Understanding the Carrier Packet Transport System

This chapter describes the Cisco Carrier Packet Transport system. This chapter includes the following topics:

Carrier Packet Transport System

Packet-based services dominate the overall network traffic and as a result service providers are required to migrate their existing transport networks from time-division multiplexing (TDM) networks to packet transport networks. Service providers need next-generation transport networks that can enable and support new mesh, multipoint, and multidirectional services. By deploying packet transport networks, service providers can benefit from statistical multiplexing, dynamic bandwidth allocation, and quality of service (QoS).

The Carrier Packet Transport (CPT) system is designed to help service providers transition from TDM networks to packet transport networks smoothly and efficiently. The CPT System is an integrated packet transport platform that enables service providers to deploy new packet transport networks.

The CPT System is the first Packet–Optical Transport System (P–OTS) built on standards-based Multiprotocol Label Switching–Transport Profile (MPLS–TP) technology. The CPT System unifies both packet and transport technologies, giving service providers a strong foundation for next-generation transport. The CPT System is designed to support transport applications so that service providers can continue to offer existing transport services while enabling new packet services.

The CPT System is a platform that provides architectural flexibility with support for MPLS–TP, IP/MPLS, and Carrier Ethernet transport. This provides service providers data plane and control plane flexibility in network deployments. The CPT platform enables service providers to provide mobile back-haul, Ethernet services, and TDM services for residential and business customers.

The CPT System integrates DWDM, Optical Transport Network (OTN), Ethernet, and standards-based MPLS-TP in a single system. The CPT System also integrates with other Cisco platforms such as the ONS 15454, Cisco ASR 9000 Series Router, and Carrier Routing System to deliver a combined IP/MPLS and MPLS–TP solution under a single control plane, forwarding mechanism, and Network Management System (NMS). This solution enables service providers to deploy this solution and interoperate with existing deployed IP/MPLS networks.

The CPT System works in the metro edge and access portion of the network providing an integrated packet and transport solution. The CPT System results in significant reduction in rack space and power consumption.

The CPT System offers:

- A unique architecture with remotely managed CPT 50 panels.
- High Gigabit Ethernet and 10 Gigabit Ethernet port density per rack unit.
- Integrated A-to-Z management for packet and transport.

Understanding CPT Cards

The CPT System is supported on the CPT 200 and CPT 600 chassis. The CPT 200 chassis consists of two service slots and has a 160 GB switch capacity. The CPT 600 chassis comes with six service slots and has a 480 GB switch capacity. For more information on CPT 200 and CPT 600 shelves, see the *Cisco CPT Hardware Installation Guide*.

There are two cards in the CPT System:

- Fabric card
- Line card

The CPT 50 panel is a stand-alone unit and can be connected to the CPT System. The CPT 50 panel enables you to scale the number of ports on the CPT System.

Fabric Card

The fabric card is a single slot card with two 10 Gigabit Ethernet SFP+ ports and two 10 Gigabit Ethernet XFP ports. The XFP ports on the fabric card support the OTN protocol. The fabric card provides high availability and high switching capacity. The 10GE XFPs of the fabric card removes the need to deploy additional transponders for DWDM applications. It also supports telnet connection.

Line Card

The line card has four 10 Gigabit Ethernet SFP+ ports. The line card expands the I/O capacity of CPT 200 and CPT 600 chassis by interconnecting with other line and fabric cards. It offers carrier class reliability, network flexibility, network ease of provisioning, and industrial grade Operations, Administration, and Maintenance (OAM).

CPT 50 Panel

The CPT 50 panel has four 10 Gigabit Ethernet SFP+ ports and 44 Gigabit Ethernet SFP ports. The four 10 Gigabit Ethernet SFP+ ports can be used to connect with the fabric and line cards.

The CPT 50 panel can be combined with CPT 200 or CPT 600 to create a platform that behaves as a single integrated system. The CPT 50 panel can be deployed locally with the CPT 200 or CPT 600 or remotely up to 40 km away from the main chassis. In either case, the CPT 50 panel is managed as part of the same node, effectively as a virtual line card.

For more information on the CPT cards and CPT 50 panel, see the Hardware chapter.

CPT Software Features

The software features supported by the CPT System are shown in Table 1: CPT Software Features, on page 3.

Table 1: CPT Software Features

Feature	See
Ethernet Virtual Circuit (EVC)	Configuring Ethernet Virtual Circuit
Multiprotocol Label Switching (MPLS)	Configuring Multiprotocol Label Switching
Multiprotocol Label Switching – Transport Profile (MPLS–TP)	Configuring MPLS–Transport Profile
Pseudowire	Configuring Pseudowire
Quality of service (QoS)	Configuring Quality of Service
Resilient Ethernet Protocol (REP)	Configuring Resilient Ethernet Protocol
Link Aggregation Group (LAG)	Configuring Link Aggregation Group and Link Aggregation Control Protocol
MAC Learning	Configuring MAC Learning
Multicast VLAN Registration (MVR)	Configuring Multicast VLAN Registration
IGMP Snooping	Configuring IGMP Snooping

CPT Packet Profile Package

The CPT package is a single packet profile package that supports both SONET and SDH nodes. The terminology used in CPT package is similar to the terminology used in SONET.

The SONET and SDH nodes can be added to the CPT network through CTC. When the nodes are added to the CPT network, the respective configurations (SONET or SDH) are supported by the CTC session. The

CPT nodes can be added to the CPT network even when there are non CPT nodes in the network. However, you cannot add both the SONET and SDH nodes to the same CTC session.

Configuration Rules

When both CPT and non CPT nodes are present in a shelf, the following configuration rules apply:

- Add SDH nodes of various types such as 15454SDH-DWDM LITE, 15454SDH-DWDM, 15454SDH-M6, and 15454SDH-M2 to CPT CTC. The terminology of the CPT nodes changes to the terminology of the SDH node. The change in terminology is specific only to the CTC session.
- Add SONET nodes of various types such as 15454-DWDM LITE, 15454-DWDM, 15454-M6, and 15454-M2 to CPT CTC. The terminology of the CPT nodes changes to the terminology of the SONET node. The change in terminology is specific only to the CTC session.
- The creation of Optical Channel Trail and Provisionable Patchcords is allowed between CPT and non CPT nodes.
- The non CPT nodes are not listed while creating L2+ services between CPT nodes.
- The nodes that belong to a different release and multishelf nodes are allowed in the same CTC session.
- The TL1 sessions for CPT nodes use SONET terminology.
- CPT supports FE/GE OSC provisioning; However, CPT does not support OC3 OSC provisioning.
- In the Edit -> Preferences -> Managed Network tab of CTC, the following options are listed:
    - ANSI and Packet (default option)
    - ETSI and Packet

  When you add the SDH nodes to the CPT network, the option changes automatically to ETSI and Packet. When you close the CTC session and start a new session, the option does not change back to ANSI and Packet. Hence, you need to manually change the option by editing the network preferences.

Supported Loopbacks

The following loopbacks are supported in CPT.

- Facility loopback at the interface level
- Terminal loopback at the interface level
- Ethernet OAM loopback
- Connectivity Fault Management ping

Understanding CPT Configuration Modes

You can configure the CPT System features either through Cisco Transport Controller (CTC) or Cisco Internetwork Operating System (IOS) commands.

CTC

CTC is a Java application that is installed in two locations—it is stored on the Transport Node Controller (TNC) or Transport Shelf Controller (TSC) card and it is downloaded to your workstation the first time you log into the CPT System with a new software release.

Cisco IOS

Cisco IOS is the software used on the majority of Cisco systems routers and network switches. Cisco IOS is a package of routing, switching, internetworking, and telecommunications functions tightly integrated with a multitasking operating system.

The Cisco IOS is designed as a modal operating system. The term modal describes a system where there are different modes of operation, each having its own domain of operation. The CLI command mode structure is hierarchical, and each mode supports a set of specific commands.

The following table lists the common command modes with associated CLI prompts, access and exit methods, and a brief description of how each mode is used.

Table 2: IOS CLI Command Modes

Command Mode	Access Method	Prompt	Exit Method	Mode Usage
User EXEC	Log in.	`Router>`	Issue the **logout** or **exit** command.	• Change terminal settings. • Perform basic tests. • Display device status.
Privileged EXEC	From user EXEC mode, issue the **enable** command.	`Router#`	Issue the **disable** command or the **exit** command to return to user EXEC mode.	• Issue **show** and **debug** commands. • Copy images to the device. • Reload the device. • Manage device configuration files. • Manage device file systems.

Command Mode	Access Method	Prompt	Exit Method	Mode Usage
Global configuration	From privileged EXEC mode, issue the **configure terminal** command.	`Router(config)#`	Issue the **exit** command or the **end** command to return to privileged EXEC mode.	Configure the device.
Interface configuration	From global configuration mode, issue the **interface** command.	`Router(config-if)#`	Issue the **exit** command to return to global configuration mode or the **end** command to return to privileged EXEC mode.	Configure individual interfaces.

Note Even in IOS mode, the following configurations can be performed only through CTC:

- Creating a Fan–Out–Group (FOG)
- Provisioning Pluggable Port Modules (PPM) and port
- Viewing performance monitoring parameters
- Configuring and monitoring Optical Transport Network (OTN) settings
- Modifying Ethernet settings and alarm thresholds
- Viewing Alarms
- Creating a provisionable patchcord
- Performing In-Service Software Upgrade (ISSU)

NTP-J20 Change the CPT System Configuration Mode Using CTC

Purpose	This procedure changes the CPT System configuration mode to CTC or Cisco IOS mode.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed

Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note The fabric/line/CPT 50 card reboots when you change the configuration mode from CTC to Cisco IOS mode or vice versa.

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 13 procedure at a node where you want to change the CPT System configuration mode.

Step 2 From the View menu, choose **Go to Home View**.

Step 3 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 4 Click the **Configuration Mode** tab.

Step 5 To change the CPT System configuration mode from CTC to Cisco IOS:

a) Click **IOS Mode**.
b) Click **Apply**. The Apply Provisioning Mode Change dialog box appears.
c) Click **Yes** in the dialog box to retain the configuration changes that were performed through CTC.
d) Click **No** in the dialog box to start the Cisco IOS mode with the default configuration.
The Provisioning tab, Maintenance (OAM) tab, and Service Level Alarm tab in CTC are disabled when you change the CPT System configuration mode from CTC to Cisco IOS.

Step 6 To change the CPT System configuration mode from Cisco IOS to CTC:

a) Click **CTC Mode**.
b) Click **Apply**. The Apply Provisioning Mode Change dialog box appears.
c) Click **Yes** in the dialog box to change the configuration mode to CTC.
Note The configuration changes performed through Cisco IOS are lost when you change the configuration mode from Cisco IOS to CTC.

Step 7 To open the Cisco IOS configuration mode using CTC, see DLP-J56 Open the Cisco IOS Configuration Mode and View the Feature Configuration Details Using CTC, on page 7.
Stop. You have completed this procedure.

DLP-J56 Open the Cisco IOS Configuration Mode and View the Feature Configuration Details Using CTC

Purpose	This procedure opens the Cisco IOS configuration mode and views the feature configuration details using CTC.

Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 13 procedure at a node where you want to open the Cisco IOS configuration mode and view the feature configuration details.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Maintenance** tab.

Step 4 From the left pane, click **IOS**.

Step 5 Click **Open IOS Connection**. The IOS Login dialog box appears.

Step 6 Enter the user name and password.

Step 7 Enter any show command.

Note You can use show commands in CTC and Cisco IOS to display the configuration status. When the **show** command with **more** option is simultaneously used in Cisco IOS and CTC, the system crashes.

Step 8 Press **Enter**. The output is displayed.

Step 9 Return to your originating procedure (NTP).

NTP-J21 Set Up the Computer for CTC

Purpose	This procedure configures your Windows PC or Solaris workstation to run CTC.
Tools/Equipment	CPT System software CD
Prerequisite Procedures	Install the CPT 200 and CPT 600 shelf.
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	None

Procedure

Complete one of the following procedures:

- If your computer is a Windows PC, complete the DLP-J57 Run the CTC Installation Wizard for Windows PCs, on page 9 procedure.
- If your computer is a Solaris workstation, complete the DLP-J58 Run the CTC Installation Wizard for Solaris Workstations, on page 11 procedure.

Stop. You have completed this procedure.

DLP-J57 Run the CTC Installation Wizard for Windows PCs

Purpose	This procedure configures your Windows PC or Solaris workstation to run CTC.
Tools/Equipment	CPT System software CD
Prerequisite Procedures	None
Required/As Needed	This procedure is required if you use a Windows computer to run CTC and if any one of the following is true: • JRE 1.6 is not installed. • CTC online user manuals are not installed and are needed. • CTC JAR files are not installed and are needed.
Onsite/Remote	Onsite or remote
Security Level	None

Procedure

Step 1 Insert the CPT System software CD into your computer CD drive. The installation program begins running automatically. If it does not start, navigate to the CD directory and double-click **setup.exe**.
The Cisco Transport Controller Installation Wizard displays the components that will be installed on your computer:

- JRE 1.6
- Acrobat Reader 8.1.2
- Online User Manuals
- CTC JAR files

Step 2 Click **Next**.

Step 3 Complete one of the following:

- Click **Typical** to install the JRE, CTC JAR files, online user manuals, and Acrobat Reader. If you already have JRE 1.6 installed on your computer, choose **Custom**.
- Click **Custom** if you want to choose the components that you want to install. By default, Acrobat Reader and the online user manuals are selected. Check the CTC components that you want to install and click **Next**.

Step 4 Click **Next**.
The directory where the installation wizard will install the CTC online user manuals appears. The default is C:\Program Files\Cisco\CTC\Documentation.

Step 5 Click **Next**.

Step 6 Review the components that will be installed and click **Next**. It might take a few minutes for the JRE installation wizard to appear.

Step 7 To install the JRE, complete the following:

a) In the Java 2 Runtime Environment License Agreement dialog box, view the license agreement and accept the terms of the license agreement.
b) Click **Next**.
c) Choose one of the following:

   - Click **Typical** to install all JRE features. If you select Typical, the JRE version installed will automatically become the default JRE version for your browsers.
   - Click **Custom** if you want to select the components to install and select the browsers that will use the JRE version.

d) Click **Next**.
e) If you selected Typical, continue with 7.i, on page 11. If you selected Custom, click the drop-down list for each program feature that you want to install and choose the desired setting. The program features include:

   - Java 2 Runtime Environment—(Default) Installs JRE 1.6 with support for European languages.
   - Support for Additional Languages—Adds support for non-European languages.
   - Additional Font and Media Support—Adds Lucida fonts, Java Sound, and color management capabilities.

f) Click **Next**.
g) In the Browser Registration dialog box, check the browsers that you want to register with the Java Plug-In. The JRE version will be the default for the selected browsers. It is acceptable to leave both browser check boxes unchecked.
   Note Setting the JRE as the default for these browsers might cause problems with these browsers.
h) Click **Next**.

i) Click **Finish**.

Step 8 In the Cisco Transport Controller Installation Wizard, click **Next**. The online user manuals and Adobe Acrobat Reader are installed.

Step 9 Click **Finish**.

Step 10 Return to your originating procedure (NTP).

DLP-J58 Run the CTC Installation Wizard for Solaris Workstations

Purpose	This procedure installs the CTC online user manuals, Acrobat 8.1.2, and JRE 1.6 on Solaris workstations, as necessary.
Tools/Equipment	CPT System software CD
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Procedure

Step 1 Change the directory. Enter:
cd /cdrom/cdrom0/

Step 2 From the CD directory, enter:
./setup.bat
The Cisco Transport Controller Installation Wizard displays the components that are installed on your computer:

- JRE 1.6
- Acrobat Reader 8.1.2
- Online User Manuals
- CTC JAR files

Step 3 Click **Next**.

Step 4 Complete one of the following:

- Click **Typical** to install both the JRE and the online user manuals. If you already have JRE 1.6 installed on your computer, choose **Custom**.
- Click **Custom** if you want to install either the JRE or the online user manuals.

Step 5 Click **Next**.

Step 6 Complete the following, as applicable:

a) If you selected Typical, continue with the next step.
b) If you selected Custom, check the CTC component that you want to install and click **Next**.

Step 7 The directory where the installation wizard installs the CTC online user manuals appears. The default is /usr/doc/ctc. Click **Next**.

Step 8 Review the components that will be installed and click **Next**. It might take a few minutes for the JRE installation wizard to appear.

Step 9 To install the JRE, complete the following:

a) In the Java 2 Runtime Environment License Agreement dialog box, view the license agreement and accept the terms of the license agreement.
b) Click **Next**.
c) Choose one of the following:

   - Click **Typical** to install all JRE features. If you select Typical, the JRE version installed will automatically become the default JRE version for your browsers.
   - Click **Custom** if you want to select the components to install and select the browsers that will use the JRE version.

d) Click **Next**.
e) If you selected Typical, continue with 9.i, on page 12. If you selected Custom, click the drop-down list for each program feature that you want to install and choose the desired setting. The program features include:

   - Java 2 Runtime Environment—(Default) Installs JRE 1.6 with support for European languages.
   - Support for Additional Languages—Adds support for non-European languages.
   - Additional Font and Media Support—Adds Lucida fonts, Java Sound, and color management capabilities.

f) Click **Next**.
g) In the Browser Registration dialog box, check the browsers that you want to register with the Java Plug-In. The JRE version will be the default for the selected browsers. It is acceptable to leave both browser check boxes unchecked.

   Note Setting the JRE as the default for these browsers might cause problems with these browsers.

h) Click **Next**.
i) Click **Finish**.

Step 10 In the Cisco Transport Controller Installation Wizard, click **Next**. The online user manuals are installed.

Step 11 Click **Finish**.

Step 12 Return to your originating procedure (NTP).

NTP-J22 Log into CTC

Purpose	This procedure logs into the GUI of CTC.
Tools/Equipment	None
Prerequisite Procedures	NTP-J21 Set Up the Computer for CTC, on page 8
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Note JRE 1.6 is required to log into nodes running CPT system.

Procedure

Step 1 From the computer connected to the CPT 200 or CPT 600 shelves, start Windows Internet Explorer (Windows PC) or Mozilla Firefox (Solaris workstation):

- If you are using a Windows PC, launch Windows Internet Explorer from the Windows Start menu or a shortcut icon.
- If you are using a Solaris workstation, determine the directory where Mozilla Firefox is installed by typing **whereis mozilla**, navigate to that directory and type:

  # mozilla -install

Step 2 In Windows Internet Explorer or Mozilla Firefox web address (URL) field, enter the CPT 200 or CPT 600 IPv4 or IPv6 address. For initial setup, this is the default IP address, 192.1.0.2.

Note The IP address appears on the LCD. You can suppress the LCD IP address display using CTC after you log in.

Step 3 Press **Enter**. The browser displays a window with a Delete CTC Cache field and information about the Cisco Transport Controller Java and System environments.

Note

- To log into CTC using an IPv6 address, you must first log into CTC using an IPv4 address and assign an IPv6 address to the node. Then, use the IPv6 address that you assigned to the node to log into CTC.
- The Delete CTC Cache field deletes the CTC JAR (Java Archive) files that are downloaded to your computer when you log into CPT 200 or CPT 600. You perform this action if connectivity problems occur or you want to delete older CTC JAR file versions from your computer.
- If you are logging into CPT 200 or CPT 600 nodes in an operation network that are running different releases of CTC software, log into the node running the most recent release. If you log into a node running an older release, you will receive an INCOMPATIBLE–SW alarm for each node in the network running a new release, and CTC will not be able to manage these nodes. To check the software version of a node, select **About CTC** from the CTC Help menu. This will display the software version for each node visible on the network view. If the node is not visible, the software version can be read from the LCD display.

Step 4 If a Java Plug-in Security Warning dialog box appears, complete the DLP-J59 Install the Public-Key Security Certificate Using CTC, on page 15 procedure to install the public-key security certificate.
After you complete the security certificate dialog box (or if the certificate is already installed), a Java Console window displays the CTC file download status. The web browser displays information about your Java and system environments. If this is the first login, CTC caching messages appear while CTC files are downloaded to your computer. The first time you connect to CPT 200 or CPT 600, this process can take several minutes. After the download, a warning message window appears.

Step 5 Click **OK**. The CTC Login dialog box appears.

Step 6 In the CTC Login dialog box, type a user name and password (both are case sensitive).

Note

- For CPT 200 or CPT 600 shelves, the default user is CISCO15. CISCO15 has Superuser privileges, so you can create other users. You must create another Superuser before you can delete the CISCO15 user. CISCO15 is delivered with the otbu+1 password. To change the password for CISCO15, complete the DLP-J60 Change the User Password and Security Level on a Single Node Using CTC, on page 16 procedure after you log in to CTC.
- To access CPT 50 through console, the default user is CISCO15 and the default password is otbu+1. This password cannot be modified.

Step 7 Each time you log into CPT 200 or CPT 600, you can select the following login options:

- Additional Nodes — Displays a list of current login node groups.
- Disable Network Discovery — Check this box to view only the CPT 200 or CPT 600 (and additional nodes within the login node group, if any) entered in the Node Name field. Nodes linked to this node through DCCs are not discovered and will not appear in CTC network view. Using this option, you can decrease the CTC startup time in networks with many DCC–connected nodes, and can reduce memory consumption.
- Disable Circuit Management — Check this box to disable discovery of existing circuits. Using this option, you can decrease the CTC initialization time in networks with many existing circuits and reduce memory consumption. After you are logged in, you can enable circuit discovery at any time by choosing the Enable Circuit Discovery button on the Circuits tab.

Step 8 If you keep Disable Network Discovery unchecked, CTC attempts to upgrade the CTC software by downloading more recent versions of the JAR files it finds during the network discovery. Click **Yes** to allow CTC to download the newer JAR files, or **No** to prevent CTC from downloading the JAR files.

Note Upgrading the CTC software will overwrite your existing software. You must restart CTC after the upgrade is complete.

Step 9 Click **Login**.

If the login is successful, the CTC node view window appears. From here, you can navigate to other CTC views to provision and manage the CPT 200 or CPT 600 shelves.

Step 10 Perform the following procedures as needed:

- DLP-J60 Change the User Password and Security Level on a Single Node Using CTC, on page 16
- DLP-J59 Install the Public-Key Security Certificate Using CTC, on page 15

Stop. You have completed this procedure.

DLP-J59 Install the Public-Key Security Certificate Using CTC

Purpose	This procedure installs the ITU Recommendation X.509 public-key security certificate using CTC.
Tools/Equipment	None
Prerequisite Procedures	This procedure can be performed only during the NTP-J22 Log into CTC, on page 13 procedure.
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note JRE 1.6 is required to log into nodes running CPT System.

Procedure

Step 1 If the Java Plug-in Security Warning dialog box appears, choose one of the following options:

- Yes—Installs the public-key certificate to your PC only for the current session. After the session is ended, the certificate is deleted. This dialog box will appear the next time you log into CPT 200 or CPT 600.
- No—Denies permission to install the certificate. If you choose this option, you cannot log into CPT 200.
- Always—Installs the public-key certificate and does not delete it after the session is over. It is recommended to use this option.
- More Details—Allows you to view the public-key security certificate.

Step 2 Return to your originating procedure (NTP).

DLP-J60 Change the User Password and Security Level on a Single Node Using CTC

Purpose	This procedure changes the settings for an existing user at one node using CTC.
Tools/Equipment	None
Prerequisite Procedures	NTP-J22 Log into CTC, on page 13
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note Each CPT 200 or CPT 600 must have only one user with a Superuser security level. The default CISCO15 user name and security level cannot be changed unless you create another user with Superuser security.

Procedure

Step 1 In node view (single-shelf mode) or multi shelf view (multi shelf mode), click the **Provisioning** > **Security** > **Users** tabs.

Step 2 Click the user whose settings you want to modify, then click **Edit**.

Step 3 In the Change User dialog box:

- Change a user password.
- Modify the user security level.
- Lock out the user.
- Disable the user.
- Force the user to change password on next login.

Step 4 Click **OK**.

Step 5 Click **OK** in the confirmation dialog box.

Note The user settings that you changed during this procedure do not appear until that user logs out and logs back in.

Step 6 Return to your originating procedure (NTP).

DLP-J380 Create User Using CTC

Purpose	This procedure allows you to create a new user using CTC.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Procedure

Step 1 In node view (single-shelf mode) or multi shelf view (multi shelf mode), click the **Provisioning** > **Security** > **Users** tabs.

Step 2 Enter the name of the user in the Name field.

Step 3 Enter the password in the Password field.

Step 4 Reenter the password in the Confirm Password field.

Step 5 From the Security-Level drop down list, choose security level.

Step 6 Click **OK** to save the user.

Step 7 Return to your originating procedure (NTP).

DLP-J381 Delete User Using CTC

Purpose	This procedure allows you to delete an existing user using CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-J380 Create User Using CTC, on page 17
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Procedure

Step 1 In node view (single-shelf mode) or multi shelf view (multi shelf mode), click the **Provisioning** > **Security** > **Users** tabs.

Step 2 Select the user to delete.

Step 3 Click **Delete**.

Step 4 Check Logout before Delete checkbox to end the telnet session.

Step 5 Click **OK** to delete the user.

Step 6 Return to your originating procedure (NTP).

Note When Line VTY is enabled, checking the Logout before Delete checkbox will not end the telnet session. To end the telnet session manually, run the following commands:**show users**

clear line <vty num>