Upgrading the Cisco ONS 15454 MSTP to Release 10.6.x.x

First Published: 2016-11-22

Last Modified: 2017-04-28

Upgrading the Cisco ONS 15454 MSTP to Release 10.6.x.x

This document explains how to upgrade the Cisco ONS 15454 Cisco Transport Controller (CTC) software using control cards. For a complete list of compatible cards, see Card Compatibility

To understand the supported software upgrade paths, refer to the Software Upgrade Matrix .

TCC2/ TCC2P card support

The nodes with the TCC2/TCC2P cards in releases prior to R10.6.2 cannot be upgraded to R10.6.2 as the size of the software package exceeds the size of the TCC2/TCC2P flash drive. Hence, R10.6.2 does not have the TCC2/TCC2P software package. If the user wants to continue with the ONS 15454 chassis, it is recommended to use the TCC3 control card. If the user wants to upgrade to a ONS 15454 M6 or NCS 2015 chassis, it is recommended to use the TNCS or TNCS-O control cards.

Errorless Upgrades and Exceptions

This section describes important information to be aware of before you begin the upgrade process:

- During an upgrade from R8.5.x, R9.0, or R9.1 to R9.2.x or later releases, a loss of Gigabit Ethernet traffic of up to one second is incurred. This traffic loss occurs when auto-negotiation is disabled on the far end of the ADM-10G card. If the node has a path protection circuit, a path protection switchover occurs. To avoid this switchover during an upgrade, perform the path protection lockout procedure before upgrading the software. Note, however, this procedure does not help avoid hits in the flow of traffic.
- During a revert procedure, if Gigabit Ethernet traffic is not flowing or GFP alarms are present on an ADM-10G card, hard-reset the ADM-10G card to ensure smooth traffic flow.

Document Procedures

Procedures in this document must be performed in consecutive order unless noted otherwise. Ensure that the procedure is completed for each node in a given network. If you are new to upgrading the software, make a printed copy of this document and use it as a checklist.

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 as “procedures” and DLPs as “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 a 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-U487 Preparing to Upgrade to a New Release, on page 2—This procedure contains critical information and tasks that you must read and complete before beginning the upgrade process.
2. NTP-U488 Back Up the Cisco ONS 15454 Software Database, on page 3—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-U489 Upgrade the Cisco ONS 15454 Software , on page 4—Complete this procedure to complete the upgrade.
4. NTP-U490 Install Public-Key Security Certificate, on page 11— Complete this procedure to be able to run the software.
5. NTP-U491 Restore the Previous Software Load and Database, on page 12— Complete this procedure if you want to return to the previous software load you were running before activating the new release.
6. — Complete this procedure only if you want to upgrade to a new release using Transaction Language (TL1).

NTP-U487 Preparing to Upgrade to a New Release

Purpose	This procedure provides critical information checks and tasks you must complete before beginning an upgrade to the latest release. R10.6.x.x.
Tools/Equipment	Cisco ONS 15454 nodes
Prerequisite Procedures	"DLP-G46 Log into CTC" in the "Connect the PC and Log into the GUI" document.
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser

Procedure

Step 1 Before you begin, make sure that information related to your site, for example, date, street address, site phone number, and dialup number are stored in a safe and accessible location. The data will be useful during and after the upgrade.

Step 2 Read the release notes of the release you are upgrading to. Visit http://www.cisco.com/c/en/us/support/optical-networking/ons-15454-series-multiservice-transport-platforms/products-release-notes-list.html to download the release notes.

Step 3 Ensure your workstation meets the minimum hardware and software requirements before starting the upgrade. For more information on the hardware and software requirements, read the release notes.

Step 4 Refer to the Software Upgrade Matrix to verify if the upgrade path is supported.

Step 5 Make sure that the control cards are installed in the appropriate slots on all the nodes in the network and on both the slots as indicated here. For a complete list of supported control cards, see https://www.cisco.com/c/en/us/td/docs/optical/15000r10_0/dwdm/controlcard_nodeconfig/guide/b_ons_control_card_node_config/b_ons_control_card_node_config_chapter_01101.html#ID6:

- ONS 15454 shelf
  - cards are in Slots 7 and 11
- ONS 15454 M6 shelf — cards in Slots 1 and 8
- ONS 15454 M2 shelf— cards in Slot 1

Note When upgrading network elements with a subtended M12 shelf and TCC3 as shelf-controller, the following steps are to be followed:

1. Upgrade the M6 or M15 node controller without the M12 connected.
2. At the end of the upgrade, connect the M12 shelf.
3. Wait till the M12 configuration is complete.

It is not possible to revert from R10.6.2 to a previous release, with an M12 as a subtended shelf. The download of a legacy package on a subtended M12 in a flex node is not allowed.

Step 6 Repeat the above step for every node in the network.

Step 7 Collect the node diagnostics logs from the node. This action is very useful incase the upgrade fails, as the diagnostics help in understanding if the node had issues before the upgrade.

Step 8 Export the current alarms and conditions to your local storage. After the upgrade, if new alarms or conditions arise, then comparing the time stamp of the alarm to the previously saved time stamp helps in identifying new alarms or conditions.

Step 9 Perform a backup of the node database. This is very useful incase the upgrade fails, then the database can be restored using the backup. The detailed procedure for backing up the database is discussed in the next section.

Stop. You have completed this procedure.

NTP-U488 Back Up the Cisco ONS 15454 Software Database

Purpose	This procedure retains all configuration data for your network before performing the upgrade.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	• "DLP-G46 Log into CTC" in the "Connect the PC and Log into the GUI" document. • NTP-U487 Preparing to Upgrade to a New Release, on page 2
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser

Procedure

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

Step 2 In the database pane, click the **Backup** button.

The Database Backup dialog box is displayed.

Step 3 Click **Browse**. Navigate to the local PC directory or network directory and type a database name using the IP address of the node to upgrade (such as database15454SONET010107.db) in the File Name field and click **OK**. To overwrite an existing file, click **Yes**.

Step 4 When the backup is complete, click **OK.**

Step 5 Repeat Steps 1 through 5 for each node in the network.

Step 6 (Optional) It is recommended that you manually log critical information by either writing it down, printing screens, or by exporting the data to an appropriate format, as applicable. Use the following table to determine the information that should be logged.

Information	Record Data Here
IP address of the node	
Node name	
Timing settings	
DCC[1] connections—list all optical ports with active DCCs	
User IDs of all users, including at least one Superuser	
Inventory—A print screen of the Inventory window	
Active TCC2/TCC2P/TCC3 card	Slot 7 or Slot 11
Network information—A print screen of the Provisioning tab in the network view	
List all protection groups in the system—A print screen of the Protection group window	
List alarms—A print screen of the Alarm window	
List circuits—A print screen of the Circuit window	

[1] DCC=data communications channel

Stop. You have completed this procedure.

NTP-U489 Upgrade the Cisco ONS 15454 Software

Purpose	This procedure upgrades the CTC software to R10.6.x.x and must be performed on all nodes, or groups of nodes to be upgraded.

Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-U488 Back Up the Cisco ONS 15454 Software Database, on page 3
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser

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

Note If you are upgrading multiple nodes from a release prior to Software R7.0 and have at least one optical channel network connection (OCHNC) circuit, you will see transient OCHTERM-INC conditions raised during the upgrade. This condition clears after all the nodes have been upgraded.

Note During the upgrade of R8.0 or R8.5.x to a later release, if path protection circuits of type UPSR_DRI or 2waydc was created on an ADM-10G card, any existing software provisioning on the card is lost. Therefore, make sure that these path protection circuit types are not present before you upgrade to a later release.

Note The ADM-10G card does not support adding drops to existing Synchronous Transport Signal (STS) circuits. Therefore, when upgrading from R8.0 to a later release, delete any STS circuits with multiple drops on the ADM-10G card.

Procedure

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

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

Step 2 Complete the DLP-U546 Download the ONS 15454 Software, on page 6 task for all nodes to be upgraded.

Step 3 Complete the DLP-U548 Activate the New Cisco ONS 15454 Software, on page 7 task for all nodes to be upgraded.

Note Only one node can be activated at a time. During a parallel upgrade, activate another node as soon as the controller cards reboot successfully. To perform parallel upgrade remotely, wait five minutes for the controller cards to reboot completely.

Step 4 Complete the DLP-U549 Delete Cached JAR Files, on page 9 task, as necessary.

Step 5 (Optional) If you want to prevent a software revert to an earlier software release, complete the DLP-U546 Download the ONS 15454 Software, on page 6 task on all nodes, or groups of nodes you are upgrading a second time.

Caution If the software is downloaded again after a version is activated, a revert to the previous version cannot be performed.

Step 6 If you need to return to the software and database you had before activating Software R10.6.x.x, proceed with the NTP-U491 Restore the Previous Software Load and Database, on page 12 procedure.

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.

Note When you upgrade a TCC2P card to a TCC3, the SFTWDOWN alarm can be raised and cleared more than once before the software download is complete. For example, when you remove the standby TCC2P card in Slot 11 and replace it with a TCC3 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 7 To back up the Software R10.6.x.x database for the working software load, see NTP-U488 Back Up the Cisco ONS 15454 Software Database, on page 3 procedure in order to preserve the database for the current release.

After the upgrade is complete, the date and time in CTC is reset.

Stop. You have completed this procedure.

What to do next

After upgrading the software to a different build, if there is a change in the FPGA, the FPGA is upgraded automatically. During the FPGA upgrade process, the card goes for a cold reboot. If Optical Supervisory Channel (OSC) is provisioned, then the transient PPM-IMPROPER-REMOVAL alarm is raised, which gets cleared in a short span of time. This happens because of the power glitches to the PPM while the card is coming up after the cold reboot.

DLP-U546 Download the ONS 15454 Software

Purpose	This task downloads R10.6.x.x software to the ONS 15454 nodes prior to activation.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-U488 Back Up the Cisco ONS 15454 Software Database, on page 3
Required/As Needed	Required
Onsite/Remote	Onsite or remote

Security Level	Maintenance user or higher

Note The control card contains flash memory with two partitions—working and protect (backup). The software is downloaded to the protect (backup) partition of the flash memory on both the standby and active cards. This download is not traffic affecting because the active software continues to run in the primary RAM location. The software can therefore be downloaded at any time.

Note To download and upgrade the software using TL1, see the procedure.

Procedure

Step 1 From CTC View menu, choose **Go to Network View**.

Step 2 Make sure that the alarm filter is turned off. To do so, complete the following:

a) Click the **Filter** tool located at the lower-left side of the window.

The Alarm Filter dialog box appears.

b) Click to select any check box that is not selected in the Show Severity section of the **General** tab.

Step 3 Resolve any outstanding alarms. To view alarms for all the nodes in the network, click the **Alarms** tab.

Note The SFTWDOWN alarm is raised on the standby and active control cards during software download. The alarms clears as soon as the download is complete.

Step 4 From the CTC View menu, choose **Go to Home View** to go to the node view.

Step 5 Click the **Maintenance**> **Software** tabs.

Step 6 Click the **Download** button. The Download Selection dialog box appears.

Step 7 Locate the software files on the software CD or on your hard drive.

Step 8 To open the Cisco ONS 15454 folder, choose the file with the PKG extension and click **Open**.

Step 9 From the list of compatible nodes, select the nodes where the software must be downloaded.

Note It is recommended that simultaneous software downloads on the section data communications channel (SDCC) be limited to eight nodes at a time, using the central node to complete the download. If more than eight concurrent software downloads are selected at a time, it is placed in a queue.

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

Step 11 Return to your originating procedure (NTP).

DLP-U548 Activate the New Cisco ONS 15454 Software

Purpose	This task activates the software on each node in the network.
Tools/Equipment	PC or UNIX workstation

Prerequisite Procedures	DLP-U546 Download the ONS 15454 Software, on page 6
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser

Note It is recommended that the first node that is activated be connected via LAN. This ensures that the new CTC JAR files download to the workstation as quickly as possible.

If a node is provisioned to have no LAN access, the value is overridden in the case of node isolation. Additionally, if the node is not reachable, the LAN access is turned on. It is recommended that you avoid node isolation.

Procedure

Step 1 If CTC is not already started, 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 Make sure that the alarm filter is turned off. To do so, complete the following:

a) Click the **Filter** tool at the lower-left side of the window.

The Alarm Filter dialog box appears.

b) Click to select any check box that is not selected in the Show Severity section of the **General** tab.

Step 4 Make sure that all cards that are part of a 1+1 or Y-cable protection group must be active on the working card of the protection group and no protection switches are occurring. Also, ensure that traffic carrying protect cards are in a standby state. To do so, complete the following:

a) In the node view, click **Maintenance** > **Protection** tabs.

b) Select each protection group listed and view the active or standby status of each card in the Selected Group area.

Step 5 In shelf view, click the **Maintenance** > **Software** tabs.

Step 6 Verify that the version in the Protect Version column is R10.6.x.x.

Step 7 Click the **Activate** button. The Activate dialog box displays a warning message.

Step 8 Click **Yes** to proceed with the activation.

During node activation, all the common control cards in the node reboot beginning with the standby card. As soon as the standby card recovers from the reboot, it signals the active card to reset as a standby card and the standby card transitions to active. An Activation Successful message indicates that the software is successfully activated.

Step 9 Click **OK**.

The connection between CTC and the node is lost and CTC displays the Network view. The INCOMPATIBLE-SW alarm is raised in CTC for the first node that is activated because CTC is unable to connect to the NE due to differing, incompatible versions of the software between CTC and the NE. A CTC

alert is displayed to update the CTC software. To clear the INCOMPATIBLE-SW alarm, perform steps 10 through 12 only for the first node that is activated on the network.

During the activation process:

- The SYSBOOT alarms are raised when the common control cards and cross-connect card reset. These alarms clears when all the cards reset.

  The activation process can take up to 30 minutes, depending on the number of cards installed in the node.

- The GCC-EOC, EOC, and EOC-E alarms are transient. These alarms are raised and cleared during the upgrade process when the control cards and line cards reset.
- Protect cards in the Y-cable protection group boot next, in the order that the protection group was created.
- Other line cards reset one after the other in the order of slot number.

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 10 In CTC, choose **File > Update CTC**. The CTC software is updated. A CTC alert is displayed to restart CTC.

Step 11 In CTC, choose **File > Exit.**

Step 12 Start CTC again.

Step 13 (Optional) Run the Cache Loader pre-caching utility. This logs you into CTC at a faster pace after an upgrade. However, you must log into nodes running releases prior to Software R4.6.

Note If you do not plan to run the pre-caching utility, it is recommended 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.

Perform the following steps to run the Cache Loader.

a) Load the Software 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 appears.
c) Click the **Next** button. The Setup Options dialog box appears.
d) Choose **Custom**, and click the **Next** button. The Custom Options dialog box appears.
e) Click to select **Cisco Transport Controller**, and **CTC JAR files** (deselect any other preselected options) and click the **Next** button. A confirmation dialog box appears.
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 in the wizard, click **Finish.**

Step 14 Click the **Launch CTC** button in the CTC launcher window.

The new CTC applet loads. The login window is displayed.

Step 15 Type the user name and password and click **Login**.

Step 16 Return to your originating procedure (NTP).

DLP-U549 Delete Cached JAR Files

Purpose	This task deletes cached JAR files.

Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	None
Required/As Needed	You need to complete this task after you activate the first network node.
Onsite/Remote	Onsite or remote
Security Level	Maintenance user or higher

Note Whenever the CTC software is upgraded or reverted, make sure that the browser and hard drive cache files are cleared.

Procedure

Step 1 Delete cached files from your browser directory.

In Netscape:

a) Select **Edit** > **Preferences**. Click the **Advanced** tab and 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) Select **Tools** > **Internet Options**. The Internet Options dialog box appears.
b) Click the **General** tab, and then click the **Delete Files** button.
c) Select the **Delete all offline content** check box.
d) Click **OK** twice.

Step 2 Close the browser.

Note Cached JAR files cannot be deleted from the hard drive until the browser is closed. Other applications that use JAR files must also be closed.

Step 3 On Windows systems, delete cached files from your workstation in this location:

`C:\Documents and Settings\`*`username`*`\Application Data\Cisco\CTC`

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

Step 5 Return to your originating procedure (NTP).

DLP-U551 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
Security Level	Superuser

Note If you are using SNTP, this task is not applicable.

Procedure

Step 1 In CTC node view, click the **Provisioning** > **General** tabs.

Step 2 Set the correct date and time. Click **Apply** .

Step 3 Repeat Steps 1 and 2 on all the remaining nodes.

Step 4 Return to your originating procedure (NTP).

NTP-U490 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 software R4.1 or later.
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

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 on the PC only for the current session. After the session ends, the certificate is deleted. This dialog box appears at the next login into the node.
- Deny—Denies permission to install the certificate. If this option is chosen, login into the node is denied.

- Grant always—Installs the public-key certificate and does not delete it after the session is over. It is recommended to use this option.
- View Certificate—The public-key security certificate is displayed.

After the completion of the security certificate dialog boxes, the web browser displays information about the Java and system environments. If this is the first login, a CTC downloading message appears while CTC files are downloaded to the computer. The process can take several minutes, if it is the first time. After the download, the CTC Login dialog box appears.

Step 3 Return to the software and database you had before activating the software, proceed with the NTP-U491 Restore the Previous Software Load and Database, on page 12 procedure.

Stop. You have completed this procedure.

NTP-U491 Restore the Previous Software Load and Database

Purpose	This procedure returns to the software and database provisioning that was present before R10.6.x.x was activated. The software load and database cannot be restored to the previous version if the software on both the working and protect cards were upgraded to R10.6.x.x.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	"DLP-G46 Log into CTC" in the "Connect the PC and Log into the GUI" document. NTP-U487 Preparing to Upgrade to a New Release, on page 2 NTP-U488 Back Up the Cisco ONS 15454 Software Database, on page 3 NTP-U489 Upgrade the Cisco ONS 15454 Software , on page 4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Note Tasks to revert to a previous load are not part of the upgrade, and are provided here as a convenience to those wishing to perform a revert after an upgrade. If you have successfully performed all necessary procedures up to this point, you have finished the software upgrade.

Caution If a node is set to secure, dual-IP mode, the database information is overwritten with this configuration and cannot be reverted to single-IP repeater mode.

Procedure

Step 1 Complete the DLP-U552 Revert to Protect Load, on page 13 task.

Step 2 If the software revert to your previous release failed to restore the database, complete the DLP-U553 Manually Restore the Database, on page 14 task.

Stop. You have completed this procedure.

DLP-U552 Revert to Protect Load

Purpose	This task reverts to the software you were running prior to the last activation.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-U487 Preparing to Upgrade to a New Release, on page 2 NTP-U488 Back Up the Cisco ONS 15454 Software Database, on page 3 NTP-U489 Upgrade the Cisco ONS 15454 Software , on page 4
Required/As Needed	Required for revert
Onsite/Remote	Onsite or remote
Security Level	Superuser

Note To perform a supported (non-service-affecting) revert from R10.6.x.x, the release you want to revert to must have been working at the time you activated to the current software version on that node. Also, a supported revert automatically restores the node configuration at the time of the previous activation. The exception to this is when you have downloaded R10.6.x.x a second time, ensuring that no revert to a previous load can take place. In this case, the revert occurs, but is not traffic-affecting and does not change the database.

Note Ensure that all cards that are part of a protection group (1+1 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. View the active/standby status of each card in the Maintenance tab.

Procedure

Step 1 From the node view, click the **Maintenance** tab, then click the **Software** button.

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

Step 3 Click the **Revert** button. Revert activates the protect software and restores the database from the previous load. A confirmation dialog box appears.

Note Any FPGA downgrades during the revert process may affect traffic. Configuration changes made after activation are lost when you revert.

Step 4 Click **OK**. This begins the revert process and drops the connection to the node.

Step 5 Wait until the software revert completes before continuing.

Note The system reboot may take up to 30 minutes to complete.

Step 6 Wait one minute before reverting another node.

Step 7 After reverting all 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 8 Perform the DLP-U549 Delete Cached JAR Files, on page 9 task.

Step 9 Return to your originating procedure (NTP).

DLP-U553 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-U552 Revert to Protect Load, on page 13
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
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.

Procedure

Step 1 In CTC node view, click the **Maintenance** tab, then click the **Database** button.

Step 2 Click the **Restore** button. The DB Restore dialog box appears.

Step 3 Click **Browse** to locate the database file stored on the workstation hard drive or on network storage.

Step 4 Click the database file to highlight it and click **Open**. The DB Restore dialog box appears.

Step 5 If you need a complete database restore, check the **Complete database (System and Provisioning)** checkbox.

Note The following parameters are restored only when the **Complete Database (System and Provisioning)** checkbox is checked: node name, IP address, subnet mask and gateway, and IIOP port. If you change the node name and then restore a backed up database on this node, the circuits automatically map to the newly renamed node. It is recommended to keep a record of the old and new node names.

Step 6 Click **Ok**.

The database is restored and the control cards reboot.

Step 7 When the control cards have finished rebooting, log into CTC and verify that the database is restored.

Wait one minute before restoring the next node.

Step 8 Repeat Steps 1 to 7 for each node in the network.

You have now completed the manual database restore.

Note When the complete database is restored, the node does not report an event regarding the IP change; the node reboots and configures the new IP from the database. If the IP address being restored is not in the CTC network IP addressing scheme, you might lose visibility of the node. To resolve this, you must launch CTC with the IP mentioned in the table against the database backup. Refer to the table, "Manually Recorded Data" in the NTP-U488 Back Up the Cisco ONS 15454 Software Database, on page 3 procedure for more information.

Step 9 Return to your originating procedure (NTP).

NTP-U494 Upgrading the Software from the Cisco ONS 15454 DWDM Lite Package to the Cisco ONS 15454 DWDM Full Package

Purpose	This procedure upgrades the 15454 DWDM lite package to the 15454 DWDM full package on the active and standby TCC3 cards before adding the Cisco ONS 15454 M6 shelves to the multishelf node.
Tools/Equipment	Cisco ONS 15454 nodes
Prerequisite Procedures	Complete the upgrade procedure on the node containing the TCC2/TCC2P card.
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser

Procedure

Step 1 Complete the "DLP-G46 Log into CTC" task in the Connect the PC and Log into the GUI document on the node where you want to upgrade the 15454 DWDM lite package to the 15454 DWDM full package. If you are already logged in, continue with the next step.

Step 2 Complete the DLP-U546 Download the ONS 15454 Software, on page 6 task to download the 15454 DWDM full package on the node. The 15454 DWDM full package is downloaded on the active TCC3 card. In a multishelf node, the 15454 DWDM full package is also downloaded on the subtended shelf controller.

Step 3 Complete the DLP-U548 Activate the New Cisco ONS 15454 Software, on page 7 task on the node to activate the software.

Step 4 Repeat the DLP-U546 Download the ONS 15454 Software, on page 6 task to download the 15454 DWDM full package on the standby TCC3 card.

Stop. You have completed this procedure.

NTP-U493 Upgrade to the ONS 15454 Software Using TL1

Purpose	This procedure upgrades the software to R10.6.x.x using TL1 rather than CTC.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-U487 Preparing to Upgrade to a New Release, on page 2 NTP-U488 Back Up the Cisco ONS 15454 Software Database, on page 3
Required/As Needed	Optional
Onsite/Remote	Onsite or remote
Security Level	Superuser

Note This procedure assumes you are upgrading using TL1 Release 6.x and later. TL1 commands used prior to activation to Release 6.x vary in syntax depending on the ONS 15454 release that you are actually upgrading from. To ensure that your syntax for each command is correct, see the TL1 syntax in the TL1 Command Guide for your particular release when issuing the following commands:

- ACT-USER
- COPY-RFILE
- OPR-PROTNSW-<OCN_TYPE>
- RTRV-COND-ALL
- RTRV-ALM-ALL
- RLS-PROTNSW-<OCN_TYPE>

Note To download the software using TL1, an FTP server or a terminal emulation program like HyperTerminal must be running on the workstation.

Note The download (COPY-RFILE) command is different when downloading software to a gateway network element (GNE) or an end network element (ENE) under the following conditions:

- FTP is being used.
- Server is set up with a login and password of FTPUSER1 and FTPUSERPASSWORD1.
- FTP server has an IP address of 10.1.1.1.
- FTP server is running on the standard FTP port.
- Software package is called “15454DWDMxxx-0930-xxxx-xxxx.pkg.”

Note When upgrading from R8.0 and later, if the path protection circuits of type UPSR_DRI or 2waydc is created on the ADM-10G card, software provisioning is lost. Ensure that there are no path protection circuits of type UPSR_DRI or 2waydc created on the ADM-10G card before upgrading to the latest release.

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 ":2361" after the FTP server IP address 10.111.11.1 denotes port 21 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 PKG 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";
```

Procedure

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 node.

Step 2 Type the IP address for the node, using port 3083 or 2361.

The terminal emulation interface displays a warning message and a command prompt (usually >). You can enter 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 Operation Support System (OSS) profile user ID (required).
- <CTAG> is the correlation tag that correlates command and response messages (required).
- <pid> is the password identifier (required).

  For example, in the TL1 command:

  ```
  ACT-USER::CISCO99:100::PASSWORD;
  ```

  CISCO99 is the user ID, 100 is the correlation tag (used to correlate commands to command responses), and PASSWORD is the password associated with the user ID.

  A response message containing the CTAG that you specified indicates the completion status of the command.

Step 4 Repeat Step 2 for each node to be upgraded.

Step 5 Type the **COPY-RFILE** command in the TL1 window or, if you are using HyperTerminal, click **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 the controller card.

```
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 (required).
- <xfertype> 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 6 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-U487 Preparing to Upgrade to a New Release, on page 2" procedure on page 8 for each node to be upgraded.

Step 9 Complete NTP-U488 Back Up the Cisco ONS 15454 Software Database, on page 3 for each node to be upgraded.

Step 10 Verify that there are no outstanding alarms or conditions on each node using the following commands:

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

where:

- <TID> is the target identifier (optional)
- <AID> is the access identifier that indicates the facility in the node to which the switch request is directed (must not be null) (required).
- <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:

- <TID> is the target identifier
- <AID> is the Access IDentifier that indicates the facility in the node to which the switch request is directed (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, in a parallel upgrade you can begin activation of the next node as soon as the controller cards for the current node have rebooted successfully. If you wish to perform a parallel upgrade remotely, wait five minutes for the controller cards to complete the reboot.

Step 11 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 (optional).
- <CTAG> is the correlation tag that correlates command and response messages.
- <MEM_SW_TYPE> indicates a memory switch action during the software upgrade. MEM_SW_TYPE is ACT for activate. MEM_SW_TYPE is RVRT to revert.

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

The following occurs:

- Each card in the node reboots, beginning with the standby card. When the standby card reboots, it signals to the active card that it is ready to take over. When the active receives this signal, it resets itself, and the standby takes over and transitions to active. The pre-upgrade version of the card is now the standby .
- While the second is rebooting, the stand by cross-connect card (SONET/SDH only) reboots, and then the active cross-connect card (SONET only) reboots.
- 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).
- A system reboot (SYSBOOT) alarm is raised while activation is in progress (following the 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.) Repeat this step for each

node that will be upgraded, moving from the furthest node from the GNE toward the GNE itself, which should be activated last.

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

Step 12 After all nodes have been activated, log in using CTC or Telnet and verify there are no outstanding alarms.

Step 13 To back up the database for the working software load, see NTP-U488 Back Up the Cisco ONS 15454 Software Database, on page 3 in order to preserve the database for the current software.

Stop. You have completed this procedure.

Upgrading legacy Optical Line Amplifier nodes to R10.6.0 NCS 2000 flex package

The legacy Optical Line Amplifier (OLA) nodes can be upgraded from R10.3.0.2 ONS 15454 DWDM full package to R10.6.0 NCS 2000 flex package.

To support easy migration of customer networks to the NCS 2000 flex package, the Not Traffic Affecting (NTA) upgrade of OLA nodes from ONS 15454 DWDM full package to NCS 2000 flex package is supported. In this case, when activating the NCS 2000 flex package, there is no traffic interruption and the system does not delete the existing database. For successful activation, the OLA nodes must meet the following conditions, else the node database is deleted.

- The OLA nodes must be running on M6 or M15 shelf
- Only OPT-EDFA-xx or OPT-AMP-C line cards are provisioned
- Upgrade all the OLA nodes present in the network to 10.6.0 ONS 15454 DWDM before proceeding to migrate to 10.6.0 NCS 2000 flex package

The limitations for the upgrade are:

- It is not possible to migrate from the R10.3.0.2 ONS 15454 DWDM full package directly to R10.6.0 NCS 2000 flex package. An intermediate step is to upgrade the nodes to NCS 2000 10.6.0 fixed-grid package.
- Once the nodes are activated to R10.6.0 NCS flex package, it is not possible to revert to R10.3.0.2, as the original database for 10.3.0.2 is no longer available.

Related Documentation

Use this document in conjunction with the following publications:

- Release notes:

  http://www.cisco.com/en/US/products/ps13234/prod_release_notes_list.html

- TL1 command guides:

  http://www.cisco.com/en/US/products/hw/optical/ps2006/prod_command_reference_list.html

- Troubleshooting guides:

  http://www.cisco.com/en/US/products/ps13234/prod_troubleshooting_guides_list.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the What's New in Cisco Product Documentation as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.