPGA will be downgraded in the case of such a revert.



Note

Ensure that all cards that are part of a protection group (1+1, 1:1, 1:N, or Y-cable) are active on the working card of that protection group and that no protection switches are occurring. To ensure that traffic carrying protect cards are in a standby state, in the node view, click the Maintenance tab, then click the Protection button. Select each of the listed protection groups, then view the active/standby status of each card in the Selected Group area.



Note

Cisco recommends that you run the optional Cache Loader pre-caching utility in [Step 16](#) of this task. If you do not plan to run the pre-caching utility, 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

M-Series cards undergo a cold restart during an upgrade. The following alarms might be raised in conjunction with the ML cold restart. These should clear when the upgrade is complete.

On the ML port:

- LOA
- TPTFAIL
- VCG DOWN

On the paths traversed by the ML-Series circuits:

- SD-P
- SF-P
- PDI-P

Step 1 If CTC is not yet running, start CTC.

- Step 2** 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 3** In CTC node view, verify that the alarm filter is not on. Click the **Filter** tool at the lower-left of the window.
- Step 4** The Alarm Filter dialog box appears. Click to deselect any selections in the Show Severity section of the General tab.
- Step 5** Click the **Maintenance** tab, and then click the **Software** button.
- Step 6** Verify that the version in the Protect Version column is Software R8.0.



Note After activating Software R8.0 on both the working and the protect card, you cannot revert to a prior software version.

- Step 7** Click the **Activate** button. The Activate dialog box displays a warning message.
- Step 8** Click **Yes** to proceed with the activation.
- Step 9** An Activation Successful message indicates that the software is successfully activated.
- Step 10** Click **OK** in the message box.



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

- Step 11** Click **OK** in the message box.
- Step 12** After activating the node, the software upgrade reboot occurs as follows:
- Each card in the node reboots, beginning with the standby TCC2 or TCC2P card. When the standby TCC2/TCC2P card reboots, it signals to the active TCC2/TCC2P card that it is ready to take over. When the active TCC2/TCC2P receives this signal, it resets itself, and the standby TCC2/TCC2P takes over and transitions to active. The pre-upgrade version of the TCC2/TCC2P card is now the standby TCC2/TCC2P.
 - While the second TCC2/TCC2P is rebooting, the cross-connect card (SONET/SDH only) in Slot 8 reboots, and then the cross-connect card (SONET/SDH only) in Slot 10 reboots. Next, the E-Series Ethernet cards reset simultaneously.
 - Any cards in Y-cable protection groups boot next, one at a time (protect card first), in order of first creation (refer to the CTC protection group list for order of first creation).
 - Next, the traffic cards, G-Series Ethernet cards, CE-Series Ethernet cards, and ML-Series Ethernet cards boot consecutively, in ascending order of slot number, with the exception that E1-42 protect cards will always be reset before any of their peer working cards.
 - A system reboot (SYSBOOT) alarm is raised while activation is in progress (following the TCC2/TCC2P and cross-connect card resets). When all cards have reset, this alarm clears. The complete activation process can take up to 30 minutes, depending on how many cards are installed.

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

**Note**

During the software upgrade, a reset alarm is raised on all the cards. When upgrading from release 6.0.x, 6.1.x, 6.2.x, 7.0, 7.2, 7.2.x to 8.x, a MANRESET alarm is raised on Standby TCC cards and an AUTORESET alarm in all the other cards. However, from release 8.0, the MANRESET alarm is not raised and the AUTORESET alarm is raised on all the cards.

Step 13 In CTC, choose **File > Exit**.

Step 14 In your browser window, click the **Delete CTC Cache** button.

**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-U323 Delete Cached JAR Files” task on page 19](#).

Step 15 Close your browser and then reopen it.

Step 16 (Optional) Run the Cache Loader pre-caching utility, which can improve your speed logging back into CTC after an upgrade, and which is required to log into nodes running releases prior to R4.6. Perform the following steps to run the Cache Loader.

- a. Load the Software R8.0 CD into your CD-ROM drive. If the directory of the CD does not open automatically, open it.
- b. Double-click the setup.exe file to run the Installation Wizard. The CTC Installation Wizard dialog box opens.
- c. Click **Next**. The Setup Options dialog box opens.
- d. Choose **Custom**, and click **Next**. The Custom Options dialog box opens.
- e. Click to select **Cisco Transport Controller**, and **CTC JAR files** (deselect any other preselected options), then click the **Next** button. A confirmation dialog box opens.
- f. Click the **Next** button again. The CTC Cache Loader pre-caches the JAR files to your workstation, displaying a progress status box.
- g. When the utility finishes, click **OK**, and then in the wizard, click **Finish**.

Step 17 Reconnect to CTC using the IP address from [Step 2](#). The new CTC applet for Software R8.0 uploads. During this logon, enter your Superuser user ID and password.

**Note**

Steps [13](#) through [17](#) 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 18 Return to your originating procedure (NTP).

**Note**

When you revert the software to an earlier version, a reset alarm is raised on all the cards. When you revert from release 8.x or later to 6.0.x, 6.1.x, 6.2.x, 7.0, 7.2, or to 7.2.x, an AUTORESET alarm is raised on the Standby TCC cards and a MANRESET alarm in all other cards. However, in releases earlier to 8.0, the AUTORESET alarm is not raised and the MANRESET alarm is raised on all the cards.

DLP-U323 Delete Cached JAR Files

Purpose	This task deletes cached Java 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	Maintenance or higher

Step 1 Delete cache files from your browser directory.

In Netscape:

- a. Choose **Edit > Preferences**, click the **Advanced** tab, then click the **Cache** button.
- b. Click the **Clear Memory Cache** button, and click **OK**.
- c. Click the **Clear Disk Cache** button, and click **OK** twice.

In Microsoft Internet Explorer:

- a. Choose **Tools > Internet Options**. The Internet Options dialog box appears.
- b. Click the **General** tab.
- c. Click **Delete Files**.
- d. Select the **Delete all offline content** check box.
- e. 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 On Windows systems only, delete cached files from your workstation ().


- a. In your Windows start menu, choose **Control Panel > System** and click the **Advanced** tab.
- b. Click the **Environment Variables** button. 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. click **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-U324 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-U322 Activate the New ONS 15454 SDH Software Load, page 15
Required/As Needed	Required for MS-SPRing
Onsite/Remote	Onsite or remote (but in the presence of the workstation)
Security Level	Maintenance

-
- Step 1** If CTC is not yet running, start CTC.
- Step 2** In CTC node view, click the **Maintenance** tab, then click the **MS-SPRing** button.
- Step 3** For each of the MS-SPRing trunk (span) cards (STM-4, STM-16, STM-64, MRC-2.5G-12, MRC-12, STM64-XFP), perform the following steps:
- Next to the trunk card row, click the West Switch column to show the drop-down menu.
 - From the menu options, choose **Clear**.
 - 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.
- In the same row, click the East Switch column to show the drop-down menu.
 - From the menu options, choose **Clear**.
 - Click **Apply** to activate the command.
- Step 4** Repeat this task as many times as necessary to remove all MS-SPRing span lockouts on the upgrade nodes.
- Step 5** Return to your originating procedure (NTP).
-

DLP-U325 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 the **Apply** button.
- Step 3** Repeat Steps 1 and 2 for each remaining node.
- Step 4** Return to your originating procedure (NTP).
-

NTP-U216 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 you need to return to the software and database you had before activating Software R8.0, proceed with the [“NTP-U217 Revert to Previous Software Load and Database” procedure on page 22](#).
- Stop. You have completed this procedure.**
-

NTP-U217 Revert to Previous Software Load and Database

Purpose	This procedure returns you to the software and database provisioning you had before you activated Software R8.0.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-U213 Prepare for Upgrade to ONS 15454 SDH Software Release 8.0, page 6 NTP-U214 Back Up the Software Database, page 8 NTP-U215 Upgrade to ONS 15454 SDH Release 8.0, page 10
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 R8.0, you should have backed up the existing database at all nodes in the network (this is part of the “[NTP-U214 Back Up the Software Database](#)” procedure on page 8). Cisco recommends that you record or export all critical information to your hard drive. If you need to revert to the backup database, use the following tasks, in order.



Caution

G-Series cards (G1000-4 and G1000) purchased prior to Software R7.2 will incur a traffic hit of 2 to 3 minutes per card during activation, while FPGA upgrade to the card takes place. Upgraded cards will also incur the same traffic hit if the software is subsequently reverted, as the FPGA will be downgraded in the case of such a revert.



Caution

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



Note

TCC2P cards act as TCC2 cards in software releases prior to R5.0.

- Step 1** Log into the node. For detailed instructions, refer to the *Cisco ONS 15454 SDH Procedure Guide*. If you are already logged in and this is not an MS-SPRing, continue with Step 4.
- Step 2** (For MS-SPRing nodes only) The database must be backed up prior to locking the MS-SPRing nodes. See “[NTP-U214 Back Up the Software Database](#)” procedure on page 8 for details.
- Step 3** (For MS-SPRing nodes only) Complete the “[DLP-U321 Perform an MS-SPRing Lockout](#)” task on page 13.
- Step 4** Complete the “[DLP-U326 Revert to Protect Load](#)” task on page 23.
- Step 5** (For MS-SPRing nodes only) Complete the “[DLP-U324 Remove the MS-SPRing Lockout](#)” task on page 20.

- Step 6** If the software revert to your previous release failed to restore the database, complete the “[DLP-U327 Manually Restore the Database](#)” task on page 24.
Stop. You have completed this procedure.

DLP-U326 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. You cannot revert backwards to a previous version of the protect load if the software on both the working and protect sides is Software R8.0.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-U213 Prepare for Upgrade to ONS 15454 SDH Software Release 8.0, page 6 NTP-U214 Back Up the Software Database, page 8 NTP-U215 Upgrade to ONS 15454 SDH Release 8.0, page 10 DLP-U321 Perform an MS-SPRing Lockout, page 13
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 R8.0, the release you want to revert to must have been working at the time you activated to Software R8.0 on that node. Also, a supported revert automatically restores the node configuration at the time of the previous activation. Any configuration changes made after activation will be lost when you revert. The exception to this is when you have downloaded Software R8.0 a second time, ensuring that no revert to a previous load can take place. In this case, the revert will occur, but will not be traffic affecting and will not change you database.



Note

Ensure that all cards that are part of a protection group (1+1, 1:1, 1:N, or Y-cable) are active on the working card of that protection group and that no protection switches are occurring. To ensure that traffic carrying protect cards are in a standby state, in the node view click the Maintenance tab, and view the Protect column for each of the listed protection groups, then view the active/standby status of each card in the Maintenance tab.

- Step 1** From the node view, click the **Maintenance** tab, and then click the **Software** button.
- Step 2** Verify that the protect software displays the release you upgraded from.
- Step 3** Click the **Revert** button. This action 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 reversion and drops the connection to the node.
- Step 5** Wait until the software reversion finishes before continuing.



Note

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

- Step 6** Wait one minute before restoring another node.
- Step 7** Perform the “[DLP-U323 Delete Cached JAR Files](#)” task on page 19.
- 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.
- Step 9** Return to your originating procedure (NTP).
-

DLP-U327 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-U326 Revert to Protect Load , page 23 DLP-U324 Remove the MS-SPRing Lockout , page 20 (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 CTC node view, click the **Maintenance** tab, and then click the **Database** button.
- Step 2** Click the **Restore** button. The Open dialog box appears.
- Step 3** Select the previously saved database file and choose **Open**.
The database is restored and the TCC2/TCC2P cards reboot.
- Step 4** When the TCC2/TCC2P 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 restore.
- Step 6** Return to your originating procedure (NTP).
-

NTP-U218 Upgrade to ONS 15454 SDH Release 8.0 Using TL1

Purpose	This procedure upgrades the software to Software R8.0 using TL1 rather than CTC.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-U213 Prepare for Upgrade to ONS 15454 SDH Software Release 8.0, page 6 NTP-U214 Back Up the Software Database, page 8
Required/As Needed	Optional
Onsite/Remote	Onsite or remote (but in the presence of the workstation)
Security Level	Superuser



Note

This procedure assumes you are upgrading using Release 6.x TL1 syntax. TL1 commands issued prior to software activation to Software R8.0 will vary in syntax depending on the release you are actually upgrading from. To ensure that your syntax for each command is correct, use the TL1 syntax supplied in the *Cisco ONS SDH TL1 Command Guide* for your particular release when issuing the following commands:

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



Note

To perform an R8.0 software download using TL1, you must first have an FTP server or a terminal emulation program like HyperTerminal running on your workstation. In the following conditions, the download (COPY-RFILE) command is different when downloading software to a gateway network element (GNE) or an end network element (ENE):

- - FTP is being used.
- - The server is set up with a login and password of FTPUSER1 and FTPUSERPASSWORD1.
- - The FTP server has an IP address of 10.1.1.1.
- - The FTP server is running on the standard FTP port.
- - The software package is called "15454-03xx-A04K-1405.pkg"

The GNE and ENE commands are as follows:

- When downloading software to a GNE, use a command similar to:

```
COPY-RFILE:NODENAME:RFILE-PKG:CTAG::TYPE=SWDL,
SRC="ftp://FTPUSER1:FTPUSERPASSWORD1@10.1.1.1/15454-03xx-A04K-1405.pkg";
```

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

```
COPY-RFILE:NODENAME:RFILE-PKG:CTAG::TYPE=SWDL,
SRC="ftp://FTPUSER1:FTPUSERPASSWORD1@10.111.11.1:2361@90.90.90.90/15454-03xx-A04K-1405.pkg";
```

The ":21" after the FTP server IP address 10.111.11.1 denotes port 2361 on the server.

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

```
COPY-RFILE:NODENAME:RFILE-PKG:CTAG::TYPE=SWDL,
SRC="ftp://FTPUSER1:FTPUSERPASSWORD1@10.1.1.1:21@90.90.90.90/CISCO/SOFTWARE/15454-03xx-A04K-1405.pkg";
```

Step 1 To use TL1 commands, set up an FTP session or use HyperTerminal or a similar terminal emulation package to establish a session with the ONS 15454 SDH node. Select the IP address for the node, using port 3083 or 2361.

Step 2 The terminal emulation interface will display a warning message and a command prompt (usually >). You will issue TL1 commands at this prompt.

Step 3 Type the ACT-USER (Activate User) command in the TL1 request window to open a TL1 session:

```
ACT-USER: [<TID>] : <uid> : <CTAG> [ : : <pid> ] ;
```

where:

- <TID> is the target identifier (optional).
- <UID> is the operations support system (OSS) profile user ID (required).
- <CTAG> is the correlation tag that correlates command and response messages (optional).
- <PID> is the password identifier (required).

Step 4 Select the IP address for the node, using port 3083 or 2361.

The terminal emulation interface will display a warning message and a command prompt (usually >). You will issue TL1 commands at this prompt.

Step 5 Type the **COPY-RFILE** command in the TL1 window or, if using HyperTerminal, select **Transfer > Receive File**, and use the associated dialog box to select a file to receive. The **COPY-RFILE** command downloads a new software package from the location specified by the FTP URL into the inactive flash partition residing on either of the TCC2/TCC2P cards.

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

where:

- <TID> is the target identifier (optional).
- <SRC> is the source AID (required).
- <CTAG> is the correlation tag that correlates command and response messages (optional).

- <TYPE> is the file transfer protocol (required).
- <SRC1> specifies the source of the file to be transferred (required).
- <DEST> is the destination of the file to be transferred (required).
- <OVWRT> is overwrite. If <OVWRT> is yes, then files should be overwritten. If <OVWRT> is no, then file transfers will fail if the file already exists at the destination (required).
- <FTTD> is the URL format (required).

Step 6 Repeat [Step 5](#) for all nodes to be upgraded.

Step 7 Look for the **REPT EVT FXFR** message in the TL1 window. REPT EVT FXFR is an autonomous message used to report the start, completion, and completed percentage status of the software download. REPT EVT FXFR also reports any failure during the software upgrade, including invalid package, invalid path, invalid user ID/password, and loss of network connection. The format of the message is:

```
REPT EVT FXFR

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

where:

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

Step 8 Complete “[NTP-U213 Prepare for Upgrade to ONS 15454 SDH Software Release 8.0](#)” procedure on [page 6](#) for each node to be upgraded.

Step 9 Complete “[NTP-U214 Back Up the Software Database](#)” procedure on [page 8](#) for each node to be upgraded.

Step 10 (MS-SPRing nodes only) The database must be backed up prior to locking the BLSR. See “[NTP-U214 Back Up the Software Database](#)” procedure on [page 8](#) for details.

Step 11 Lock out each MS-SPRing span on each node being upgraded using the following command.

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

where:

- <AID> identifies the facility in the node to which the switch request is directed.
- <CTAG> is the correlation tag that correlates command and response messages
- <SC> is the switch command that is to be initiated on the paths.
- <SWITCHTYPE> is the MS-SPRing switch type.
- <DIRN> is the direction of transmission in which switching is to be made and is relative to the SDH line or path identified by the AID. The default value is RCV and should be changed to BTH.

**Note**

Some nodes might have more than one MS-SPRing. If this is the case, all MS-SPRing spans on all nodes being upgraded need to be backed up and then locked out. Nodes that are not being upgraded do not need to have the MS-SPRing spans locked out. You must be aware of each span that is part of an MS-SPRing to make sure all necessary spans are locked out.

**Note**

MS-SPRing lockouts must remain in place until the upgrade is complete for all nodes.

**Note**

Ignore any Default K alarms that occur on the protect STS time slots during the lockout.

**Note**

Certain Multiservice Switching Platform (MSSP) related alarms might be raised following activation of the first node in the ring. The following alarms, if raised, are normal, and should not cause concern. They clear upon completion of the upgrade, after all nodes have been activated: MSSP-OOSYNC (MN); RING-MISMATCH (MJ); APSCDFLTK (MN); MSSP-RESYNC (NA).

Step 12 Verify that all necessary MS-SPRing spans on each node being upgraded have been locked out using the following command:

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

where:

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

Step 13 Verify that there are no outstanding alarms or conditions on each node using the following commands:

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

where:

- <AID> indicates the entity in the node. <AID> must not be null.
- <CTAG> is the correlation tag that correlates command and response messages (optional).
- <TYPEREQ> is the type of condition to be retrieved. A null value is equivalent to ALL.

```
RTRV-ALM-ALL : [<TID>] : [<AID>] : <CTAG> : : [<NTFCNCDE>] , [<CONDITION>] , [<SRVEFF>] [ , , , ] ;
```

where:

- <AID> indicates the entity in the node. <AID> must not be null.
- <CTAG> is the correlation tag that correlates command and response messages (optional).
- <NTFCNCDE> is a notification code. A null value is equivalent to ALL.
- <CONDITION> is the type of alarm condition. A null value is equivalent to ALL.
- <SRVEFF> is the effect on service caused by the alarm condition. A null value is equivalent to ALL.

Resolve all issues before proceeding.



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

Step 14 Starting at the node farthest from the GNE, type the **APPLY** command to activate the system software.

```
APPLY: [<TID>] : :<CTAG> [ : :<MEM_SW_TYPE> ] ;
```

where:

- <TID> is the target identifier.
- <CTAG> is the correlation tag that correlates command and response messages.
- <MEM_SW_TYPE> indicates a memory switch action during the software upgrade, either:
 - MEM_SW_TYPE is ACT to activate
 - MEM_SW_TYPE is CANC to cancel the activation.

If the command is successful, the appropriate flash is selected and the TCC2/TCC2P card reboots.

The following occurs:

- Each card in the node reboots, beginning with the standby TCC2 or TCC2P card. When the standby TCC2/TCC2P card reboots, it signals to the active TCC2/TCC2P card that it is ready to take over. When the active TCC2/TCC2P receives this signal, it resets itself, and the standby TCC2/TCC2P takes over and transitions to active. The pre-upgrade version of the TCC2/TCC2P card is now the standby TCC2/TCC2P.
- While the second TCC2/TCC2P is rebooting, the cross-connect card (SONET/SDH only) in Slot 8 reboots, and then the cross-connect card (SONET/SDH only) in Slot 10 reboots. Next, the E-Series Ethernet cards reset simultaneously.
- Next, the E-Series Ethernet cards reset simultaneously.
- Any cards in Y-cable protection groups boot next, one at a time (protect card first), in order of first creation (refer to the CTC protection group list for order of first creation).
- Next, the traffic cards, G-Series Ethernet cards, CE-Series Ethernet cards, and ML-Series Ethernet cards boot consecutively, in ascending order of slot number, first standby, then working, for each card pair, with the exception that E1-42 protect cards will always be reset before any of their peer working cards.
- A system reboot (SYSBOOT) alarm is raised while activation is in progress (following the TCC2/TCC2P and cross-connect card resets). When all cards have reset, this alarm clears. The complete activation process can take up to 30 minutes, depending on how many cards are installed.

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

Step 15 Perform [Step 14](#) for each node that will be upgraded.



Note You might have to log into each node again to activate the software.

Step 16 After all nodes have been activated, log in using CTC or Telnet and verify there are no outstanding alarms.

Step 17 Remove all MS-SPRing lockouts using the following TL1 command:

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

where:

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

For example:

```
RLS-PROTNSW-OC48:PETALUMA:FAC-6-1:209::BTH;
```

Step 18 To back up the database for the Working software load, see the [“NTP-U214 Back Up the Software Database” procedure on page 8](#).

Stop. You have completed this procedure.

Related Documentation

Release-Specific Documents

- *Release Notes for the Cisco ONS 15454 SDH Release 8.0*

Platform-Specific Documents

- *Cisco ONS 15454 SDH Procedure Guide*
Provides installation, turn-up, test, and maintenance procedures for SDH networks
- *Cisco ONS 15454 SDH Reference Manual*
Provides technical reference information for ONS 15454 SDH cards, nodes, and networks
- *Cisco ONS 15454 DWDM Procedure Guide*
Provides installation, turn-up, test, and maintenance procedures for DWDM networks
- *Cisco ONS 15454 DWDM Reference Manual*
Provides technical reference information for DWDM cards, nodes, and networks
- *Cisco ONS 15454 SDH Troubleshooting Guide*
Provides a list of ONS 15454 SDH alarms, errors, and transient conditions, as well as alarm and general troubleshooting procedures

- *Cisco ONS 15454 DWDM Troubleshooting Guide*
Provides a list of DWDM alarms, errors, and transient conditions, as well as alarm and general troubleshooting procedures
- *Cisco ONS SDH TL1 Command Guide*
Provides a full TL1 command and autonomous message set including parameters, access identifiers (AIDs), conditions, and modifiers for the Cisco ONS 15454 SDH
- *Cisco ONS SDH TL1 Reference Guide*
Provides general information, procedures, and errors for TL1 in the Cisco ONS 15454 SDH

Obtaining Documentation

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

Cisco.com

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

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

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

Product Documentation DVD

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

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

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

Cisco Optical Networking Product Documentation CD-ROM

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

Ordering Documentation

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

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

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

Documentation Feedback

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

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

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

We appreciate your comments.

Cisco Product Security Overview

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

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

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

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

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

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

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

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

Reporting Security Problems in Cisco Products

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

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

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

- For non-emergencies—psirt@cisco.com

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

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



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

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

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

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

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

Obtaining Technical Assistance

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

Cisco Technical Support & Documentation Website

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

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

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

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

**Note**

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

Submitting a Service Request

Using the online Cisco 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 Cisco TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The Cisco TAC Service Request Tool is located at this URL:

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

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

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

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

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

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

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

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

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

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

<http://www.ciscopress.com>

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

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

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

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

or view the digital edition at this URL:

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

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

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

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:
<http://www.cisco.com/en/US/products/index.html>
- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:
<http://www.cisco.com/discuss/networking>
- World-class networking training is available from Cisco. You can view current offerings at this URL:
<http://www.cisco.com/en/US/learning/index.html>

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

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

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