



Cisco ONS 15454 Software Upgrade Guide, Release 3.4.x

Software Release 3.4.x
April 2003

Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number: DOC-7815220=
Text Part Number: 78-15220-02



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0303R)

Cisco ONS 15454 Software Upgrade Guide
Copyright © 2003, Cisco Systems, Inc.
All rights reserved.



About this Manual v

Obtaining Documentation	v
Cisco.com	v
Documentation CD-ROM	v
Ordering Documentation	vi
Documentation Feedback	vi
Obtaining Technical Assistance	vi
Cisco.com	vi
Technical Assistance Center	vii
Obtaining Additional Publications and Information	viii

CHAPTER 1

Upgrading Release 2.2.x to 3.4.x Using the TCC+ Card 1-1

Before You Begin	1-1
NTP-408 Prepare for Release 2.2.x to Release 3.4.x Upgrade	1-2
DLP-433 Verify CTC Workstation Requirements	1-2
DLP-434 Verify IP Addresses	1-3
DLP-435 Verify LAN Connections	1-3
DLP-436 Verify Common Control Cards	1-4
DLP-437 Verify AIP	1-4
NTP-409 Back Up the Database	1-5
DLP-438 Back Up the Software	1-5
DLP-439 Perform a Manual Backup	1-6
NTP-410 Upgrade the Software	1-7
DLP-440 Run the Script	1-8
DLP-441 Download Release 3.4.x Software	1-9
DLP-442 Perform a Release 2.2.x BLSR Lockout	1-10
DLP-U18 Activate the New Load	1-11
DLP-444 Delete Cached JAR Files	1-13
DLP-445 Remove the Release 3.4.x BLSR Lockout	1-14
DLP-446 Set the Date and Time	1-15
DLP-447 Upgrade Spare TCC+ Cards	1-15
NTP-411 Revert to Previous Load	1-16
DLP-448 Perform a Release 3.4.x BLSR Lockout	1-17
DLP-449 Revert to Protect Load	1-18

DLP-450 Remove Release 2.2.x BLSR Lockout 1-19
 DLP-451 Manually Restore the Database 1-20

CHAPTER 2

Upgrading Release 3.x to 3.4.x Using the TCC+ Card 2-1

Before You Begin 2-1
 NTP-404 Prepare for Release 3.x to Release 3.4.x Upgrade 2-2
 DLP-452 Verify CTC Workstation 2-2
 DLP-453 Verify IP Addresses 2-3
 DLP-454 Verify LAN Connections 2-3
 DLP-455 Verify Common Control Cards 2-4
 NTP-405 Back Up the Database 2-4
 DLP-456 Back Up Software 2-5
 DLP-457 Perform a Manual Backup 2-5
 NTP-406 Upgrade the Software 2-6
 DLP-458 Download the Release 3.4.x Software 2-7
 DLP-459 Perform a BLSR Lockout 2-8
 DLP-U19 Activate the New Load 2-9
 DLP-461 Delete Cached JAR Files 2-11
 DLP-462 Remove the BLSR Lockout 2-12
 DLP-463 Set the Date and Time 2-13
 DLP-464 Upgrade Spare TCC+ Units 2-13
 NTP-407 Revert to Previous Load 2-14
 DLP-465 Perform a BLSR Lockout 2-15
 DLP-466 Revert to Protect Load 2-15
 DLP-467 Remove the BLSR Lockout 2-16
 DLP-468 Manually Restore the Database 2-17



About this Manual

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco websites can be accessed from this URL:

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

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Registered Cisco.com users can order a single Documentation CD-ROM through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order monthly or quarterly subscriptions through the online Subscription Store:

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

Ordering Documentation

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:
http://www.cisco.com/cgi-bin/order/order_root.pl
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. In the Cisco Documentation home page, click the **Fax** or **Email** option in the “Leave Feedback” section at the bottom of the page.

You can e-mail your comments to bug-doc@cisco.com.

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

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

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise

- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL:

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

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The type of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration. There is little or no impact to your business operations.
- Priority level 3 (P3)—Operational performance of the network is impaired, but most business operations remain functional. You and Cisco are willing to commit resources during normal business hours to restore service to satisfactory levels.
- Priority level 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively impacted by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.
- Priority level 1 (P1)—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.

Cisco TAC Website

The Cisco TAC website provides online documents and tools to help troubleshoot and resolve technical issues with Cisco products and technologies. To access the Cisco TAC website, go to this URL:

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

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC website. Some services on the Cisco TAC website require a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

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

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

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

If you have Internet access, we recommend that you open P3 and P4 cases online so that you can fully describe the situation and attach any necessary files.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

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

Before calling, please check with your network operations center to determine the Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

Obtaining Additional Publications and Information

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

- 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://www.cisco.com/en/US/products/products_catalog_links_launch.html

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary*, *Internetworking Technology Handbook*, *Internetworking Troubleshooting Guide*, and the *Internetworking Design Guide*. For current Cisco Press titles and other information, go to Cisco Press online at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access *Packet* magazine at this URL:

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

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

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

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

http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html



Upgrading Release 2.2.x to 3.4.x Using the TCC+ Card

This chapter explains how to upgrade Cisco ONS 15454's Cisco Transport Controller (CTC) software from Release 2.2.x to Release 3.4.x using the Timing, Communications, and Control + (TCC+) card.

Before You Begin

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



Caution

Read each procedure before you begin the upgrade.



Caution

This chapter is only supported for Release 2.2.x. If you wish to upgrade from Releases 3.0 – 3.2, use the procedures in [Chapter 2, “Upgrading Release 3.x to 3.4.x Using the TCC+ Card”](#). If you wish to upgrade from a release prior to Release 2.2.0, you must call the Technical Assistance Center (TAC) at 877 323-7368 for assistance.



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 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, you may wish to check off each procedure on your printed copy of this chapter as you complete it.

This section lists the chapter procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. [NTP-408 Prepare for Release 2.2.x to Release 3.4.x Upgrade, page 1-2](#)—This procedure contains critical information and tasks that you must read and complete before beginning the upgrade process.
2. [NTP-409 Back Up the Database, page 1-5](#)—Complete the database backup to ensure that you have preserved your node and network provisioning in the event that you need to restore them.
3. [NTP-410 Upgrade the Software, page 1-7](#)—You must complete this entire procedure before the upgrade is finished.

4. [NTP-411 Revert to Previous Load, page 1-16](#)—Complete this procedure only if you need to return to the software load you were running before activating the Release 3.4.x software.

NTP-408 Prepare for Release 2.2.x to Release 3.4.x Upgrade

Purpose	This procedure steps you through the critical information checks and tasks you must complete before beginning an upgrade.
Tools/Equipment	PC or UNIX workstation; Cisco ONS 15454 Release 3.4.x software.
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite or remote

-
- Step 1** Read the appropriate release notes.
- Step 2** Complete the [“DLP-433 Verify CTC Workstation Requirements” task on page 1-2](#).
- Step 3** Complete the [“DLP-434 Verify IP Addresses” task on page 1-3](#).
- Step 4** Complete the [“DLP-435 Verify LAN Connections” task on page 1-3](#).
- Step 5** Complete the [“DLP-436 Verify Common Control Cards” task on page 1-4](#).
- Step 6** Complete the [“DLP-437 Verify AIP” task on page 1-4](#).
- Step 7** When you have completed the tasks for this section, proceed with the [“NTP-409 Back Up the Database” procedure on page 1-5](#).
-

DLP-433 Verify CTC Workstation Requirements

Purpose	Before upgrading the workstation to run CTC Release 3.4.x, verify all PC or UNIX workstation hardware and software requirements.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of the 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, or Windows NT
 - UNIX workstation running Solaris
- Step 2** Ensure that your web browser software is one of:
- Netscape Navigator 4.73 or higher (Netscape Navigator is included on the ONS 15454 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 software CD).



Note Because you upgrade to JRE 1.3.1.02, you will no longer be able to log into an ONS 15454 running Release 2.2.1 or prior, or an ONS 15327 running release 1.0.0. If you must later revert to a release that requires a previous version of the JRE, you will have to reinstall Java and delete the jar files from your workstation's user "temp" directory after reverting all of the nodes in the network. 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 Once you have verified that your workstation meets CTC Release 3.4.x requirements, proceed to the ["DLP-434 Verify IP Addresses" task on page 1-3](#).

DLP-434 Verify IP Addresses

Purpose	Use this task to ensure that there are no IP address conflicts with CTC.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	DLP-433 Verify CTC Workstation Requirements, page 1-2
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of the workstation)

- Step 1** Disable all other Ethernet devices (such as a dial-up adapter) on the workstation that runs CTC.
- Step 2** If you have multiple IP addresses on your workstation, you should remove them; you cannot install CTC Release 3.4.x if multiple IP addresses are configured.
- Step 3** You have completed the IP address check task. Now perform the ["DLP-435 Verify LAN Connections" task on page 1-3](#).

DLP-435 Verify LAN Connections

Purpose	Use this task to ensure LAN connections are correct.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	DLP-434 Verify IP Addresses, page 1-3
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of the workstation)

- Step 1** If you have multiple ONS 15454 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 Reference Guide* for LAN-connection suggestions.

- Step 2** After verifying that your LAN is properly configured, proceed to the “[DLP-436 Verify Common Control Cards](#)” task on page 1-4.

DLP-436 Verify Common Control Cards

Purpose	This task verifies two TCC+ cards and two cross-connect cards (two XCs, or two XCVTs) are installed at each node.
Tools/Equipment	PC or UNIX workstation with CTC installed
Prerequisite Procedures	DLP-435 Verify LAN Connections , page 1-3
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of the workstation)



Caution

You must be using TCC+, and not TCC cards to upgrade to Release 3.4.x. If you have any TCC cards installed, you must first upgrade to TCC+ before proceeding with the software upgrade. Refer to the Maintenance chapter of the *Cisco ONS 15454 Procedure Guide* for Release 3.4.x, or to the documentation accompanying your TCC+ cards, for the upgrade procedure.

- Step 1** Log into the node.
- Step 2** Ensure that Slots 7, 8, 10, and 11 have cards installed. Release 2.2.x does not support simplex operation.
- Step 3** Repeat Steps 1 and 2 at every node in the network.
- Step 4** When you have completed the verification of duplex common control cards. Proceed to the “[DLP-437 Verify AIP](#)” task on page 1-4.

DLP-437 Verify AIP

Purpose	Use this task to ensure AIP board quality.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	DLP-436 Verify Common Control Cards , page 1-4
Required/As Needed	Required
Onsite/Remote	Onsite



Caution

If any of your nodes has an AIP board with the part number 67-xx-xxxxx, where each “x” can be any number or letter, the board must be replaced. Perform the following steps to ensure that all of your AIP boards are good.

- Step 1** Look at the back of your ONS 15454 node and locate the green board with “AIP” stamped into the right hand side (the writing will be sideways as you face the board).
- Step 2** Locate the sticker with the part number. The number should be preceded by “P/N” on the sticker.



Note If there is no sticker with a part number, the number may be stamped into the board itself. If you cannot find the part number, you must contact the Technical Assistance Center (TAC) at 877 323-7368 for assistance.

- Step 3** If the part number is any number other than 67-xx-xxxxx, go to the next node and start from Step 1 again.
- Step 4** If the part number is any 67-xx-xxxxx combination, contact the TAC at 877 323-7368 to request a Return Materials Authorization (RMA).
- Step 5** Repeat Steps 1 – 4 for every node.
- Step 6** You have completed the AIP verification. Before you upgrade your CTC software you must now back up the database for each node you will upgrade. Proceed to the [“NTP-409 Back Up the Database” procedure on page 1-5](#).

NTP-409 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	NTP-408 Prepare for Release 2.2.x to Release 3.4.x Upgrade, page 1-2
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of the workstation)

- Step 1** Complete the [“DLP-438 Back Up the Software” task on page 1-5](#).
- Step 2** Complete the [“DLP-439 Perform a Manual Backup” task on page 1-6](#).
- Step 3** Once you have backed up the database, proceed to the [“NTP-410 Upgrade the Software” procedure on page 1-7](#).

DLP-438 Back Up the Software

Purpose	Before upgrading from Release 2.2.x to Release 3.4.x software, you must back up the current database for all nodes in the network.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-408 Prepare for Release 2.2.x to Release 3.4.x Upgrade, page 1-2
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of the 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 the workstation's hard drive or on network storage. Use an appropriate file name with the file extension .db (for example, myDatabase.db).
- Step 5** Click **Save**. A message appears indicating that the backup is complete.
- Step 6** Click **OK**.
- Step 7** Repeat Steps 1 – 6 for each node in the network.
- Step 8** You have completed the software backup. Proceed to the “[DLP-439 Perform a Manual Backup](#)” task on [page 1-6](#).

DLP-439 Perform a Manual Backup

Purpose	Cisco recommends that you manually log critical information by either writing it down or printing screens where applicable. This task is optional after you have backed up the database.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	DLP-438 Back Up the Software, page 1-5
Required/As Needed	Recommended
Onsite/Remote	Onsite or remote (but in the presence of the workstation)

- Step 1** Use the following table to determine the information you should log; complete the table (or your own version) for every node in the network.

Table 1-1 *Manually Logged 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+	Slot 7 or Slot 11 (circle one)
Active XC	Slot 8 or Slot 10 (circle one)
Network information; do a print screen from the Provisioning tab in the network view.	
Current configuration: BLSR, linear, etc. (do print screens as needed)	

Table 1-1 Manually Logged 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	

Step 2 Once you have backed up all databases and recorded all necessary information using the checklist, you can begin the “[NTP-410 Upgrade the Software](#)” procedure on page 1-7.

NTP-410 Upgrade the Software

Purpose	Use this procedure to upgrade your CTC software.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-409 Back Up the Database, page 1-5
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of the workstation)

Step 1 Insert the Release 3.4.x software CD into the workstation CD-ROM (or otherwise acquire access to the software) to begin the upgrade process.



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



Caution

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



Caution

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

Step 2 If upgrading from Release 2.2.0, perform the “[DLP-440 Run the Script](#)” task on page 1-8; if upgrading from Release 2.2.1 or 2.2.2, skip this task.

Step 3 Complete the [DLP-441 Download Release 3.4.x Software, page 1-9](#) (all nodes).

Step 4 Complete the [DLP-442 Perform a Release 2.2.x BLSR Lockout, page 1-10](#) (BLSR nodes only).

Step 5 Complete the [DLP-U18 Activate the New Load, page 1-11](#) (all nodes).

Step 6 Complete the [DLP-444 Delete Cached JAR Files, page 1-13](#).

- Step 7** Complete the [DLP-445 Remove the Release 3.4.x BLSR Lockout, page 1-14](#) (BLSR nodes only).
- Step 8** Complete the [DLP-446 Set the Date and Time, page 1-15](#) (any nodes not using SNTP).
- Step 9** Complete the [DLP-447 Upgrade Spare TCC+ Cards, page 1-15](#) (as needed for upgrading spare TCC+ cards).
- Step 10** To upgrade the software successfully, you must read and perform each of the tasks that applies to your network in the proper order. Begin with the “[DLP-440 Run the Script](#)” task on page 1-8.

DLP-440 Run the Script

Purpose	Use this task to prepare your Release 2.2.0 nodes for upgrade with a software patch.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-409 Back Up the Database, page 1-5
Required/As Needed	Required for Release 2.2.0 only
Onsite/Remote	Onsite or remote (but in the presence of the workstation)



Note

This task is only necessary with Release 2.2.0 upgrades. If you are upgrading from Release 2.2.1 or greater, you can skip this task and continue with the “[DLP-441 Download Release 3.4.x Software](#)” task on page 1-9.



Caution

Do not run the script on more than one node and one workstation at the same time.



Note

Running the script takes approximately 2 to 3 minutes.

- Step 1** Using CTC Release 2.2.0, log into the node from which you will run the script.
- Step 2** Check the ONS 15454 for existing alarms. Resolve any outstanding alarms before proceeding.
- Step 3** From the node view, click the **Maintenance > Software** tabs.
- Step 4** Verify that the active load is 2.2.0 (02.20-001A-00.38).



Note

The script will only work for the Release 2.2.0 (02.20-001A-00.38) load.

- Step 5** Close all active telnet connections to the ONS 15454.
- Step 6** Run the script:

In a command window, from the CD software “Cisco15454” directory, run **ptfix.exe** (or **ptfix.pl**, in UNIX) using the IP address of the node you are running the script on.

```
EXAMPLE G:\Cisco15454> ptfix 172.16.17.18
```

This step takes approximately 2 to 3 minutes. When the script has completed successfully, an “Upgrade Preparation Complete” message appears.

- Step 7** Close CTC and then reconnect to the node.
- Step 8** From the network view, log into the node you ran the script on.
- Step 9** Click the **Maintenance > Software** tabs.
- Step 10** Verify that the protect software is now “none.”
- Step 11** Return to the network view.
- Step 12** Repeat Steps 1 – 11 for each node in the network running Release 2.2.0.

**Caution**

Rerun the script on any node for which the active/standby TCC+ reboots at any time before the Release 3.4.x load is activated.

- Step 13** Once you have run the script for all nodes in the network, continue to the “[DLP-441 Download Release 3.4.x Software](#)” task on page 1-9.

DLP-441 Download Release 3.4.x Software

Purpose	Download the Release 3.4.x software to the ONS 15454 nodes prior to activation.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	DLP-440 Run the Script, page 1-8 if applicable; otherwise, NTP-409 Back Up the Database, page 1-5
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of the workstation)

**Note**

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

- Step 1** 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 node view, click the **Maintenance > Software** tabs.
- Step 3** Click **Upgrade**. The File Open dialog box opens.
- Step 4** Browse to locate the software files on the ONS 15454 System Software CD (or on your hard drive, if you are working from a local copy).
- Step 5** Open the “Cisco15454” folder.
- Step 6** Select the file with the “.pkg” extension and click **Open**. CTC displays a status window so you can monitor the download process. A message indicating that your files transferred successfully will appear after the software has finished loading.

Step 7 Repeat Steps 1 – 7 for each node.



Note The software download process can take 30 minutes or more per node.

Step 8 Once you have successfully downloaded the CTC Release 3.4.x software to each node you are upgrading, perform the “[DLP-442 Perform a Release 2.2.x BLSR Lockout](#)” task on page 1-10. If none of your nodes participate in a BLSR, you can skip the BLSR lockout and begin the “[DLP-U18 Activate the New Load](#)” task on page 1-11.

DLP-442 Perform a Release 2.2.x BLSR Lockout

Purpose	If any node you are upgrading is in a bidirectional line switched ring (BLSR) configuration, you must perform a span lockout at each node in the ring before activating the software for Release 3.4.x. Perform this task to issue a span lockout on a BLSR using CTC Release 2.2.x.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	DLP-441 Download Release 3.4.x Software, page 1-9
Required/As Needed	Required for BLSR
Onsite/Remote	Onsite or remote (but in the presence of the workstation)



Note During the lockout, BLSR spans will not be 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 BLSR trunk cards (OC-12, OC-48, or OC-192), go to the row in the table for that card and perform the following steps:

- a. Click in the West Operation column to show the pull-down menu.
- b. From the menu options, choose **Ring Lockout**.
- c. In the same row, click in the East Operation column to show the pull-down menu.
- d. From the menu options, choose **Ring 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 BLSR in the lockout state until you have finished activating all nodes.

- Step 4** You have completed the BLSR lockout. You must now perform the “[DLP-U18 Activate the New Load](#)” task on page 1-11.
-

DLP-U18 Activate the New Load

Purpose	Log into and activate each node in the network.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	DLP-442 Perform a Release 2.2.x BLSR Lockout , page 1-10, if required; otherwise, DLP-441 Download Release 3.4.x Software , page 1-9
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of the 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 workstation as quickly as possible.



Note Make sure 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 before proceeding.

- Step 1** To ensure database synchronization, run the memAudit utility:
- Close all active telnet connections to the ONS 15454.
 - Copy the memAudit.exe from the ONS 15454 software CD or the following Cisco.com web page to a folder on your hard drive:
<http://www.cisco.com/cgi-bin/tablebuild.pl/ons15454>
 - In a command window, change the prompt to the folder where the memAudit.exe is located.
 - At the prompt, type the following command:
`memAudit <nodename or IP address>`



Note Optional parameters exist for the memAudit command. For more information about the memAudit utility, view the memAudit_readme.htm file on the CD or Cisco.com web page.

- Step 2** Log into a node.
- Step 3** Record the IP address of that node.
- Step 4** Verify that the node has no new alarms. If alarms exist, clear them before proceeding.
- Step 5** From the CTC node view, click the **Maintenance > Software** tabs.
- Step 6** Verify that the protect version is 3.4.x.

- Step 7** Click **Activate**. The **Activate** dialog box appears with a warning message.
- Step 8** Click **Yes** to proceed with the activation. The “Activation Successful” message appears when the software is successfully activated.
- Step 9** Click **OK** to begin the node rebooting process.
- Step 10** 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. Once all cards have reset, this alarm clears.

Each card in the node reboots, beginning with the standby TCC+. Once the standby TCC+ is fully activated and fully rebooted, it becomes the active TCC+ and the other TCC+ reboots. When the TCC+s are finished, the XC/XCVT in Slot 8 reboots, and then the XC/XCVT 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. TDM traffic can endure a hit of up to 50 ms. Expect Ethernet traffic to remain down from the time the TCC+s switch to the time all Ethernet cards have finished resetting. Once all the cards finish rebooting and all alarms clear, you can safely proceed to the next step. (If you are upgrading remotely and cannot see the nodes, wait for 30 minutes for the process to complete, then check to ensure 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 removed to the network view during the node reboot, but after the reboot is complete, CTC will restore connectivity to the node.

- Step 11** In CTC, choose **File > Exit**.
- Step 12** Follow all steps in the “[DLP-444 Delete Cached JAR Files](#)” task on page 1-13. When you have performed all of the steps in that task, continue here with the next step (Step 12).
- Step 13** 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/Refresh button). The new CTC applet for Release 3.4.x uploads. Because CTC Release 3.4.x is backwardly compatible with CTC Release 2.2.x, it affords you network visibility while you are upgrading.



Note Only activate one node at a time.

- Step 14** Log into each of the remaining nodes and perform the “[DLP-U18 Activate the New Load](#)” task on page 1-11. The activation must be performed for every node that is running software Release 2.2.x. Allow each node to finish (all alarms cleared for 10 minutes) before activating the next node.
- Step 15** You have completed the activation task when you have activated all nodes with the Release 3.4.x software. If you performed a BLSR lockout before you began activation, you must now perform the “[DLP-445 Remove the Release 3.4.x BLSR Lockout](#)” task on page 1-14. Otherwise, go to the “[DLP-446 Set the Date and Time](#)” task on page 1-15.
-

DLP-444 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	DLP-U18 Activate the New Load, page 1-11
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of the 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** checkbox.
- d. Click **OK** twice.

Step 2 Close your browser.



Note You will not be able to delete cached jar files from your hard drive until you have closed your browser. If you have other applications open that use jar files, you must also close them.

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

- a. In your Windows start menu, choose **Settings > Control Panel > System > Advanced**.
- b. Click **Environment Variables**. This will show 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 “TEMP” directory located in the path you just looked up.
- e. Select **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 task, either the “[DLP-U18 Activate the New Load](#)” task on page 1-11, or the “[DLP-449 Revert to Protect Load](#)” task on page 1-18, and continue with the steps there.
-

DLP-445 Remove the Release 3.4.x BLSR Lockout

Purpose	Release the span lockouts on all BLSR nodes after the new software load is activated on all nodes. This task restores a BLSR using Release 3.4.x.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	DLP-444 Delete Cached JAR Files , page 1-13; DLP-U18 Activate the New Load , page 1-11
Required/As Needed	Required for BLSR
Onsite/Remote	Onsite or remote (but in the presence of the workstation)

- Step 1** In CTC node view, click the **Maintenance > BLSR** tabs.
- Step 2** For each of the BLSR trunk cards (OC-12, OC-48, or OC-192), go to the row in the table for that card and perform the following steps:
- Click in the West Switch column to show the pull-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 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.

- In the same row, click in the East Switch column to show the pull-down menu.
 - From the menu options, choose **Clear**.
 - Click **Apply** to activate the command.
- Step 3** When all BLSR span lockouts are released, you have completed this task and should go to the “[DLP-446 Set the Date and Time](#)” task on page 1-15.
-

DLP-446 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 task to reset the date and time at each node.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	DLP-445 Remove the Release 3.4.x BLSR Lockout , page 1-14, if required; otherwise, DLP-444 Delete Cached JAR Files , page 1-13 and DLP-U18 Activate the New Load , page 1-11
Required/As Needed	As needed
Onsite/Remote	Onsite or remote (but in the presence of the workstation)



Note If you are using SNTP, you do not need this task and can go to the [“DLP-447 Upgrade Spare TCC+ Cards”](#) task on page 1-15.

-
- 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 [“DLP-447 Upgrade Spare TCC+ Cards”](#) task on page 1-15.
-

DLP-447 Upgrade Spare TCC+ Cards

Purpose	Use this task to upgrade all spare TCC+ units to Release 3.4.x.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	DLP-445 Remove the Release 3.4.x BLSR Lockout , page 1-14 if required; otherwise, DLP-U18 Activate the New Load , page 1-11 and DLP-444 Delete Cached JAR Files , page 1-13
Required/As Needed	Required for all spare TCC+ cards
Onsite/Remote	Onsite or remote (but in the presence of the workstation)

- Step 1** To upgrade a spare TCC+, place it in the standby slot of a node running Release 3.4.x. The card will upgrade automatically from the active TCC+.
- The standby TCC+ will copy one or both software releases from the active TCC+, as needed. Each software copy takes about 15 minutes, and the TCC+ will reset after each copy. Thus, for a TCC+ that has no matching software with the active TCC+, you should expect to see two TCC+ resets, lasting about 30 minutes total.



Note During the TCC+ upgrade, the LEDs on the upgrading card will flash alternately between “fail” and “standby.”

- Step 2** Once you have upgraded all of your spare TCC+ units, you have completed the software upgrade.



Note If you need to upgrade your cross connect cards, please refer to the user documentation for the software you are currently running. This procedure can be performed before or after the software upgrade; however, you must also refer to the user documentation for details on hardware requirements for the XC10G before upgrading to this card type.

NTP-411 Revert to Previous Load

Purpose	Return to the exact software and database provisioning you had before you activated Release 3.4.x.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-408 Prepare for Release 2.2.x to Release 3.4.x Upgrade , page 1-2, NTP-409 Back Up the Database , page 1-5, and NTP-410 Upgrade the Software , page 1-7 (up to and including the “ DLP-U18 Activate the New Load ” task on page 1-11, and the “ DLP-445 Remove the Release 3.4.x BLSR Lockout ” task on page 1-14, if applicable)
Required/As Needed	As needed
Onsite/Remote	Onsite or remote (but in the presence of the workstation)



Note The procedure to revert to a previous load is not a part of the upgrade. The tasks that make up this procedure 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 Release 2.2.x to Release 3.4.x software, you should have backed up the existing database at all nodes in the network (this is part of the “[NTP-409 Back Up the Database](#)” procedure on page 1-5). Cisco recommends that you record or export all critical information to your hard drive. If you need to revert to the backup database, use the following tasks, in order.

- Step 1** Complete the “[DLP-448 Perform a Release 3.4.x BLSR Lockout](#)” task on page 1-17 (BLSR only).
- Step 2** Complete the “[DLP-449 Revert to Protect Load](#)” task on page 1-18.
- Step 3** Complete the “[DLP-450 Remove Release 2.2.x BLSR Lockout](#)” task on page 1-19 (BLSR only).
- Step 4** Complete the “[DLP-451 Manually Restore the Database](#)” task on page 1-20 (Release 2.2.0 only).
- Step 5** Once you have completed the steps above, the revert is complete.

DLP-448 Perform a Release 3.4.x BLSR Lockout

Purpose	If you have a BLSR provisioned, before beginning the revert you must perform a span lockout at each node. Perform this task to issue a span lockout on a BLSR using CTC Release 3.4.x.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-408 Prepare for Release 2.2.x to Release 3.4.x Upgrade, page 1-2 , NTP-409 Back Up the Database, page 1-5 , and NTP-410 Upgrade the Software, page 1-7 (up to and including the “DLP-U18 Activate the New Load” task on page 1-11, and the “DLP-445 Remove the Release 3.4.x BLSR Lockout” task on page 1-14)
Required/As Needed	Required for BLSR only
Onsite/Remote	Onsite or remote (but in the presence of the workstation)



Note During the lockout, BLSR spans will not be protected. You must leave the BLSR in the lockout state until you have finished reverting all nodes, but then you must be sure to remove the lockout once you are finished reverting.



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 BLSR trunk cards (OC-12 or OC-48), go to the row in the table for that card and perform the following steps:
- Click the **East Switch** column to show the pull-down menu.
 - From the menu options, choose **Span Lockout**.
 - Click **West Switch** column to show the pull-down menu.
 - From the menu options, choose **Span Lockout**.
 - Click **Apply** to activate the command.
- Step 3** Repeat Step 2 at each node in the ring.



Note A Default K alarm or alarms on the protect STS timeslots can occur during this lockout period. Ignore these alarms if they occur.



Note Leave the BLSR in the lockout state until you have finished reverting all nodes.

- Step 4** Once you have performed the BLSR lockout on all BLSR nodes, perform the “[DLP-449 Revert to Protect Load](#)” task on page 1-18.

DLP-449 Revert to Protect Load

Purpose	Revert to the software you were running prior to the last activation. If you were running Release 2.2.1 or greater, this task will also restore your database to the provisioning you had prior to the activation.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-408 Prepare for Release 2.2.x to Release 3.4.x Upgrade , page 1-2; NTP-409 Back Up the Database , page 1-5; and NTP-410 Upgrade the Software , page 1-7 (up to and including the “DLP-U18 Activate the New Load” task on page 1-11, and the “DLP-445 Remove the Release 3.4.x BLSR Lockout” task on page 1-14, if applicable); DLP-448 Perform a Release 3.4.x BLSR Lockout , page 1-17 (if required)
Required/As Needed	Required for revert
Onsite/Remote	Onsite or remote (but in the presence of the workstation)


Note

To perform a supported (non service-affecting) revert from Release 3.4.x, the release you wish to revert to must have been working at the time you activated to Release 3.4.x on that node. Also, 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.


Note

In the following task, the database is restored automatically as a part of the revert only for Releases 2.2.1 and later. If you were running Release 2.2.0 before activation, you will need to manually restore the database after performing the steps to revert. Restoring the database manually is service affecting and should be performed during a service window.

- Step 1** From the node view, click the **Maintenance > Software** tabs.
- Step 2** Verify that the protect software displays 2.2.x (the release you upgraded from).
- Step 3** Click **Revert**. Revert activates the protect software and restores the database from the previous load. A dialog box asks you to confirm the choice.
- Step 4** Click **OK**. This begins the revert and drops the connection to the node.
- Step 5** 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** Shut down your Netscape or Internet Explorer browser.
- Step 7** Wait one minute before restoring another node.


Note

When you upgrade to JRE 1.3.1.02, you cannot log into an ONS 15454 running Release 2.2.1 or prior (or an ONS 15327 running Release 1.0.0). If you are reverting to a release that required a previous version of JRE, you will need to reinstall Java and delete the jar files from your workstation’s system “temp” directory after reverting all of the nodes in the network. If you are reverting to a release that also uses JRE 1.3.1.02, or if you retained your older version of JRE during the upgrade, this will not be an issue.

- 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 Release 2.2.x to your workstation.



Note It might also be necessary to delete cache files from your browser's directory, or from the "temp" directory on your MS Windows workstation. If you have trouble reconnecting to CTC, see the ["DLP-444 Delete Cached JAR Files" task on page 1-13](#).

- Step 9** After reverting all nodes, remove any BLSR lockout using the ["DLP-450 Remove Release 2.2.x BLSR Lockout" task on page 1-19](#).

DLP-450 Remove Release 2.2.x BLSR Lockout

Purpose	To restore BLSR protection you must clear the span lockouts on all BLSR nodes after reverting the software load and restoring the database on all nodes. Use the following task to restore a BLSR using Release 2.2.x.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	DLP-448 Perform a Release 3.4.x BLSR Lockout, page 1-17 , and DLP-449 Revert to Protect Load, page 1-18
Required/As Needed	Required for BLSR
Onsite/Remote	Onsite or remote (but in the presence of the workstation)

- Step 1** In CTC node view, click the **Maintenance > Ring** tabs.
- Step 2** For each of the BLSR trunk cards (OC-12 or OC-48), go to the row in the table for that card and perform the following steps:
- Click the West Switch column to show the pull-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 after each selection of 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 in the East Switch column to show the pull-down menu.
 - From the menu options, choose **Clear**.
 - 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. From the **Provisioning > Ring** tabs, click the **Ring Map** button. If a new ring map exists, click **Accept**.
- Step 4** You have now completed the software revert task. All nodes should be provisioned as they were before the last activation; however, in case of trouble, Cisco provides the ["DLP-451 Manually Restore the Database" task on page 1-20](#) to retrieve your databases.

DLP-451 Manually Restore the Database

Purpose	If you were upgrading from Release 2.2.0, and subsequently performed a revert, this task will restore the pre-upgrade database manually.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	DLP-449 Revert to Protect Load, page 1-18 , and DLP-450 Remove Release 2.2.x BLSR Lockout, page 1-19 (if required)
Required/As Needed	Required for Release 2.2.0 database restoral after a revert; otherwise, as needed
Onsite/Remote	Onsite or remote (but in the presence of the workstation)



Caution

Do not perform these steps unless you are restoring Release 2.2.0 or the software revert for a later release failed.



Caution

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

-
- 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 will be restored and the TCC+s will reboot.
- Step 4** Once the TCC+s have rebooted, log back into CTC and verify that the database is restored.
Wait one minute before restoring the next node.
- Step 5** You have now completed the manual database backup.
-



Upgrading Release 3.x to 3.4.x Using the TCC+ Card

This chapter explains how to upgrade Cisco ONS 15454's Cisco Transport Controller (CTC) software from Release 3.x to Release 3.4.x using the Timing, Communications, and Control + (TCC+) card.

Before You Begin

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


Caution

Read each procedure before you begin the upgrade.


Caution

This chapter is only supported for Release 3.x. If you wish to upgrade from Releases 2.2.0 – 2.2.2, use the procedures in [Chapter 1, “Upgrading Release 2.2.x to 3.4.x Using the TCC+ Card”](#). If you wish to upgrade from a release prior to Release 2.2.0, you must call the Technical Assistance Center (TAC) at 877 323-7368 for assistance.


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 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, you may wish to check off each procedure on your printed copy of this chapter as you complete it.

This section lists the chapter procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. [NTP-404 Prepare for Release 3.x to Release 3.4.x Upgrade, page 2-2](#)—This section contains critical information and tasks that you must read and complete before beginning the upgrade process.
2. [NTP-405 Back Up the Database, page 2-4](#)—Complete the database backup to ensure that you have preserved your node and network provisioning in the event that you need to restore them.
3. [NTP-406 Upgrade the Software, page 2-6](#)—You must complete this entire procedure before the upgrade is finished.

4. [NTP-407 Revert to Previous Load, page 2-14](#)—Complete this procedure only if you need to return to the software load you were running before activating the Release 3.4.x software.

NTP-404 Prepare for Release 3.x to Release 3.4.x Upgrade

Purpose	This procedure steps you through the critical information checks and tasks you must complete before beginning an upgrade.
Tools/Equipment	ONS 15454s to upgrade; PC or UNIX workstation; Cisco ONS 15454 Release 3.4.x software.
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite or remote

-
- Step 1** Read the appropriate release notes.
- Step 2** Complete the [“DLP-452 Verify CTC Workstation” task on page 2-2](#).
- Step 3** Complete the [“DLP-453 Verify IP Addresses” task on page 2-3](#).
- Step 4** Complete the [“DLP-454 Verify LAN Connections” task on page 2-3](#).
- Step 5** Complete the [“DLP-455 Verify Common Control Cards” task on page 2-4](#).
- Step 6** When you have completed the tasks for this section, proceed with the [“NTP-405 Back Up the Database” procedure on page 2-4](#).
-

DLP-452 Verify CTC Workstation

Purpose	Before upgrading the workstation to run CTC Release 3.4.x, verify all PC or UNIX workstation hardware and software requirements.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of the 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 (w/SP-4 or higher) or Windows XP
 - UNIX workstation running Solaris
- Step 2** Ensure that your web browser software is one of:
- Netscape Navigator 4.73 or higher (Netscape Navigator is included on the ONS 15454 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 software CD).



Note When you upgrade to JRE 1.3.1.02, you will no longer be able to log into an ONS 15454 running Release 2.2.1 or prior, or an ONS 15327 running release 1.0.0. If you must later revert to a release that requires a previous version of the JRE, you will have to reinstall Java and delete the jar files from your workstation's user "temp" directory after reverting all of the nodes in the network. 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** Once you have verified that your workstation meets CTC Release 3.4.x requirements, proceed to the ["DLP-453 Verify IP Addresses" task on page 2-3](#).

DLP-453 Verify IP Addresses

Purpose	Use this task to ensure that there are no IP address conflicts with CTC.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	DLP-452 Verify CTC Workstation, page 2-2
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of the workstation)

- Step 1** Disable all other Ethernet devices (such as a dial-up adapter) on the workstation that runs CTC.
- Step 2** If you have multiple IP addresses on your workstation, you should remove them; you cannot install CTC Release 3.4.x if multiple IP addresses are configured.
- Step 3** You have completed the IP address check procedure. Now perform the ["DLP-454 Verify LAN Connections" task on page 2-3](#).

DLP-454 Verify LAN Connections

Purpose	Use this task to ensure LAN connections are correct.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	DLP-453 Verify IP Addresses, page 2-3
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of the workstation)

- Step 1** If you have multiple ONS 15454 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 Reference Guide* for LAN-connection suggestions.

- Step 2** After verifying that your LAN is properly configured, proceed to the [“DLP-455 Verify Common Control Cards” task on page 2-4](#).
-

DLP-455 Verify Common Control Cards

Purpose	You must now use CTC to check for duplex common control cards. The node must have two TCC+ cards and two cross-connect cards (two XCs, two XCVTs, or two XC10Gs).
Tools/Equipment	PC or UNIX workstation with CTC installed
Prerequisite Procedures	DLP-454 Verify LAN Connections, page 2-3
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of the workstation)

- Step 1** Log into the 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 [“NTP-405 Back Up the Database” procedure on page 2-4](#).
-

NTP-405 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	NTP-404 Prepare for Release 3.x to Release 3.4.x Upgrade, page 2-2
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of the workstation)

- Step 1** Complete the [“DLP-456 Back Up Software” task on page 2-5](#).
- Step 2** Complete the [“DLP-457 Perform a Manual Backup” task on page 2-5](#).
- Step 3** Once you have backed up the database, proceed to the [“NTP-406 Upgrade the Software” procedure on page 2-6](#).
-

DLP-456 Back Up Software

Purpose	Before upgrading from Release 3.x to Release 3.4.x software, you must back up the current database for all nodes in the network.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-404 Prepare for Release 3.x to Release 3.4.x Upgrade, page 2-2
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of the 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 the workstation's hard drive or on network storage. Use an appropriate file name with the file extension .db (for example, myDatabase.db).
- Step 5** Click **Save**. A message appears indicating that the backup is complete.
- Step 6** Click **OK**.
- Step 7** Repeat Steps 1 – 6 for each node in the network.
- Step 8** You have completed the software backup. Proceed to the “[DLP-457 Perform a Manual Backup](#)” task on [page 2-5](#).
-

DLP-457 Perform a Manual Backup

Purpose	Cisco recommends that you manually log critical information by either writing it down or printing screens where applicable. This task is optional after you have backed up the database.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	DLP-456 Back Up Software, page 2-5
Required/As Needed	Recommended
Onsite/Remote	Onsite or remote (but in the presence of the workstation)

- Step 1** Use the following table to determine the information you should log; complete the table (or your own version) for every node in the network.

Table 2-1 *Manually Recorded Data*

Item	Record data here (if applicable)
IP address of the node	
Node name	
Timing settings	

Table 2-1 Manually Recorded Data (continued)

Item	Record data here (if applicable)
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+	Slot 7 or Slot 11 (circle one)
Active XC/XCVT/XC10G	Slot 8 or Slot 10 (circle one)
Network information; do a print screen from the Provisioning tab in the network view.	
Current configuration: BLSR, 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	

- Step 2** Once you have backed up all databases and recorded all necessary information using the checklist, you can begin the “[NTP-406 Upgrade the Software](#)” procedure on page 2-6.

NTP-406 Upgrade the Software

Purpose	Use this procedure to upgrade your CTC software.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-405 Back Up the Database, page 2-4
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of the workstation)

- Step 1** Insert the Release 3.4.x software CD into the workstation CD-ROM (or otherwise acquire access to the software) to begin the upgrade process.



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

**Caution**

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

**Caution**

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

- Step 2** Complete the [DLP-458 Download the Release 3.4.x Software, page 2-7](#) (all nodes).
- Step 3** Complete the [DLP-459 Perform a BLSR Lockout, page 2-8](#) (BLSR nodes only).
- Step 4** Complete the [DLP-U19 Activate the New Load, page 2-9](#) (all nodes).
- Step 5** Complete the [DLP-461 Delete Cached JAR Files, page 2-11](#).
- Step 6** Complete the [DLP-462 Remove the BLSR Lockout, page 2-12](#) (BLSR nodes only).
- Step 7** Complete the [DLP-463 Set the Date and Time, page 2-13](#) (any nodes not using SNTP).
- Step 8** Complete the [DLP-464 Upgrade Spare TCC+ Units, page 2-13](#) (as needed for upgrading spare TCC+ cards).
- Step 9** To upgrade the software successfully, you must read and perform each of the tasks that applies to your network in the proper order. Begin with the “[DLP-458 Download the Release 3.4.x Software](#)” task on [page 2-7](#).

DLP-458 Download the Release 3.4.x Software

Purpose	Download the Release 3.4.x software to the ONS 15454 nodes prior to activation.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-405 Back Up the Database, page 2-4
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of the workstation)

**Note**

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

- Step 1** 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 opens.

- Step 4** Browse to locate the software files on the ONS 15454 System Software CD (or on your hard drive, if you are working from a local copy).
- Step 5** Open the “Cisco15454” folder.
- Step 6** Select the file with the “.pkg” extension and click **Open**.
- Step 7** In the list of compatible nodes, select the checkboxes 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** Once you have successfully downloaded the CTC Release 3.4.x software to each node you are upgrading, perform the “[DLP-459 Perform a BLSR Lockout](#)” task on page 2-8. If none of your nodes participate in a BLSR, you can skip the BLSR lockout and begin the “[DLP-U19 Activate the New Load](#)” task on page 2-9.

DLP-459 Perform a BLSR Lockout

Purpose	If any node you are upgrading is in a bidirectional line switched ring (BLSR) configuration, you must perform a span lockout at each node in the ring before activating the software for Release 3.4.x. Perform this task to issue a span lockout on a BLSR using CTC Release 3.x.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	DLP-458 Download the Release 3.4.x Software, page 2-7
Required/As Needed	Required for BLSR
Onsite/Remote	Onsite or remote (but in the presence of the workstation)



Note During the lockout, BLSR spans will not be 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 BLSR trunk cards (OC-12, OC-48, or OC-192), go to the row in the table for that card and perform the following steps:
- Click the **East Switch** column to show the pull-down menu.
 - From the menu options, choose **Span Lockout**.
 - Click **West Switch** column to show the pull-down menu.
 - 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 BLSR in the lockout state until you have finished activating all nodes.

Step 4 You have completed the BLSR lockout. You must now perform the “[DLP-U19 Activate the New Load](#)” task on page 2-9.

DLP-U19 Activate the New Load

Purpose	Log into and activate each node in the network.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	DLP-459 Perform a BLSR Lockout, page 2-8 , if required; otherwise, DLP-458 Download the Release 3.4.x Software, page 2-7
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of the 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 workstation as quickly as possible.



Note Make sure 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 before proceeding.

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

- a. Close all active telnet connections to the ONS 15454.
- b. Copy the memAudit.exe from the ONS 15454 software CD or the following Cisco.com web page to a folder on your hard drive:


```
http://www.cisco.com/cgi-bin/tablebuild.pl/ons15454
```
- c. In a command window, change the prompt to the folder where the memAudit.exe is located.
- d. At the prompt, type the following command:

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



Note Optional parameters exist for the memAudit command. For more information about the memAudit utility, view the memAudit_readme.htm file on the CD or Cisco.com web page.

- Step 2** Log into a node.
- Step 3** Record the IP address of that node.
- Step 4** Verify that the node has no new alarms. If alarms exist, clear them before proceeding.
- Step 5** From the CTC node view, click the **Maintenance > Software** tabs.
- Step 6** Verify that the protect version is 3.4.x.
- Step 7** Click **Activate**. The **Activate** dialog box appears with a warning message.
- Step 8** Click **Yes** to proceed with the activation. The “Activation Successful” message appears when the software is successfully activated.
- Step 9** Click **OK** to begin the node rebooting process.
- Step 10** 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. Once all cards have reset, this alarm clears.

Each card in the node reboots, beginning with the standby TCC+. Once the standby TCC+ is fully activated and fully rebooted, it becomes the active TCC+ and the other TCC+ reboots. When the TCC+s are finished, the XC/XCVT, or XC10G, in Slot 8 reboots, and then the XC/XCVT, or 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. TDM traffic can endure a hit of up to 50 ms. Expect Ethernet traffic to remain down from the time the TCC+s switch to the time all Ethernet cards have finished resetting. Once 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 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 removed to the network view during the node reboot, but after the reboot is complete, CTC will restore connectivity to the node.

- Step 11** In CTC, choose **File > Exit**.
- Step 12** Follow all steps in the [“DLP-461 Delete Cached JAR Files” task on page 2-11](#). When you have performed all of the steps in that task, continue here with the next step (Step 12).
- Step 13** 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/Refresh button). The new CTC applet for Release 3.4.x uploads. Because CTC Release 3.4.x is backwardly compatible with CTC Release 3.x, it affords you network visibility while you are upgrading.



Note Only activate one node at a time.

- Step 14** Log into each of the remaining nodes and perform the [“DLP-U19 Activate the New Load” task on page 2-9](#). The activation must be performed for every node that is running software Release 3.x. Allow each node to finish (all alarms cleared for 10 minutes) before activating the next node.

- Step 15** You have completed the activation task when you have activated all nodes with the Release 3.4.x software. If you performed a BLSR lockout before you began activation, you must now perform the “[DLP-462 Remove the BLSR Lockout](#)” task on page 2-12. Otherwise, go to the “[DLP-463 Set the Date and Time](#)” task on page 2-13.

DLP-461 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	DLP-U19 Activate the New Load , page 2-9
Required/As Needed	Required
Onsite/Remote	Onsite or remote (but in the presence of the workstation)

- Step 1** Delete cache files from your browser directory.

In Netscape:

- Choose **Edit > Preferences > Advanced > Cache**.
- Click **Clear Memory Cache**.
- Click **OK**.
- Click **Clear Disk Cache**.
- Click **OK** twice.

In Microsoft Internet Explorer:

- Choose **Tools > Internet Options > General**.
- Choose **Delete Files**.
- Select the **Delete all offline content** checkbox.
- Click **OK** twice.

- Step 2** Close your browser.



Note You will not be able to delete cached jar files from your hard drive until you have closed your browser. If you have other applications open that use jar files, you must also close them.

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

- In your Windows start menu, choose **Settings > Control Panel > System > Advanced**.
- Click **Environment Variables**. This will show you a list of user variables and a list of system variables.
- 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.
- Open the “TEMP” directory located in the path you just looked up.

- e. Select **View > Details**.
 - f. Select and delete all files with “jar” in 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 task, either the “[DLP-U19 Activate the New Load](#)” task on page 2-9, or the “[DLP-466 Revert to Protect Load](#)” task on page 2-15, and continue with the steps there.
-

DLP-462 Remove the BLSR Lockout

Purpose	Release the span lockouts on all BLSR nodes after the new software load is activated on all nodes. This task restores a BLSR using Release 3.4.x.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	DLP-461 Delete Cached JAR Files , page 2-11; DLP-U19 Activate the New Load , page 2-9
Required/As Needed	Required for BLSR
Onsite/Remote	Onsite or remote (but in the presence of the workstation)

- Step 1** In CTC node view, click the **Maintenance > BLSR** tabs.
- Step 2** For each of the BLSR trunk cards (OC-12, C-48, or OC-192), go to the row in the table for that card and perform the following steps:
- a. Click in 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 in 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** When all BLSR span lockouts are released, you have completed this task and should go to the “[DLP-463 Set the Date and Time](#)” task on page 2-13.
-

DLP-463 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 task to reset the date and time at each node.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	DLP-462 Remove the BLSR Lockout, page 2-12 , if required; otherwise, DLP-461 Delete Cached JAR Files, page 2-11 and DLP-U19 Activate the New Load, page 2-9
Required/As Needed	As needed
Onsite/Remote	Onsite or remote (but in the presence of the workstation)



Note If you are using SNTP, you do not need this task and can go to the [“DLP-464 Upgrade Spare TCC+ Units” task on page 2-13](#).

-
- 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 [“DLP-464 Upgrade Spare TCC+ Units” task on page 2-13](#).
-

DLP-464 Upgrade Spare TCC+ Units

Purpose	Upgrade all spare TCC+ units to Release 3.4.x.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	DLP-462 Remove the BLSR Lockout, page 2-12 if required; otherwise, DLP-U19 Activate the New Load, page 2-9 and DLP-461 Delete Cached JAR Files, page 2-11
Required/As Needed	Required for all spare TCC+ cards
Onsite/Remote	Onsite or remote (but in the presence of the workstation)

- Step 1** To upgrade a spare TCC+, place it in the standby slot of a node running Release 3.4.x. The card will upgrade automatically from the active TCC+.
- The standby TCC+ will copy one or both software releases from the active TCC+, as needed. Each software copy takes about 15 minutes, and the TCC+ will reset after each copy. Thus, for a TCC+ that has no matching software with the active TCC+, you should expect to see two TCC+ resets, lasting about 30 minutes total.



Note During the TCC+ upgrade, the LEDs on the upgrading card will flash alternately between “fail” and “standby.”

- Step 2** Once you have upgraded all of your spare TCC+ units, you have completed the software upgrade.



Note If you need to upgrade your cross connect cards, please refer to the user documentation for the software you are currently running. This procedure can be performed before or after the software upgrade; however, you must also refer to the user documentation for details on hardware requirements for the XC10G before upgrading to this card type.

NTP-407 Revert to Previous Load

Purpose	Return to the exact software and database provisioning you had before you activated Release 3.4.x.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-404 Prepare for Release 3.x to Release 3.4.x Upgrade , page 2-2, NTP-405 Back Up the Database , page 2-4, and NTP-406 Upgrade the Software , page 2-6 (up to and including the “ DLP-U19 Activate the New Load ” task on page 2-9, and the “ DLP-462 Remove the BLSR Lockout ” task on page 2-12, if applicable)
Required/As Needed	As needed
Onsite/Remote	Onsite or remote (but in the presence of the workstation)



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 from Release 3.x to Release 3.4.x software, you should have backed up the existing database at all nodes in the network (this is part of the “[NTP-405 Back Up the Database](#)” procedure on page 2-4). 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 tasks, in order.

- Step 1** Complete the “[DLP-465 Perform a BLSR Lockout](#)” task on page 2-15 (BLSR only).
- Step 2** Complete the “[DLP-466 Revert to Protect Load](#)” task on page 2-15.
- Step 3** Complete the “[DLP-467 Remove the BLSR Lockout](#)” task on page 2-16 (BLSR only).



Note The “[DLP-468 Manually Restore the Database](#)” task on page 2-17 is provided for reference only. Do not complete this task unless an attempt to revert has failed.

- Step 4** Once you have completed the necessary steps above, the revert is complete.

DLP-465 Perform a BLSR Lockout

Purpose	If you have a BLSR provisioned, before beginning the revert you must perform a span lockout at each node. Perform this task to issue a span lockout on a BLSR using CTC Release 3.4.x.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-404 Prepare for Release 3.x to Release 3.4.x Upgrade, page 2-2 , NTP-405 Back Up the Database, page 2-4 , and NTP-406 Upgrade the Software, page 2-6 (up to and including the “DLP-U19 Activate the New Load” task on page 2-9, and the “DLP-462 Remove the BLSR Lockout” task on page 2-12)
Required/As Needed	Required for BLSR only
Onsite/Remote	Onsite or remote (but in the presence of the workstation)

- Step 1** If you have a BLSR provisioned, before beginning the revert you must perform a span lockout at each node. Follow the “[DLP-465 Perform a BLSR Lockout](#)” task on page 2-15 to perform a span lockout on a BLSR using CTC Release 3.4.x.



Note Leave the BLSR in the lockout state until you have finished reverting all nodes.

- Step 2** Once you have performed the BLSR lockout on all BLSR nodes, perform the “[DLP-466 Revert to Protect Load](#)” task on page 2-15.

DLP-466 Revert to Protect Load

Purpose	Revert to the software you were running prior to the last activation. This task will also restore your database to the provisioning you had prior to the activation.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-404 Prepare for Release 3.x to Release 3.4.x Upgrade, page 2-2 ; NTP-405 Back Up the Database, page 2-4 ; and NTP-406 Upgrade the Software, page 2-6 (up to and including the “DLP-U19 Activate the New Load” task on page 2-9, and the “DLP-462 Remove the BLSR Lockout” task on page 2-12, if applicable); DLP-465 Perform a BLSR Lockout, page 2-15 (if required)
Required/As Needed	Required for revert
Onsite/Remote	Onsite or remote (but in the presence of the workstation)



Note To perform a supported (non service-affecting) revert from Release 3.4.x, the release you wish to revert to must have been working at the time you activated to Release 3.4.x on that node. Also, 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.x (the release you upgraded from).
- Step 3** Click **Revert**. Revert activates the protect software and restores the database from the previous load. A dialog box asks you to confirm the choice.
- Step 4** Click **OK**. This begins the revert and drops the connection to the node.
- Step 5** 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** Shut down your Netscape or Internet Explorer browser.
- Step 7** Wait one minute before restoring another node.



Note Because you upgraded to JRE 1.3.1.02, you cannot log into an ONS 15454 running Release 2.2.1 or prior (or an ONS 15327 running Release 1.0.0). If you are reverting to a release that required a previous version of JRE, you will need to reinstall Java and delete the jar files from your workstation's system "temp" directory after reverting all of the nodes in the network. If you are reverting to a release that also uses JRE 1.3.1.02, or if you retained your older version of JRE during the upgrade, this will not be an issue.

- 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 Release 3.x to your workstation.



Note It might also be necessary to delete cache files from your browser's directory, or from the "temp" directory on your MS Windows workstation. If you have trouble reconnecting to CTC, see the ["DLP-461 Delete Cached JAR Files" task on page 2-11](#).

- Step 9** After reverting all nodes, remove any BLSR lockout using the ["DLP-467 Remove the BLSR Lockout" task on page 2-16](#).
-

DLP-467 Remove the BLSR Lockout

Purpose	To restore BLSR protection you must clear the span lockouts on all BLSR nodes after reverting the software load and restoring the database on all nodes. Use the following task to restore a BLSR using Release 2.2.x.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	DLP-465 Perform a BLSR Lockout, page 2-15 , and DLP-466 Revert to Protect Load, page 2-15
Required/As Needed	Required for BLSR
Onsite/Remote	Onsite or remote (but in the presence of the workstation)

-
- Step 1** To restore BLSR protection you must clear the span lockouts on all BLSR nodes after reverting the software load and restoring the database on all nodes. Complete the [“DLP-462 Remove the BLSR Lockout”](#) task on page 2-12 to restore a BLSR using Release 3.x.
- 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 [“DLP-468 Manually Restore the Database”](#) task on page 2-17 to retrieve your databases.
-

DLP-468 Manually Restore the Database

Purpose	The revert task should have restored your Release 3.x database completely; however, as a precaution, Cisco includes here the steps to restore the pre-upgrade database manually.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	DLP-466 Revert to Protect Load, page 2-15 , and DLP-467 Remove the BLSR Lockout, page 2-16 (if required)
Required/As Needed	Required for Release 2.2.0 database restoration after a revert; otherwise, as needed
Onsite/Remote	Onsite or remote (but in the presence of the workstation)



Caution

Do not perform these steps unless the software revert failed.



Caution

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

- 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 will be restored and the TCC+s will reboot.
- Step 4** Once the TCC+s 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.
-

■ NTP-407 Revert to Previous Load