



Cisco Transport Controller Operation

This chapter describes Cisco Transport Controller (CTC), the Cisco ONS 15600 software interface that is stored on the Timing and Shelf Controller (TSC) card and downloaded to your workstation each time you log into the ONS 15600. For CTC setup and login information, refer to the *Cisco ONS 15600 Procedure Guide*.

Chapter topics include:

- [4.1 CTC Software Delivery Methods, page 4-1](#)
- [4.2 CTC Installation Overview, page 4-2](#)
- [4.3 PC and UNIX Workstation Requirements, page 4-3](#)
- [4.4 CTC Login, page 4-4](#)
- [4.5 CTC Window, page 4-6](#)
- [4.6 CTC Card Reset, page 4-13](#)
- [4.7 TSC Card Database, page 4-13](#)
- [4.8 Software Load Revert, page 4-13](#)

4.1 CTC Software Delivery Methods

Use CTC to provision and administer the ONS 15600. CTC is a Java application that is installed in two locations:

- ONS 15600 TSC card
- PCs and UNIX workstations that connect to the ONS 15600

CTC is stored on the TSC card and is downloaded to your workstation each time you log into an ONS 15600.

4.1.1 CTC Software Installed on the TSC Card

CTC software is preloaded on the ONS 15600 TSC cards; therefore, you do not need to install software on the TSC. To upgrade to a newer CTC software version, use the *Cisco ONS 15600 Software Upgrade Guide*.

You can view the software versions that are installed on one ONS 15600 by clicking the Maintenance > Software tabs in node view. Click the tabs in network view to display the software versions installed on all the network nodes.

4.1.2 CTC Software Installed on the PC or UNIX Workstation

When you connect to the ONS 15600, the TSC card automatically downloads the CTC software to your computer, where it is automatically installed if you have the correct Java Runtime Environment (JRE). The automatic download/installation process ensures that your computer is running the same CTC software version as the TSC you are accessing. The CTC software files are stored in the temporary directory designated by your computer's operating system. You can use the Delete CTC Cache button to remove files stored in the temporary directory. If the files are deleted, they are downloaded the next time you connect to an ONS 15600. Downloading the Java archive (JAR) files for CTC takes several minutes depending on the bandwidth of the connection between your workstation and the ONS 15600. For example, JAR files downloaded from a modem or a SONET data communications channel (SDCC) network link requires more time than JAR files downloaded over a LAN connection.

4.2 CTC Installation Overview

To connect to an ONS 15600 using CTC, enter the ONS 15600 IP address in the URL field of a web browser, such as Netscape Navigator or Microsoft Internet Explorer. After connecting to an ONS 15600, the following events occur automatically:

**Note**

Each ONS 15600 has a unique IP address that you use to access the ONS 15600. The initial IP address, 192.168.1.2, is the default address for ONS 15600 access and configuration.

1. A CTC launcher applet is downloaded from the TSC to your computer's temporary directory. (If these files are deleted, they are automatically reinstalled the next time you connect to the ONS 15600.)
2. The launcher determines whether your computer has a CTC release matching the release on the ONS 15600 TSC.
3. If the computer does not have CTC installed, or if the installed release is older than the TSC version, the launcher downloads the CTC program files from the TSC.
4. The launcher starts CTC. The CTC session is separate from the web browser session, so the web browser is no longer needed. If you log into an ONS 15600 that is connected to ONS 15600s with older versions of CTC, or to Cisco ONS 15454s or ONS 15327s, CTC element files are downloaded automatically to enable you to interact with those nodes. You cannot interact with nodes on the network that have a newer software version than the node that you are logged into (the nodes will appear gray in network view). Therefore, always log into nodes with the latest software release.

Each ONS 15600 can handle up to 16 simultaneous CTC sessions. CTC performance might vary depending upon the volume of activity in each session.

**Note**

You can also use TL1 commands to communicate with the ONS 15600 through VT100 terminals and VT100 emulation software, or you can telnet to an ONS 15600 using TL1 port 3083. See the *Cisco ONS SONET TLI Command Guide* for a comprehensive list of TL1 commands.

4.3 PC and UNIX Workstation Requirements

To use CTC with an ONS 15600, your computer must have a web browser with the correct JRE installed and a modified java.policy file. The correct JRE, Java plug-in, and modified java.policy file for the CTC software release are included on the Cisco ONS 15600 software CD.



Note

To avoid network performance issues, Cisco recommends managing a maximum of 50 nodes concurrently with CTC. The 50 nodes can be on a single DCC or split across multiple DCCs. Cisco does not recommend running multiple CTC sessions when managing two or more large networks.

To manage more than 50 nodes, Cisco recommends using Cisco Transport Manager (CTM). If you do use CTC to manage more than 50 nodes, you can improve performance by adjusting the heap size; see the “General Troubleshooting” chapter of the *Cisco ONS 15600 Troubleshooting Guide*. You can also create login node groups; see the “Connect the PC and Log Into the GUI” chapter of the *Cisco ONS 15600 Procedure Guide*.

Table 4-1 provides the minimum requirements for PCs and UNIX workstations.

Table 4-1 Minimum Computer Requirements for CTC

Area	Requirements	Notes
Processor (PC only)	Pentium 4 processor or equivalent	A faster CPU is recommended if your workstation runs multiple applications or if CTC manages a network with a large number of nodes and circuits.
RAM	512 MB or more	A minimum of 1 GB is recommended if your workstation runs multiple applications or if CTC manages a network with a large number of nodes and circuits.
Hard drive	20 GB hard drive with 50 MB of space available	CTC application files are downloaded from the TSC to your computer's Temp directory. These files occupy 5 to 10 MB of hard drive space.
Operating system	<ul style="list-style-type: none"> PC: Windows 98, Windows NT 4.0, Windows 2000, or Windows XP Workstation: Ultra 10 Sun running SunOS 6, 7, or 8 	—
Web browser	<ul style="list-style-type: none"> PC: Netscape 4.76, Netscape 7.x, Internet Explorer 6.x UNIX Workstation: Netscape 4.76, Netscape 7.x 	<p>For the PC, use JRE 1.4.2 or 1.3.1_02 with any supported web browser. For UNIX, use JRE 1.4.2 with Netscape 7.x or JRE 1.3.1_02 with Netscape 4.76.</p> <p>Netscape 4.76 or 7.x is available at the following site: http://channels.netscape.com/ns/browsers/default.jsp</p> <p>Internet Explorer 6.x is available at the following site: http://www.microsoft.com</p>

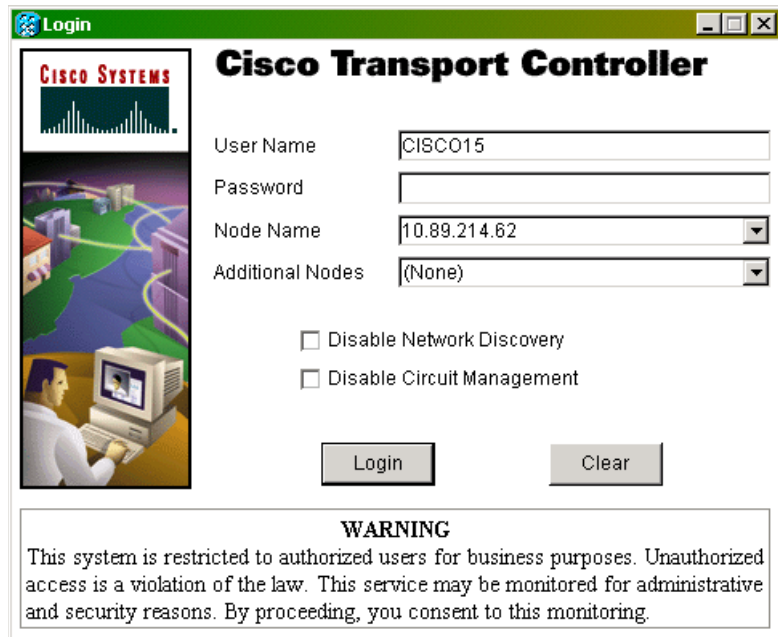
Table 4-1 Minimum Computer Requirements for CTC (continued)

Area	Requirements	Notes
Java Runtime Environment	JRE 1.4.2	JRE 1.4.2 is installed by the CTC Installation Wizard included on the Cisco ONS 15600 software and documentation CDs. JRE 1.4.2 provides enhancements to CTC performance, especially for large networks with numerous circuits. Cisco recommends that you use JRE 1.4.2 for networks with Software R5.0 nodes. If CTC must be launched directly from nodes running software earlier than R5.0, Cisco recommends JRE 1.3.1_02.
Java.policy file	A java.policy file modified for CTC	The java.policy file is modified by the CTC Installation Wizard included on the Cisco ONS 15600 software and documentation CDs.
Cable	Use a crossover or straight-through LAN (CAT-5) cable to connect: <ul style="list-style-type: none"> The ONS 15600 to a hub using the backplane RJ-45 ports, or to connect through a LAN. The ONS 15600 to a PC using the backplane RJ-45 ports. The active TSC RJ-45 port to a laptop or hub. 	A direct PC-to-ONS 15600 connection means your computer is physically connected to the ONS 15600. This is most commonly done by connecting a LAN (CAT-5) straight-through cable from your PC to the RJ-45 port on the TSC. However, direct connections include connections to switches or hubs where the ONS 15600 is physically connected. Note Use only the active TSC connector for connectivity. If you connect to the standby or switch TSCs, you will lose connectivity. Cisco recommends that you use the RJ-45 connector on the Customer Access Panel (CAP) so that connection to the ONS 15600 will not be lost during a TSC switch.

4.4 CTC Login

After you have installed CTC, you can log in to a node using your browser. To log in, you must type the node IP address in the URL window. The CTC Login window appears (Figure 4-1).

Figure 4-1 Login Window



WARNING
This system is restricted to authorized users for business purposes. Unauthorized access is a violation of the law. This service may be monitored for administrative and security reasons. By proceeding, you consent to this monitoring.

The CTC Login window provides the following options to accelerate the login process.

- The Disable Network Discovery option omits the discovery of nodes with data communications channel (DCC) connectivity. To access all nodes with DCC connectivity, make sure that Disable Network Discovery is not checked.
- The Disable Circuit Management option omits the discovery of circuits. To view circuits immediately after logging in, make sure that Disable Circuit Management is not checked. However, if disabled, after you have logged in you can click the Circuits tab and CTC will give you the option to enable circuit management.

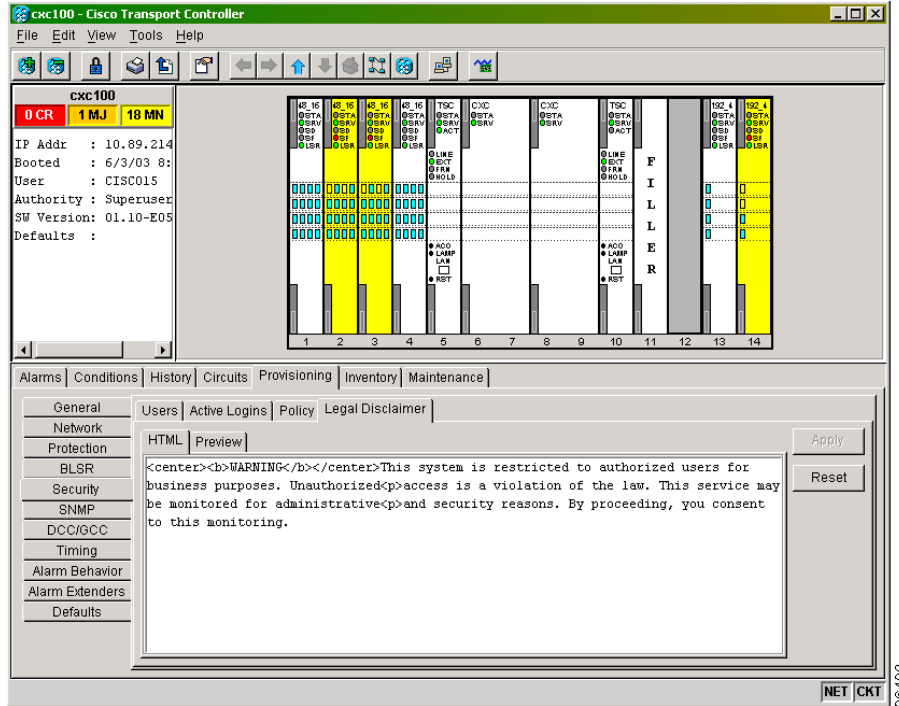
These options are useful if you want to log in to a node to perform a single task, such as placing a card in or out of service, and do not want to wait while CTC discovers DCC connections and circuits.

4.4.1 Legal Disclaimer

The CTC Login window currently displays the following warning message (Figure 4-1): “Warning: This system is restricted to authorized users for business purpose. Unauthorized access is a violation of the law. This service can be monitored for administrative and security reasons. By proceeding, you consent to this monitoring.”

The ONS 15600 allows a user with Superuser privileges to modify the default login warning message and save it to a node using the Provisioning > Security > Legal Disclaimer > HTML tab (Figure 4-2). The login warning message field allows up to 250 characters of text (1600 characters total, including HTML markup).

Figure 4-2 Legal Disclaimer Tab



4.4.2 Login Node Group

Login node groups display nodes that have only an IP connection. After you are logged into CTC, you can create a login node group from the Edit > Preferences menu. Login groups appear in the Additional Nodes list (Figure 4-1 on page 4-5) on the Login window.

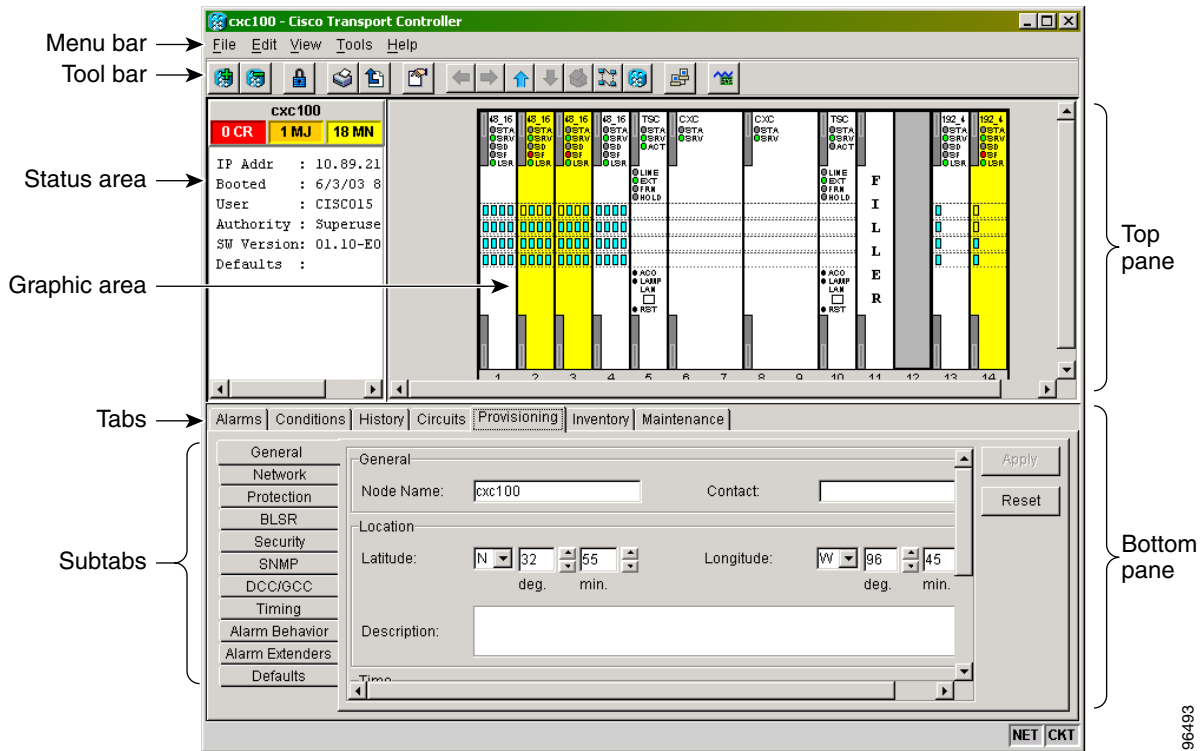
For example, if you logged into Node 1, you would see Node 2 and Node 3 because they have DCC connectivity to Node 1. You would not see Nodes 4, 5, and 6 because DCC connections do not exist. To view all six nodes at once, you create a login node group with the IP addresses of Nodes 1, 4, 5, and 6. Those nodes, and all nodes optically connected to them, appear when you select the login group from the Additional Nodes list on the Login window the next time you log in.

4.5 CTC Window

The CTC window appears after you log into an ONS 15600. The CTC node view is the first view that appears after you log into an ONS 15600 (Figure 4-3). The login node is the first node displayed, and it is the “home view” for the session (accessed by choosing View > Go To Home View).

The CTC window includes a menu bar, a toolbar, and a top and bottom pane. The top pane displays status information about the selected objects and a graphic of the current view. The bottom pane displays tabs and subtabs, which you use to view ONS 15600 information and perform ONS 15600 provisioning and maintenance. From the default node view window you can display the other two ONS 15600 views: network and card.

Figure 4-3 CTC Window Elements in the Node View (Default Login View)



96493

4.5.1 Node View

Node view allows you to view and manage one ONS 15600 node (Figure 4-3). The status area shows the node name; number of Critical (CR), Major (MJ), and Minor (MN) alarms; IP address; session boot date and time; name of the current logged-in user; and user security level.

4.5.1.1 CTC Card Colors

The graphic area of the CTC window depicts the ONS 15600 shelf assembly. The colors of the cards in the graphic reflect the real-time status of the physical card, slot, and port. Table 4-2 describes the node view card colors.

Table 4-2 Node View Card Colors

Card Color	Status
Gray	Slot is not provisioned; no card is installed.
Violet	Slot is provisioned; no card is installed (the card immediately changes to yellow because the IMPROPRMVL alarm is raised).
White	Slot is provisioned; a functioning card is installed or booting.
Yellow	Slot is provisioned; a minor alarm condition exists.
Orange	Slot is provisioned; a major alarm condition exists.
Red	Slot is provisioned; a critical alarm exists.

Port color in both card and node view indicates the port service state. [Table 4-3](#) lists the port colors and their service states. For more information about port service states, see [Appendix B, “Administrative and Service States.”](#)

Table 4-3 Node View Card Port Colors and Service States

Port Color	Service State	Description
Blue	OOS-MA,LPBK	(Out-of-Service and Management, Loopback) Port is in a loopback state. On the card in node view, a line between ports indicates that the port is in terminal or facility loopback (see Figure 4-4 and Figure 4-5). Traffic is carried and alarm reporting is suppressed. Raised fault conditions, whether or not their alarms are reported, can be retrieved on the CTC Conditions tab or by using the TL1 RTRV-COND command.
Blue	OOS-MA,MT	(Out-of-Service and Management, Maintenance) Port is out-of-service for maintenance. Traffic is carried and loopbacks are allowed. Alarm reporting is suppressed. Raised fault conditions, whether or not their alarms are reported, can be retrieved on the CTC Conditions tab or by using the TL1 RTRV-COND command. Use OOS-MA,MT for testing or to suppress alarms temporarily. Change the state to IS-NR, OOS-MA,DSBLD, or OOS-AU,AINS when testing is complete.
Gray	OOS-MA,DSBLD	(Out-of-Service and Management, Disabled) The port is out-of-service and unable to carry traffic. Loopbacks are not allowed in this service state.
Green	IS-NR	(In-Service and Normal) The port is fully operational and performing as provisioned. The port transmits a signal and displays alarms; loopbacks are not allowed.
Violet	OOS-AU,AINS	(Out-of-Service and Autonomous, Automatic In-Service) The port is out-of-service, but traffic is carried. Alarm reporting is suppressed. The node monitors the ports for an error-free signal. After an error-free signal is detected, the port stays in OOS-AU,AINS state for the duration of the soak period. After the soak period ends, the port service state changes to IS-NR. Raised fault conditions, whether or not their alarms are reported, can be retrieved on the CTC Conditions tab or by using the TL1 RTRV-COND command. The AINS port will automatically transition to IS-NR when a signal is received for the length of time provisioned in the soak field.

Figure 4-4 Terminal Loopback Indicator



Figure 4-5 Facility Loopback Indicator

4.5.1.2 Node View Card Shortcuts

If you move your mouse over cards in the graphic, popups display additional information about the card including the card type; card status (active or standby); the type of alarm, such as critical, major, and minor (if any); and the alarm profile used by the card. Right-click a card to reveal a shortcut menu that you can use to open, reset, or delete a card. Right-click a slot to preprovision a card (that is, provision a slot before installing the card).

4.5.1.3 Node View Tabs

Table 4-4 lists the tabs and subtabs available in the node view.

Table 4-4 Node View Tabs and Subtabs

Tab	Description	Subtabs
Alarms	Lists current alarms (CR, MJ, MN) for the node and updates them in real time.	—
Conditions	Allows you to retrieve a list of standing conditions on the node.	—
History	Provides a history of node alarms including date, type, and severity of each alarm. The Session subtab displays alarms and events for the current session. The Node subtab displays alarms and events retrieved from a fixed-size log on the node.	Session, Node
Circuits	Allows you to create, delete, edit, and reroute circuits.	Circuits, Rolls
Provisioning	Allows you to provision the ONS 15600 node.	General, Network, Protection, BLSR, Security, SNMP, Comm Channels, kAlarm Behavior, Alarm Extenders, Defaults
Inventory	Provides inventory information (part number, serial number, Common Language Equipment Identification [CLEI] codes) for cards installed in the node. Allows you to delete and reset cards, and change card service state. For more information on card service states, see Appendix B, “Administrative and Service States.”	—
Maintenance	Allows you to perform maintenance tasks for the node.	Database, Protection, Diagnostic, BLSR, Software, Timing, Audit, Routing Table, Test Access, Alarm Extenders, Preferred Copy

4.5.2 Network View

Network view allows you to view and manage ONS 15600s, ONS 15454s, and ONS 15327s that have DCC connections to the node that you logged into and any login node groups you have selected (Figure 4-6).

Figure 4-6 Network Displayed in CTC Network View

Asterisk indicates topology host

Bold letters indicate Login node; icon color indicates node status

Dots indicate selected node

User	Security Level	Last Login Time	Last Login Node	Failed Logins	Locked Out
CISC015	SUPERUSER	06/05/2003 11:...	Interop-471	10	No
johan1	SUPERUSER	06/05/2003 11:...	Interop-451	0	No
johan2	SUPERUSER	06/04/2003 18:...	Interop-432	0	No
johan3	SUPERUSER			0	No
rtayal	SUPERUSER			0	No



Note

Nodes with DCC connections to the login node will not be displayed if you select Disable Network Discovery on the Login dialog box.

To access network view, choose **View > Go To Network View** or click the up arrow in the CTC toolbar.

The graphic area displays a background image with colored node icons. A Superuser can set up the logical network view feature, which enables each user to see the same network view.

The node icon colors indicate the node status (Table 4-5). Lines show DCC connections between the nodes. Selecting a node or span in the graphic area displays information about the node and span in the status area.

Table 4-5 Node Status

Color	Alarm Status
Green	No alarms
Yellow	Highest-level alarm is a minor alarm
Orange	Highest-level alarm is major alarm
Red	Highest-level alarm is a critical alarm
Gray with node name	Node is initializing
Gray with IP address	Node is initializing; a problem exists with IP routing from node to CTC or your login/password is not provisioned on this node

Table 4-6 lists the tabs and subtabs available in the network view.

Table 4-6 Network View Tabs and Subtabs

Tab	Description	Subtabs
Alarms	Lists current alarms (CR, MJ, MN) for the network and updates them in real time	—
Conditions	Displays a list of standing conditions on the network	—
History	Provides a history of network alarms including date, type, and severity of each alarm	—
Circuits	Create, delete, edit, filter and search for network circuits	Circuits, Rolls
Provisioning	Provision security, alarm profiles, bidirectional line switched rings (BLSRs), and overhead circuits	Security, Alarm Profiles, BLSR, Overhead Circuits, Provisionable Patchcords (PPC)
Maintenance	Displays the type of equipment and the status of each node in the network; displays working and protect software versions, and allows software to be downloaded	Software

4.5.3 Card View

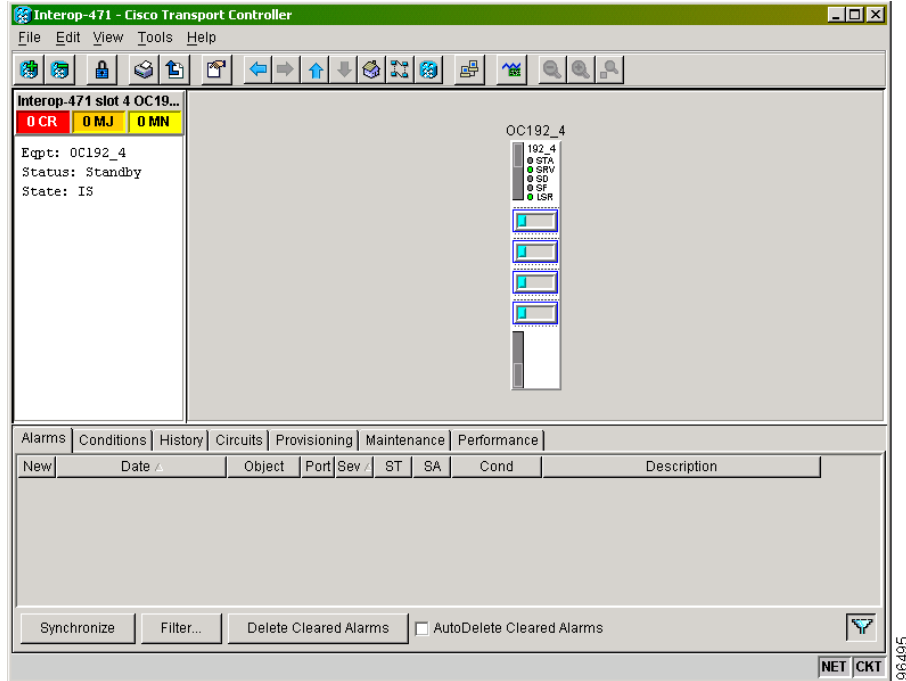
The card view provides information about individual ONS 15600 cards. Use this window to perform card-specific maintenance and provisioning (Figure 4-7). A graphic showing the ports on the card is shown in the graphic area. The status area displays the node name, slot, number of alarms, card type, equipment type, and the card status (active or standby), card service state if the card is present, and port service state (described in Table 4-3 on page 4-8). The information that appears and the actions you can perform depend on the card. For more information about card service states, see Appendix B, “Administrative and Service States.”



Note

CTC displays a card view for all ONS 15600 cards except the TSC and Single Shelf Cross-Connect (SSXC) cards. Provisioning for these common control cards occurs at the node view; therefore, no card view is necessary.

Figure 4-7 CTC Card View Showing an OC-192 Card



Use the card view tabs and subtabs, shown in [Table 4-7](#), to provision and manage the ONS 15600. The subtabs, fields, and information displayed under each tab depend on the card type selected.

Table 4-7 Card View Tabs and Subtabs

Tab	Description	Subtabs
Alarms	Lists current alarms (CR, MJ, MN) for the card and updates them in real time	—
Conditions	Displays a list of standing conditions on the card	—
History	Provides a history of card alarms including date, object, port, and severity of each alarm	Session (displays alarms and events for the current session); Card (displays alarms and events retrieved from a fixed-size log on the card)
Circuits	Create, delete, edit, and search circuits	Circuits, Rolls
Provisioning	Provision an ONS 15600 card	Line, SONET Thresholds, SONET STS, and Alarm Profiles
Maintenance	Perform maintenance tasks for the card	Loopback, Transceiver, Protection, Path Trace, AINS Soak (options depend on the card type)
Performance	Perform performance monitoring for the card	—

4.6 CTC Card Reset

You can reset the ONS 15600 cards by using the hard-reset or soft-reset commands in CTC, or by physically reseating a card (card pull). From the node view, select a card and right-click to open a menu with the hard-reset and soft-reset commands. Soft resets do not impact traffic, however hard resets are service-affecting. A card must be in the Out-of-Service and Management, Maintenance (OOS-MA,MT) service state before you can perform a hard reset.

A soft reset on the TSC reboots the TSC and reloads the operating system and the application software. You can apply a CTC soft reset to either an active or standby TSC without affecting traffic. A CTC hard reset temporarily removes power from the TSC and clears all buffer memory. You should only perform a hard reset (or a card pull) on a standby TSC. If you need to perform a CTC hard reset or card pull on an active TSC, put the TSC into standby mode first by performing a soft reset.

A soft reset on an optical card with an active port in a 1+1 protection group will result in a loss of all DCC traffic terminated or tunneled on the active port for the duration of the reset time. A soft reset of an optical card with a standby port in a 1+1 protection group will not affect DCC traffic. A CTC hard reset of an optical card causes a switch to the protect card.

4.7 TSC Card Database

Each TSC card hosts a separate database; therefore, the protect card's database is available if the database on the working TSC fails. After a database change, there might be a 30-second interval before the TSC starts writing the data to the Flash drive. If you reset the active TSC immediately after a database change, the change could be lost.

You can also store a backup version of the database on the workstation running CTC. This operation should be part of a regular ONS 15600 maintenance program at approximately weekly intervals and should also be completed when preparing an ONS 15600 for a software upgrade or a pending natural disaster, such as a flood.

**Note**

The Internet Inter-ORB Protocol (IIOP) port is not backed up and restored.

**Note**

The ONS 15600 does not allow you to restore a database from one node to another node. You can install a database from one node on another node by using the Configure Node option on the **Maintenance > Database** tab.

4.8 Software Load Revert

Before you upgrade to Software Release 5.0, you must create a database backup. If you later need to restore the original working software load from the protect software load, CTC displays a prompt requesting the location of the backup. Any provisioning performed with Software R5.0 will be lost when the Software R1.1.x backup is restored.

**Note**

After a software load is activated (upgraded to a higher software release), any circuits created and provisioning performed will not reinstate if an older database is restored. The database configuration at the time of activation is reinstated after a revert.
