Upgrading the Cisco CPT to Release 9.5.x

Note

- The terms "Cisco CPT" and "CPT" are used interchangeably.
- Release 9.5.x includes 9.5, 9.5.1, 9.5.1.1, 9.5.1.2, 9.5.2, and 9.5.3.

This guide describes the procedures to upgrade the Cisco CPT software to Release 9.5.x

Revision History

Date	Notes
August 2013	Added information about data loss after an upgrade to Release 9.5.3 in the Software Upgrade Compatibility section.
January 2013	Added information about data loss after an upgrade to Release 9.5.2 in the Software Upgrade Compatibility section.
October 2012	Added information about data loss during an upgrade to Release 9.5.1.1 in the Caveats section.
July 2012	• Added information about data loss during or after an upgrade to Release 9.5.x in the Caveats section. • Added information about the upgrade path supported in the Software Upgrade Compatibility section.

Software Upgrade Compatibility

This table lists upgrade paths supported in the Cisco CPT platform:

Release	Upgrade Options
9.3	9.3.0.1[1,12], 9.3.0.2[1,12], 9.5.0[2,3,4,12]
9.3.0.1	9.3.0.2[1,12], 9.5.0[2,3,4,12]
9.3.0.2	9.5.0 [2,3,4,5,12], 9.5.1[2,3,5,6,7,8,9,12]
9.5.0	9.5.1[1,6,7,8,9,10,12]
9.5.1	9.5.1.1[10,12], 9.5.2[11,12], 9.5.2.1[12], 9.5.3 [12]
9.5.2	9.5.2.1[13]

1 During an upgrade, the CPT line cards reload with a new image version in a staggered manner, that is, the line card in slot 2 reloads with a new image version which is followed by the line card in slot 3.
2 During an upgrade, the CPT line cards reload with a new image version simultaneously, that is, the line card in slot 2 and slot 3 reloads with a new image version at the same time.
3 After an upgrade, sometimes an MEA or PROV-MISMATCH alarm is raised on the pluggable port module (PPM)

4 During an upgrade, the fabric and line cards are in the transient-incorrect states.
5 When the cumulative bandwidth of MPLS-TP services on a link exceeds the maximum threshold defined for that link, all configuration get loss during an upgrade in CTC mode.
6 When an MPLS-TP tunnel is created with only working LSP, and this LSP is in lockout state, all configuration get loss during an upgrade in CTC mode.
7 MPLS-TP and LDP configurations cannot be enabled at the same time on a port. If enabled, it causes data loss during an upgrade due to invalid port configurations.
8 MPLS-TP and REP configurations cannot be enabled at the same time on a port. If enabled, it causes data loss during an upgrade due to invalid port configurations.
9 Selecting the **Create PW Class Automatically** check box does not create the pseudowire class automatically if the source and destination nodes are created on the different versions of CPT.
10 When you edit a VPLS circuit you create new endpoints. If the cumulative sum of entries (EFPs and neighbor node) made in the **Endpoint PW** tab and **Endpoint EFP** tab exceeds 127, it leads to data loss during an upgrade.
11 After an upgrade, database loss occurs when the tunnel ID of the pseudowire class, associated to a VPLS circuit, does not exist. This is because the tunnel ID was modified when the user edited the pseudowire class in an earlier release of CPT.
12 After an upgrade, the system fails to transmit the OAM packets and the PEER-MISSING alarm is raised. It is recommended to remove the EFM configuration and add it again to clear the alarm.
13 After an upgrade, database loss occurs if the IP of the interface on which an IP-based MPLS-TP link number exist is deleted.

Caveats

Upgrade Cisco CPT to Release 9.5.x

This section describes caveats, scenarios, and possible fixes to avoid database loss when you upgrade to Release 9.5.x.

Note Before upgrading the software, all the databases must be validated by the customers and the TAC team.

- **Upgrading to release 9.5.3**
  - Pseudowire cannot be configured on the channel-group port that is also a destination port of a SPAN. If configured, it causes data loss during an upgrade.
  - MTU value of a port cannot be configured less than MTU value of the pseudowire configured on that port. If configured, it causes data loss during an upgrade.
  - A port configured as a destination port of a SPAN cannot be used as a port when configuring an MPLS-TP tunnel. If configured, it causes data loss during an upgrade.
  - MTU value of a LAG cannot be configured less than MTU value of the pseudowire configured over this LAG. If configured, it causes data loss during an upgrade.
  - When a child policy attached to a parent policy is edited, it causes data loss during an upgrade because the parent policy does not reflect those modifications.
  - When the port with an MPLS-TP link configured on it is deleted, it causes data loss during an upgrade.
  - LDP cannot be configured on the port where REP is already configured. If configured, it causes data loss during an upgrade.
  - LDP cannot be configured on the port where EVC is already configured. If configured, it causes data loss during an upgrade.
  - When you remove the IP address from the interface on which the IP-based MPLS-TP link is configured, it causes data loss during an upgrade.

- Different services cannot be configured with same VLAN ID. If configured, it causes data loss during an upgrade.
- When the static OAM class with a pseudowire class configured on it is deleted, it causes data loss..
- When a pseudowire class (associated to a VPLS) is enabled with Static OAM class and the signaling protocol as None, it causes data loss. It is recommended to create a pseudowire with the interworking as None and the signaling protocol as LDP.
- When a CFM with Y1731 configured on it is deleted, it causes data loss during an upgrade.
- When a port with QoS table-map configured on it is deleted, it causes data loss during an upgrade.
- When a port with ARP based MPLS-TP link configured on it is deleted, it causes data loss during an upgrade.
- When a pseudowire with Y1731 configured on it is deleted, it causes data loss during an upgrade.
- When an EVC with Y1731 configured on it is deleted, it causes data loss during an upgrade.
- When a port on which a service is already configured is used to configure a service with the default encapsulation type, it leads to data loss.
- When a port on which an MPLS-TP tunnel is already configured is used to configure any other service, it leads to data loss.
- When MVR is enabled for a service that is not untagged, it leads to data loss.
- When a port on which a FOG is already configured is used as a destination port in configuring a SPAN, it leads to data loss.
- When the PTF card is not stable after restoring the database of 9.5.3 or upgrading to 9.5.3 or downgrading from 9.5.3 to earlier releases, Power-cycle the PTF card.
- Y1731 cannot be configured with the service ID that is used for VPLS or MPLS-TP tunnel. If configured, it causes data loss during an upgrade.
- When the following steps are performed, it causes data loss:
  - Create a channel group using different ports.
  - Configure the ingress policy on one of the member ports.
  - Reset the card.
- When the Sat-Comm False alarm observed after the upgrade:
  - Shut the FOG port.
  - Run the no shut command.

- **Upgrading from release 9.3.0.2 to 9.5.0 or 9.5.1**

  If the cumulative bandwidth of all existing services created over an MPLS-TP link exceeds the maximum threshold (10 Gpbs) defined for that link after an upgrade, it causes data loss.

- **Upgrading from release 9.3.0.2 to 9.5.0 or 9.5.1 and 9.5.0 to 9.5.1**

  MPLS-TP and LDP configurations cannot be enabled at the same time on a port. If enabled, it causes data loss during an upgrade due to invalid port configurations. MPLS-TP and LDP can be configured on the same port sequentially.

- **Upgrading from release 9.3.0.2 or 9.5.0 to 9.5.1**
  - When an unprotected MSTP-TP tunnel with one working LSP is created in a lockout state during an upgrade, it causes data loss. It is recommended to clear the lockout state before upgrading the node to release 9.5.1. Otherwise, all the configurations will be lost.
  - MPLS-TP link and REP configurations cannot be enabled at the same time on a port. If enabled, it causes data loss during an upgrade due to invalid port configurations

- **Upgrading from release 9.3.0.2 or 9.5.x to 9.5.x**

  When an Ethernet Virtual Circuit (EVC) is configured using the same Attachment Circuit (AC) where a pseudowire is already configured, it causes data loss.

- **Upgrading from release 9.5.0 or 9.5.1 to 9.5.1.1**

  When you create new endpoints EFPs/PWs or add existing EFPs/PWs to a VPLS circuit, CTC allows you to add only until 127 entries; EFPs or neighbor nodes. If the cumulative sum of entries made in both the **Endpoint PW** tab and **Endpoint EFP** tab exceeds 127, it leads to data loss.

- **Upgrading from release 9.5.1 to 9.5.1.1**

  If a pseudowire class (associated to a VPLS) is provisioned with the following values when a pseudowire class is created, it causes data loss:

  - Interworking value set to VLAN or Ethernet
  - Protocol value set to None

- **Upgrading from release 9.5.1 to 9.5.2**

  When you upgrade a fully loaded CPT 600 chassis, it causes data loss.

Cisco CPT Software Packages

To upgrade to a new release, download the required system software package by selecting the corresponding release from the following URL:

CPT Software Download

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 Cisco CPT 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-J107 Preparing to Upgrade to a New Release, on page 6—This procedure contains critical information and tasks that you must read and complete before beginning the upgrade process.

2 NTP-J108 Back Up the Cisco CPT Software Database, on page 10—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-J109 Upgrade the Cisco CPT Software, on page 11—Complete this procedure to complete the upgrade.

4 NTP-J113 Install Public-Key Security Certificate, on page 17— Complete this procedure to be able to run the Cisco CPT Software.

5 NTP-J110 Restore the Previous Software Load and Database, on page 18— Complete this procedure if you want to return to the previous software load you were running before activating the new release.

6 NTP-J112 Upgrade to the Cisco CPT Software Using TL1, on page 23— Complete this procedure only if you want to upgrade to a new release using Transaction Language (TL1).

NTP-J107 Preparing to Upgrade to a New Release

Purpose	This procedure provides critical information checks and tasks you must complete before beginning an upgrade to a future release.
Tools/Equipment	CPT nodes
Prerequisite Procedures	NTP-J22 Log into CTC
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser

Note During the software upgrade, the Cisco CPT 600 with active and standby fabric card configuration switches between the fabric cards. The switch-over time is approximately 50 milliseconds or less.

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/en/US/products/ps11348/prod_release_notes_list.html to download the release notes.

Step 3 Complete the task, DLP-J341 Verify CTC Workstation Requirements, on page 7.

Step 4 Complete the task, DLP-J342 Verify Common Control Cards, on page 9.

Step 5 When you have completed the tasks for this section, proceed with the procedure, NTP-J108 Back Up the Cisco CPT Software Database, on page 10.

Stop. You have completed this procedure.

DLP-J341 Verify CTC Workstation Requirements

Purpose	This task lists PC or UNIX workstation hardware and software requirements. Perform this task before upgrading the workstation to run the software.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser

Procedure

Step 1 Ensure that your workstation meets the following requirements:

Area	Requirements	Notes
Processor (PC only)	Pentium IV or a faster processor UltraSPARC-III or faster processor for UNIX workstation	—
RAM	1 GB RAM or more	—

Area	Requirements	Notes
Hard drive	20 GB hard disk with 250 MB of available hard drive space	—
Operating System	Either of the following: • Windows: ◦ Windows 2000 Professional ◦ Windows Server 2003 ◦ Windows Server 2008 ◦ Windows XP Professional ◦ Windows Vista ◦ Windows 7 • UNIX workstation ◦ Solaris Version 9 ◦ Solaris Version 10 • Apple Mac OS X	**Note** Use the latest patch or service pack released by the OS vendor. Check with the vendor for the latest patch or service pack. **Note** • For a UNIX workstation, use UltraSPARC-III or faster processor, with a minimum of 1 GB RAM and a minimum of 250 MB of available hard drive space.
Java Runtime Environment	JRE 1.6 Java Plug-in 1.6 Java Policy file	**Tip** You can check the JRE version in your browser window after entering the node IP address in the URL window under Java Version. **Note** For important information about CTC backward compatibility affected by your choice of JRE version, see the Readme.txt or Readme.html file on the software CD. **Note** To install JRE 1.6, the Java Policy file, or the online help, see the installation instructions in the *Cisco CPT Configuration Guide–CTC and Documentation Release 9.5.x and Cisco IOS Release 15.2(01)SA*.

Area	Requirements	Notes
Web browser	Either of the following: • Windows ◦ Internet Explorer 6.x ◦ Internet Explorer 7.x ◦ Internet Explorer 8.x • UNIX Workstation ◦ Mozilla 1.7 • Apple Mac OS X ◦ Safari	—

Step 2 Return to your originating procedure (NTP).

DLP-J342 Verify Common Control Cards

Purpose	This task lists card-slot requirements of common control cards in a node.
Tools/Equipment	PC or UNIX workstation with CTC installed
Prerequisite Procedures	Install the TNC, TNCE, TSC, and TSCE control cards.
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser

Procedure

Step 1 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 in the following section:

- CPT 600 shelf—TNC, TNCE, TSC, or TSCE cards in Slots 1 and 8
- CPT 200 shelf —TNC, TNCE, TSC, or TSCE card is in Slot 1

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

Step 3 Return to your originating procedure (NTP).

NTP-J108 Back Up the Cisco CPT Software Database

Purpose	This procedure retains all configuration data for your network before performing the upgrade.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	• NTP-J22 Log into CTC • NTP-J107 Preparing to Upgrade to a New Release, on page 6
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser

Note After configuring a CPT service, it is recommended to wait for at least two minutes before taking a backup of the database. Otherwise, the last configuration data does not get saved in the database and hence, cannot be restored.

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 in the File Name field and click **OK**. To overwrite an existing file, click **Yes**.

Step 4 Click the **Save** button to save the database on the local machine or a network storage device.

Step 5 When the backup is complete, click **OK.**

Step 6 Repeat Steps 1 through 5 for each node in the network.

Step 7 (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	
GCC[14] 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 TNC/TNCE/TSC/TSCE (Cisco CPT 600) cards	Slot 1 and Slot 8
Active TNC/TNCE/TSC/TSCE (Cisco CPT 200) cards	Slot 1
Network information—A print screen of the Provisioning tab in the network view	
List alarms—A print screen of the Alarm window	
List circuits—A print screen of the Circuit window	

14 GCC=Generic communications channel

Stop. You have completed this procedure.

NTP-J109 Upgrade the Cisco CPT Software

Purpose	This procedure upgrades the CTC software to a future release and must be performed on all nodes, or groups of nodes to be upgraded.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-J108 Back Up the Cisco CPT Software Database, on page 10
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 ISSU allows you to perform a software upgrade while the system continues to forward packets. For more information on ISSU, see the ISSU section in the *Cisco CPT Configuration Guide*.

Procedure

Step 1 Insert the Cisco CPT 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-J343 Download the Cisco CPT Software, on page 12 task for all nodes to be upgraded.

Step 3 Complete the DLP-J344 Activate the New Cisco CPT Software, on page 14 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-J345 Delete Cached JAR Files, on page 16 task, as necessary.
Caution If the Cisco CPT software is downloaded again after a version is activated, a revert to the previous version cannot be performed.

Step 5 (Optional) If you wish to ensure that a software revert to the previous software release is no longer possible, complete the DLP-J343 Download the Cisco CPT Software, on page 12 task or all nodes, or groups of nodes you are upgrading a second time.

Step 6 If you need to return to the software and database you had before activating the latest software release, proceed with the NTP-J110 Restore the Previous Software Load and Database, on page 18 procedure.

Step 7 To back up the latest software release database for the working software load, see NTP-J108 Back Up the Cisco CPT Software Database, on page 10 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.

DLP-J343 Download the Cisco CPT Software

Purpose	This task downloads Cisco CPT software to the CPT nodes prior to activation.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-J108 Back Up the Cisco CPT Software Database, on page 10
Required/As Needed	Required

Onsite/Remote	Onsite or remote
Security Level	Maintenance user or higher

Note The TNC/TNCE/TSC/TSCE card contains flash memory with two partitions—working and protect (backup). An upgrade downloads the software to the protect (backup) partition of the flash memory on both the standby and active TNC/TNCE/TSC/TSCE 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 NTP-J109 Upgrade the Cisco CPT Software, on page 11 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 SWFTDWN alarm is raised on the standby and active TNC/TNCE/TSC/TSCE cards during software download. The alarms clear 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 CPT software CD or on your hard drive.

Step 8 To open the Cisco CPT software 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 generic communications channel (GCC) 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-J344 Activate the New Cisco CPT Software

Purpose	This task activates the software on each node in the network.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	DLP-J343 Download the Cisco CPT Software, on page 12
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 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 the latest software version.

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

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

Step 10 After activating the node, the software upgrade reboot occurs as follows:

- All the common control cards (TNC/TNCE/TSC/TSCE) in the node reboot beginning with the standby card. As soon as the standby card reboots, it signals the active card to reset as a standby card and the standby card transitions to active.
- The SYSBOOT alarm is raised as soon as the common control cards reset. This alarm 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.

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

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

Step 12 In the browser window, click **Delete CTC Cache**.

Note Make sure that CTC is closed before clicking the **Delete CTC Cache** button.

Note It might also be necessary to delete cached files from your browser's directory, or from the MS Windows workstation in C:\Documents and Settings*username*\Application Data\Cisco\CTC. If you have trouble reconnecting to CTC, complete the DLP-J345 Delete Cached JAR Files, on page 16 task.

Step 13 Close your browser and then reopen it.

Step 14 (Optional) Run the Cache Loader pre-caching utility. This logs you into CTC at a faster pace after an upgrade.

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 15 Enter the IP address recorded in step 2. The new CTC applet loads. During this login, type the user name followed by the password.

Note Complete Steps 11 through 15 only after upgrading the first node in a network. This is because cached files must be removed from your workstation only once. For the remaining nodes, you will still be disconnected and moved to the network view during the node reboot. After the reboot is complete, CTC restores connectivity to the node.

Step 16 Return to your originating procedure (NTP).

DLP-J345 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 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-J346 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-J113 Install Public-Key Security Certificate

Purpose	This procedure installs the ITU Recommendation X.509 public-key security certificate.
Tools/Equipment	None
Prerequisite Procedures	This procedure is performed when logging into CTC. You cannot perform it at any other time.
Required/As Needed	Required.
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 Cisco CPT Software.
- Deny—Denies permission to install the certificate. If this option is chosen, login into the Cisco CPT Software 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 latest software version, proceed with the NTP-J110 Restore the Previous Software Load and Database, on page 18 procedure.
Stop. You have completed this procedure.

NTP-J110 Restore the Previous Software Load and Database

Purpose	This procedure returns to the software and database provisioning that was present before the latest release 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 the latest release.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-J22 Log into CTC NTP-J107 Preparing to Upgrade to a New Release, on page 6 NTP-J108 Back Up the Cisco CPT Software Database, on page 10 NTP-J109 Upgrade the Cisco CPT Software, on page 11
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.

Note The defaults database files (db files) used to restore the basic configuration on a single node are shipped along with the standard software release package.

Procedure

Step 1 Complete the DLP-J347 Revert to Protect Load, on page 19 task.

Step 2 If the software revert to your previous release failed to restore the database, complete the DLP-J348 Manually Restore the Database, on page 20 task.

Stop. You have completed this procedure.

DLP-J347 Revert to Protect Load

Purpose	This task reverts to the software you were running prior to the last activation. 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 the latest release.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-J107 Preparing to Upgrade to a New Release, on page 6 NTP-J108 Back Up the Cisco CPT Software Database, on page 10 NTP-J109 Upgrade the Cisco CPT Software, on page 11
Required/As Needed	Required for revert
Onsite/Remote	Onsite or remote
Security Level	Superuser

Note 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 the latest release.

Note To perform a supported revert from the latest release, 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.

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 dialog box asks you to confirm the choice.

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-J345 Delete Cached JAR Files, on page 16 task.

Step 9 Return to your originating procedure (NTP).

DLP-J348 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-J347 Revert to Protect Load, on page 19
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 Open dialog box appears.

Step 3 Select the previously saved database file and click the **Open** button.
The database is restored and the TNC/TNCE/TSC/TSCE cards reboot.

Step 4 When the TNC/TNCE/TSC/TSCE cards have finished rebooting, log into CTC and verify that the database is restored.
Wait one minute before restoring the next node.

Step 5 Repeat Steps 1 to 4 for each node in the network.
You have now completed the manual database restore.

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-J108 Back Up the Cisco CPT Software Database, on page 10 procedure for more information.

Step 6 Return to your originating procedure (NTP).

NTP-J111 Upgrade the TSC Card to the TNC Card

Purpose	This procedure upgrades the TSC card to the TNC card on the CPT node.
Tools/Equipment	Two TNC cards
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Maintenance or higher

Note Downgrade procedures from TNC or TNCE cards to TSC or TSCE cards are not supported. Contact Cisco TAC for more information.

This procedure is also applicable to the below mentioned card upgrades. Replace the source and the destination cards and repeat the same procedure to upgrade from:

- TSC to TNCE
- TSCE to TNCE
- TNC to TNCE
- TSC to TSCE

Procedure

Step 1 Complete the "NTP-J22 Log into CTC" task. For more information, see the *Cisco CPT Configuration Guide–CTC and Documentation Release 9.5.x and Cisco IOS Release 15.2(01)SA*.

Step 2 Verify that the LAN wires on the RJ-45 LAN port are installed properly. The TNC card does not autodetect miswired LAN connections. If a LAN connection is miswired, a LAN Connection Polarity Reversed condition appears.

Step 3 Verify that the node you are upgrading has latest version of the Cisco CPT Software installed. The software version is displayed in the upper left corner of the window.

Step 4 Complete the NTP-J108 Back Up the Cisco CPT Software Database, on page 10 procedure before beginning the upgrade.

Step 5 Physically replace the standby TSC card with a TNC card.

a) Check the LED on the faceplate. The ACT/STBY LED on the faceplate of the TNC/TSC card indicates whether the card is in active or standby mode. A green ACT/STBY LED indicates an active card and an amber light indicates a standby card.
b) Open the ejectors on the standby TSC card.
c) Slide the card out of the slot. This raises the IMPROPRMVL alarm, which clears when the upgrade is complete.
d) Right-click the slot from which the TSC card was ejected out.
e) Click **Delete Card** to delete TSC from CTC.

Note If the TSC card is not deleted from the CTC shelf view before inserting the TNC card, the MEA (card mismatch) alarm appears on that slot.

f) Open the ejectors on the TNC card to be installed.
g) Slide the TNC card into the slot along the guide rails.
h) Close the ejectors.
i) In CTC node view, Ldg (loading) appears on the newly installed TNC card.

Note It takes approximately 10 minutes for the active TSC card to copy the system software and database to the newly installed TNC card. During this operation, the LEDs on the TNC card flash Fail and then the active/standby LED flashes. When the transfer completes, the TNC card reboots and goes into standby mode after approximately three minutes. Do not remove the card from the shelf during a database transfer.

Caution If your active TSC card resets during the upgrade before the new TNC card is in full standby mode, remove the new TNC card immediately.

Step 6 When the newly installed TNC card is in standby, right-click the active TSC card in CTC.

Step 7 From the pull-down menu, click **Reset Card**.
Wait for the TSC card to reboot. The standby TNC card is switched to active mode. The TSC card verifies that it has the same database as the TNC card and then switches to standby.

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

Step 9 Physically replace the remaining TSC card with the second TNC card.

a) Open the ejectors on the TSC card.
b) Slide the card out of the slot. This raises the IMPROPRMVL alarm, which clears when the upgrade is complete.
c) Right-click the slot from which the TSC card was ejected out.
d) Click **Delete Card** to delete TSC from CTC.
If the TSC card is not deleted from the CTC shelf view before inserting the TNC card, the MEA (card mismatch) alarm appears on that slot.
e) Open the ejectors on the TNC card.
f) Slide the TNC card into the slot along the guide rails.
g) Close the ejectors.

The second TNC card boots up. The second TNC card must also copy the database. Do not remove the card from the shelf during a database transfer.

Step 10 If power-related alarms occur after the second TNC card is installed, check the voltage on the RJ-45 LAN port. Refer to the *Cisco CPT Configuration Guide–CTC and Documentation Release 9.5.x and Cisco IOS Release 15.2(01)SA* for information on clearing the alarms.
Stop. You have completed this procedure.

NTP-J112 Upgrade to the Cisco CPT Software Using TL1

Purpose	This procedure upgrades the Cisco CPT Software to the latest software release to using TL1 rather than CTC.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-J107 Preparing to Upgrade to a New Release, on page 6 NTP-J108 Back Up the Cisco CPT Software Database, on page 10
Required/As Needed	Optional
Onsite/Remote	Onsite or remote
Security Level	Superuser

Note To ensure that your syntax for each command is correct, see the TL1 syntax in the Command Guide for your particular release when issuing the following commands:

- ACT-USER
- COPY-RFILE
- REPT EVT FXFR
- APPLY
- RTRV-COND-ALL
- RTRV-ALM-ALL

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 CPT-0950-012A-1115.pkg

The GNE and ENE commands are as follows:

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

```
COPY-RFILE:NODENAME:RFILE-PKG:CTAG::TYPE=SWDL,
SRC="ftp://FTPUSER1:FTPUSERPASSWORD1@10.1.1.1/CPT-0950-012A-1115.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/CPT-0950-012A-1115.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/CPT-0950-012A-1115.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 CPT 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;`

  ACT-USER is the activation command, 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 Select the IP address for the node, using port 3083 or 2361.

Step 6 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 7 Repeat Step 6 for all nodes to be upgraded.

Step 8 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 9 Complete "NTP-J107 Preparing to Upgrade to a New Release, on page 6" procedure for each node to be upgraded.

Step 10 Complete NTP-J108 Back Up the Cisco CPT Software Database, on page 10 for each node to be upgraded.

Step 11 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 12 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 CANC to cancel the activation.

If the command is successful, the appropriate flash is selected and the TNC/TNCE/TSC/TSCE card reboots.

The following occurs:

- Each card in the node reboots, beginning with the standby TNC/TNCE/TSC/TSCE card. When the standby TNC/TNCE/TSC/TSCE card reboots, it signals to the active TNC/TNCE/TSC/TSCE card that it is ready to take over. When the active TNC/TNCE/TSC/TSCE receives this signal, it resets itself, and the standby TNC/TNCE/TSC/TSCE takes over and transitions to active. The pre-upgrade version of the TNC/TNCE/TSC/TSCE card is now the standby TNC/TNCE/TSC/TSCE.
- A system reboot (SYSBOOT) alarm is raised while activation is in progress (following the TNC/TNCE/TSC/TSCE card resets). When all cards have reset, this alarm clears. The complete activation process can take up to 30 minutes, depending on how many cards are installed.

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

Step 13 Perform Step 14 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 14 After all nodes have been activated, log in using CTC or Telnet and verify there are no outstanding alarms.

Step 15 To back up the database for the working software load, see NTP-J108 Back Up the Cisco CPT Software Database, on page 10 in order to preserve the database for the current software.

Stop. You have completed this procedure.

Related Documentation

Use the Cisco CPT Upgrade Guide, Release 9.5.x in conjunction with the following referenced Release 9.5.x publication:

- Cisco CPT Hardware Installation Guide

- Cisco CPT Configuration Guide-CTC and Documentation Release 9.5.x and Cisco IOS Release 15.2(01)
- Cisco CPT Command Reference Guide-CTC and Documentation Release 9.5.x and Cisco IOS Release 15.2(01)
- Release Notes for Cisco CPT–CTC and Documentation Release 9.5.x and Cisco IOS Release 15.2(01)SB
- Cisco CPT Licensing Configuration Guide

Additional References

The following link provides additional information on CPT:

- http://www.cisco.com/go/cpt

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 an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS version 2.0.