C H A P T E R **8**

Cisco Transport Controller Operation

This chapter describes Cisco Transport Controller (CTC), the software interface for the Cisco ONS 15454. For CTC set up and login information, refer to the *Cisco ONS 15454 Procedure Guide*.

Chapter topics include:

8.1 CTC Software Delivery Methods

ONS 15454 provisioning and administration is performed using the CTC software. CTC is a Java application that is installed in two locations; CTC is stored on the Advanced Timing, Communications, and Control (TCC2) card or the Advanced Timing, Communications, and Control Plus (TCC2P) card, and it is downloaded to your workstation the first time you log into the ONS 15454 with a new software release.

8.1.1 CTC Software Installed on the TCC2/TCC2P Card

CTC software is preloaded on the ONS 15454 TCC2/TCC2P cards; therefore, you do not need to install software on the TCC2/TCC2P cards. When a new CTC software version is released, use the release-specific software upgrade document to upgrade the ONS 15454 software on the TCC2/TCC2P cards.

When you upgrade CTC software, the TCC2/TCC2P cards store the new CTC version as the protect CTC version. When you activate the new CTC software, the TCC2/TCC2P cards store the older CTC version as the protect CTC version, and the newer CTC release becomes the working version. You can view the software versions that are installed on an ONS 15454 by selecting the Maintenance > Software tabs in node view (Figure 8-1).
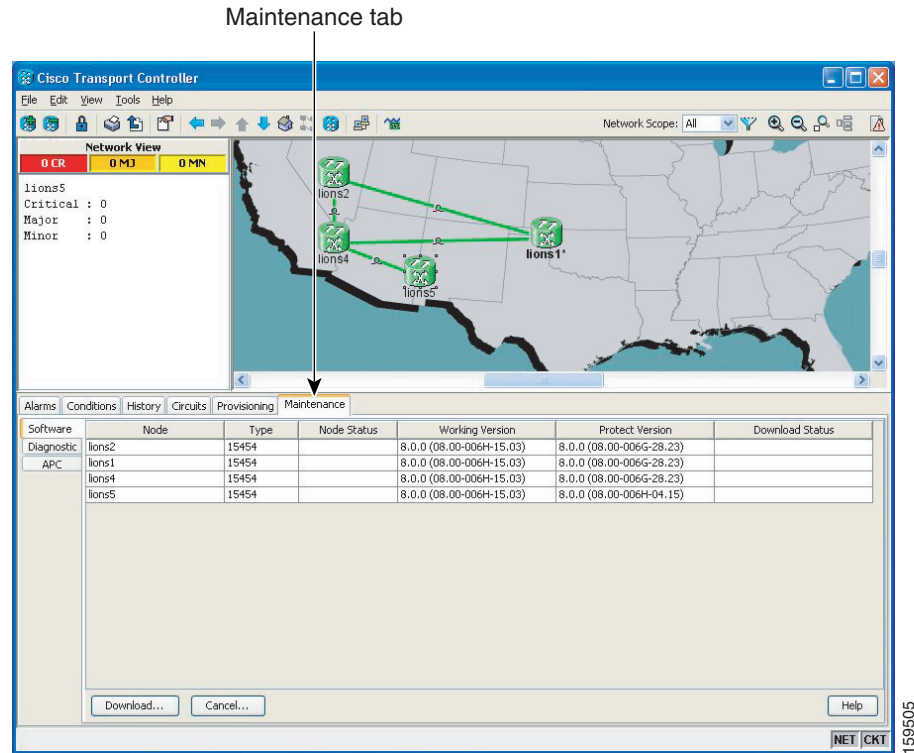
Figure 8-1　　　*CTC Software Versions, Node View*
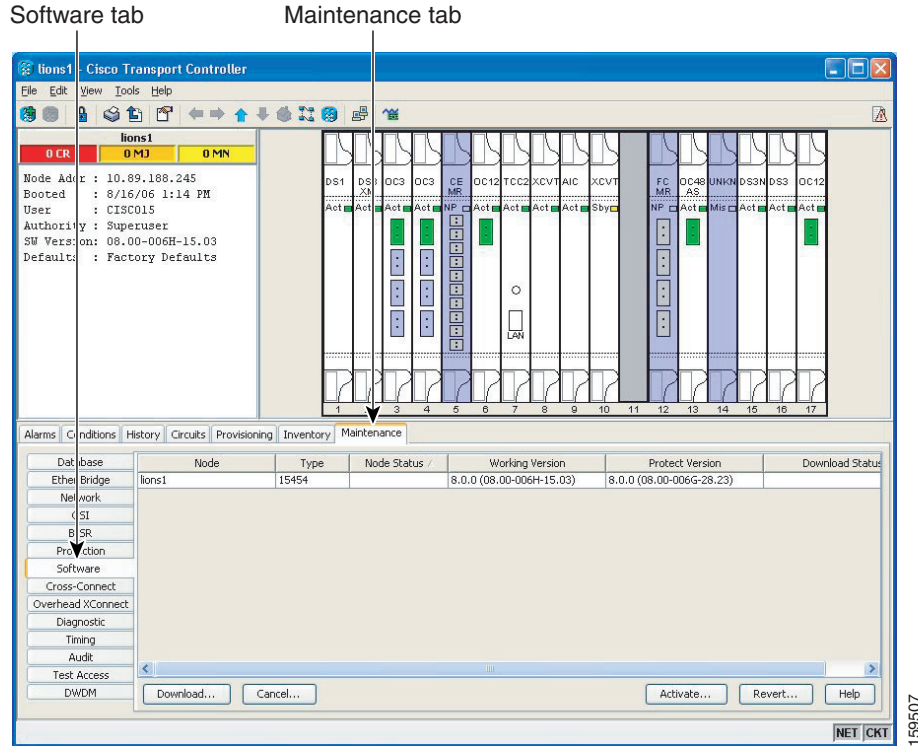
Select the Maintenance > Software tabs in network view to display the software versions installed on all the network nodes (Figure 8-2).

Figure 8-2   CTC Software Versions, Network View

8.1.2 CTC Software Installed on the PC or UNIX Workstation

CTC software is downloaded from the TCC2/TCC2P cards and installed on your computer automatically after you connect to the ONS 15454 with a new software release for the first time. Downloading the CTC software files automatically ensures that your computer is running the same CTC software version as the TCC2/TCC2P cards you are accessing. The CTC files are stored in the temporary directory designated by your computer operating system. You can use the Delete CTC Cache button to remove files stored in the temporary directory. If the files are deleted, they download the next time you connect to an ONS 15454. Downloading the Java archive (JAR) files for CTC takes several minutes depending on the bandwidth of the connection between your workstation and the ONS 15454. For example, JAR files downloaded from a modem or a data communications channel (DCC) network link require more time than JAR files downloaded over a LAN connection.

During network topology discovery, CTC polls each node in the network to determine which one contains the most recent version of the CTC software. If CTC discovers a node in the network that has a more recent version of the CTC software than the version you are currently running, CTC generates a message stating that a later version of the CTC has been found in the network and offers to install the CTC software upgrade JAR files. If you have network discovery disabled, CTC will not seek more recent versions of the software. Unreachable nodes are not included in the upgrade discovery.

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

8.2 CTC Installation Overview

To connect to an ONS 15454 using CTC, you enter the ONS 15454 IP address in the URL field of Netscape Navigator or Microsoft Internet Explorer. After connecting to an ONS 15454, the following occurs automatically:

1. A CTC launcher applet is downloaded from the TCC2/TCC2P card to your computer.

2. The launcher determines whether your computer has a CTC release matching the release on the ONS 15454 TCC2/TCC2P card.

3. If the computer does not have CTC installed, or if the installed release is older than the TCC2/TCC2P card's version, the launcher downloads the CTC program files from the TCC2/TCC2P card.

4. The launcher starts CTC. The CTC session is separate from the web browser session, so the web browser is no longer needed. Always log into nodes having the latest software release. If you log into an ONS 15454 that is connected to ONS 15454s with older versions of CTC, or to Cisco ONS 15327s or Cisco ONS 15600s, CTC files are downloaded automatically to enable you to interact with those nodes. The CTC file download occurs only when necessary, such as during your first login. You cannot interact with nodes on the network that have a software version later than the node that you used to launch CTC.

Each ONS 15454 can handle up to five concurrent CTC sessions. CTC performance can vary, depending on the volume of activity in each session, network bandwidth, and TCC2/TCC2P card load.

> **Note** You can also use TL1 commands to communicate with the Cisco ONS 15454 through VT100 terminals and VT100 emulation software, or you can telnet to an ONS 15454 using TL1 port 3083. Refer to the *Cisco ONS SONET TL1 Command Guide* for a comprehensive list of TL1 commands.

8.3 PC and UNIX Workstation Requirements

To use CTC for the ONS 15454, your computer must have a web browser with the correct Java Runtime Environment (JRE) installed. The correct JRE for each CTC software release is included on the Cisco ONS 15454 software CD. If you are running multiple CTC software releases on a network, the JRE installed on the computer must be compatible with the different software releases.

You can change the JRE version on the Preferences dialog box JRE tab. When you change the JRE version on the JRE tab, you must exit and restart CTC for the new JRE version to take effect. Table 8-1 shows JRE compatibility with ONS 15454 software releases.

Table 8-1   JRE Compatibility

ONS Software Release	JRE 1.2.2 Compatible	JRE 1.3 Compatible	JRE 1.4 Compatible	JRE 5.0 Compatible
ONS 15454 Release 2.2.1 and earlier	Yes	No	No	No
ONS 15454 Release 2.2.2	Yes	Yes	No	No
ONS 15454 Release 3.0	Yes	Yes	No	No
ONS 15454 Release 3.1	Yes	Yes	No	No
ONS 15454 Release 3.2	Yes	Yes	No	No
ONS 15454 Release 3.3	Yes	Yes	No	No
ONS 15454 Release 3.4	No	Yes	No	No
ONS 15454 Release 4.0 [1]	No	Yes	No	No
ONS 15454 Release 4.1	No	Yes	No	No
ONS 15454 Release 4.5	No	Yes	No	No
ONS 15454 Release 4.6	No	Yes	Yes	No
ONS 15454 Release 5.0	No	No	Yes	No
ONS 15454 Release 6.0	No	No	Yes	No
ONS 15454 Release 7.0	No	No	Yes	Yes
ONS 15454 Release 7.2	No	No	Yes	Yes
ONS 15454 Release 8.0	No	No	No	Yes

1.   Software Releases 4.0 and later notify you if an older version of the JRE is running on your PC or UNIX workstation.

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 15454 Troubleshooting Guide.* You can also create login node groups; see the "Connect the PC and Log Into the GUI" chapter of the *Cisco ONS 15454 Procedure Guide*.

Table 8-2 lists the requirements for PCs and UNIX workstations. In addition to the JRE, the Java plug-in is included on the ONS 15454 software CD.

Table 8-2   *Computer Requirements for CTC*

Area	Requirements	Notes
Processor	Pentium III 700 MHz, UltraSPARC, or equivalent	700 MHz is the recommended processor speed. You can use computers with a lower processor speed; however, you might experience longer response times and slower performance.
RAM	384 MB RAM recommended, 512 MB RAM optimum	Cisco recommends using 512 MG RAM for networks with 25 nodes or more to avoid longer response times and slower performance.
Hard drive	20 GB hard drive with 50 MB of space available	—
Operating System	• PC: Windows 98, Windows NT 4.0 with Service Pack 6a, Windows 2000 with Service Pack 3, or Windows XP with Service Pack 1 • Workstation: Solaris versions 8 or 9	—
Java Runtime Environment	JRE 5.0	JRE 5.0 is installed by the CTC Installation Wizard included on the Cisco ONS 15454 software CD. JRE 5.0 provide enhancements to CTC performance, especially for large networks with numerous circuits. Cisco recommends that you use JRE 5.0 for networks with Software R8.0 nodes. If CTC must be launched directly from nodes running software R7.0 or R7.2, Cisco recommends JRE 1.4.2 or JRE 5.0. If CTC must be launched directly from nodes running software R5.0 or R6.0, Cisco recommends JRE 1.4.2.If CTC must be launched directly from nodes running software earlier than R5.0, Cisco recommends JRE 1.3.1_02.

Table 8-2 *Computer Requirements for CTC (continued)*

Area	Requirements	Notes
Web browser	• PC: Internet Explorer 6.x, Netscape 7.x • UNIX Workstation: Mozilla 1.7 on Solaris 9 and 10, Netscape 4.76, Netscape 7.x	For the PC, use JRE 5.0 with any supported web browser. Cisco recommends Internet Explorer 6.x. For UNIX, use JRE 5.0 with Netscape 7.x. Netscape 7.x is available at the following site: http://channels.netscape.com/ns/browsers/default.jsp Internet Explorer 6.x is available at the following site: http://www.microsoft.com
Cable	User-supplied CAT-5 straight-through cable with RJ-45 connectors on each end to connect the computer to the ONS 15454 directly or through a LAN	—

8.4 ONS 15454 Connection

You can connect to the ONS 15454 in multiple ways. You can connect your PC directly the ONS 15454 (local craft connection) using the RJ-45 port on the TCC2/TCC2P card or the LAN pins on the backplane, connect your PC to a hub or switch that is connected to the ONS 15454, connect to the ONS 15454 through a LAN or modem, or establish TL1 connections from a PC or TL1 terminal. Table 8-3 lists the ONS 15454 connection methods and requirements.

Table 8-3 ONS 15454 Connection Methods

Method	Description	Requirements
Local craft	Refers to onsite network connections between the CTC computer and the ONS 15454 using one of the following: • The RJ-45 (LAN) port on the TCC2/TCC2P card • The LAN pins on the ONS 15454 backplane • A hub or switch to which the ONS 15454 is connected	If you do not use Dynamic Host Configuration Protocol (DHCP), you must change the computer IP address, subnet mask, and default router, or use automatic host detection.
Corporate LAN	Refers to a connection to the ONS 15454 through a corporate or network operations center (NOC) LAN.	• The ONS 15454 must be provisioned for LAN connectivity, including IP address, subnet mask, and default gateway. • The ONS 15454 must be physically connected to the corporate LAN. • The CTC computer must be connected to the corporate LAN that has connectivity to the ONS 15454.
TL1	Refers to a connection to the ONS 15454 using TL1 rather than CTC. TL1 sessions can be started from CTC, or you can use a TL1 terminal. The physical connection can be a craft connection, corporate LAN, or a TL1 terminal.	Refer to the *Cisco ONS SONET TL1 Reference Guide*.
Remote	Refers to a connection made to the ONS 15454 using a modem.	• A modem must be connected to the ONS 15454. • The modem must be provisioned for the ONS 15454. To run CTC, the modem must be provisioned for Ethernet access.

8.5 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.

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. If you have network discovery disabled, CTC will not poll the network for more recent versions of the software. (For more information about the automatic download of the latest CTC JAR files, see the "8.1.2 CTC Software Installed on the PC or UNIX Workstation" section on page 8-3.)

- 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.

8.5.1 Legal Disclaimer

The CTC Login window currently displays the following warning message: "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. The login warning message field allows up to 250 characters of text (1600 characters total, including HTML markup).

8.5.2 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 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.

8.6 CTC Window

The CTC window appears after you log into an ONS 15454 (Figure 8-3). The window includes a menu bar, a toolbar, and a top and bottom pane. The top pane provides status information about the selected objects and a graphic of the current view. The bottom pane provides tabs and subtab to view ONS 15454 information and perform ONS 15454 provisioning and maintenance. From this window you can display three ONS 15454 views: network, node, and card.

Figure 8-3   Node View (Default Login View)
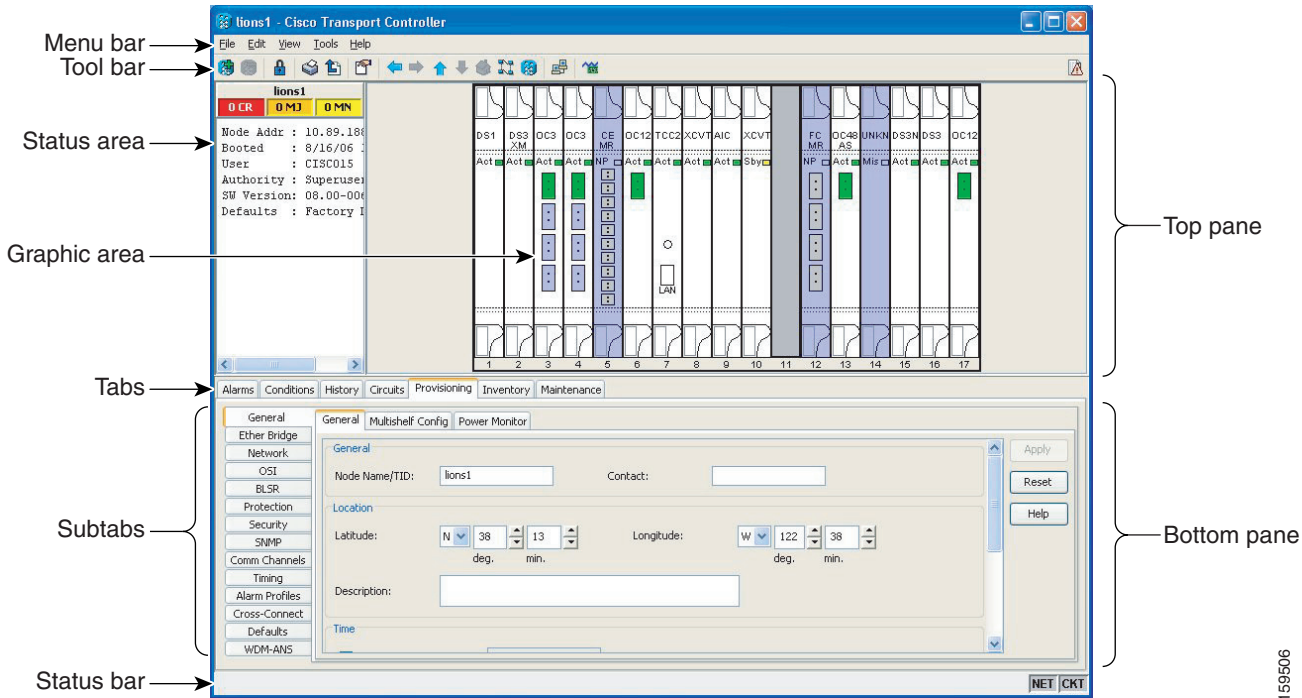
8.6.1 Node View

Node view, shown in Figure 8-3, is the first view that appears after you log into an ONS 15454. The login node is the first node shown, and it is the "home view" for the session. Node view allows you to manage one ONS 15454 node. The status area shows the node name; IP address; session boot date and time; number of Critical (CR), Major (MJ), and Minor (MN) alarms; the name of the current logged-in user; and the security level of the user; software version; and the network element default setup.

8.6.1.1 CTC Card Colors

The graphic area of the CTC window depicts the ONS 15454 shelf assembly. The colors of the cards in the graphic reflect the real-time status of the physical card and slot (Table 8-4).

Table 8-4   Node View Card Colors

Card Color	Status
Gray	Slot is not provisioned; no card is installed.
Violet	Slot is provisioned; no card is installed.
White	Slot is provisioned; a functioning card is installed.
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.

The wording on a card in node view shows the status of a card (Active, Standby, Loading, or Not Provisioned). Table 8-5 lists the card statuses.

Table 8-5 *Node View Card Statuses*

Card Status	Description
Sby	Card is in standby mode.
Act	Card is active.
NP	Card is not present.
Ldg	Card is resetting.
Mis	Card is mismatched.

The port color in both card and node view indicates the port service state. Table 8-6 lists the port colors and their service states. For more information about port service states, see Appendix B, "Administrative and Service States."

Table 8-6 *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 8-4 on page 8-12 and Figure 8-5 on page 8-12). 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.

Table 8-6   Node View Card Port Colors and Service States (continued)

Port Color	Service State	Description
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 8-4   Terminal Loopback Indicator

Figure 8-5   Facility Loopback Indicator

8.6.1.2 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; the card status (active or standby); the type of alarm, such as Critical, Major, or Minor (if any); and the alarm profile used by the card. Right-click a card to reveal a shortcut menu, which you can use to open, reset, delete, or change a card. Right-click a slot to preprovision a card (that is, provision a slot before installing the card).

8.6.1.3 Node View Tabs

Table 8-7 lists the tabs and subtabs available in the node view.

Table 8-7   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	Displays a list of standing conditions on the node.	—

Table 8-7 Node View Tabs and Subtabs (continued)

Tab	Description	Subtabs
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, Shelf
Circuits	Creates, deletes, edits, and maps circuits and rolls.	Circuits, Rolls
Provisioning	Provisions the ONS 15454 node.	General, Ether Bridge, Network, OSI, BLSR, Protection, Security, SNMP, Comm Channels, Timing, Alarm Profiles, Cross-Connect, Defaults, WDM-ANS
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	Performs maintenance tasks for the node.	Database, Ether Bridge, Network, OSI, BLSR, Protection, Software, Cross-Connect, Overhead XConnect, Diagnostic, Timing, Audit, Test Access, DWDM

8.6.2 Network View

Network view allows you to view and manage ONS 15454s that have DCC connections to the node that you logged into and any login node groups you have selected (Figure 8-6).

Figure 8-6   Network in CTC Network View
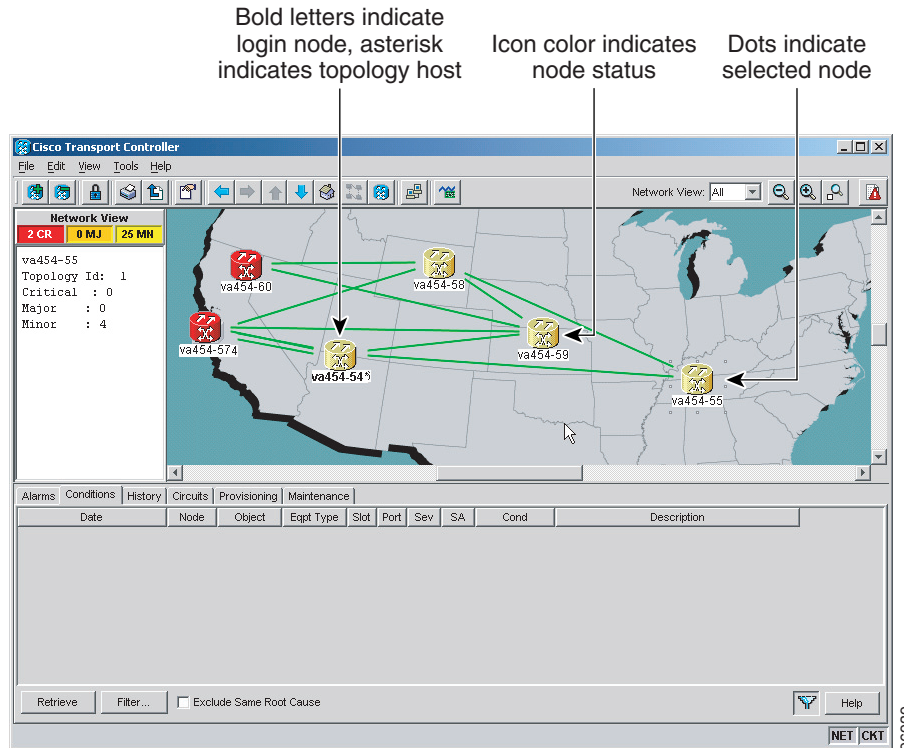
Note   Nodes with DCC connections to the login node do not appear if you checked the Disable Network Discovery check box in the Login dialog box.

The graphic area displays a background image with colored ONS 15454 icons. A Superuser can set up the logical network view feature, which enables each user to see the same network view. Selecting a node or span in the graphic area displays information about the node and span in the status area.

8.6.2.1 Network View Tabs

Table 8-8 lists the tabs and subtabs available in network view.

Table 8-8   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	Creates, deletes, edits, filters, and searches for network circuits and rolls.	Circuits, Rolls

Table 8-8 Network View Tabs and Subtabs (continued)

Tab	Description	Subtabs
Provisioning	Provisions security, alarm profiles, bidirectional line switched rings (BLSRs), overhead circuits, server trails, and loads/manages a VLAN database	Security, Alarm Profiles, BLSR, Overhead Circuits, Server Trails, VLAN DB Profile
Maintenance	Displays the working and protect software versions and allows software to be downloaded, retrieves Open Shortest Path First (OSPF) node information, and displays the list of automatic power control (APC) domains for a network	Software, Diagnostic, APC

8.6.2.2 CTC Node Colors

The color of a node in network view, shown in Table 8-9, indicates the node alarm status.

Table 8-9 Node Status Shown in Network View

Color	Alarm Status
Green	No alarms
Yellow	Minor alarms
Orange	Major alarms
Red	Critical alarms
Gray with Unknown#	Node initializing for the first time (CTC displays Unknown# because CTC has not discovered the name of the node yet)

8.6.2.3 DCC Links

The lines show DCC connections between the nodes (Table 8-10). DCC connections can be green (active) or gray (fail). The lines can also be solid (circuits can be routed through this link) or dashed (circuits cannot be routed through this link). Circuit provisioning uses active/routable links.

Table 8-10 DCC Colors Indicating State in Network View

Color and Line Style	State
Green and solid	Active/Routable
Green and dashed	Active/Nonroutable
Gray and solid	Failed/Routable
Gray and dashed	Failed/Nonroutable

8.6.2.4 Link Consolidation

CTC provides the ability to consolidate the DCC, general communications channel (GCC), optical transport section (OTS), provisionable patchcord (PPC), and server trail links shown in the network view. Link consolidation allows you to condense multiple inter-nodal links into a single link. The link consolidation sorts links by class; for example, all DCC links are consolidated together.You can access individual links within consolidated links using the right-click shortcut menu.

Each link has an associated icon (Table 8-11).

Table 8-11   *Link Icons*

| Icon	Description
	DCC icon
	GCC icon
	OTS icon
	PPC icon
	Server Trail icon

Note Link consolidation is only available on non-detailed maps. Non-detailed maps display nodes in icon form instead of detailed form, meaning the nodes appear as rectangles with ports on the sides. Refer to the *Cisco ONS 15454 Procedure Guide* for more information about consolidated links.

8.6.3 Card View

The card view provides information about individual ONS 15454 cards. Use this window to perform card-specific maintenance and provisioning (Figure 8-7). 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 8-6 on page 8-11). 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."

Figure 8-7   CTC Card View Showing a DS1 Card

Card identification and status

![Note icon]
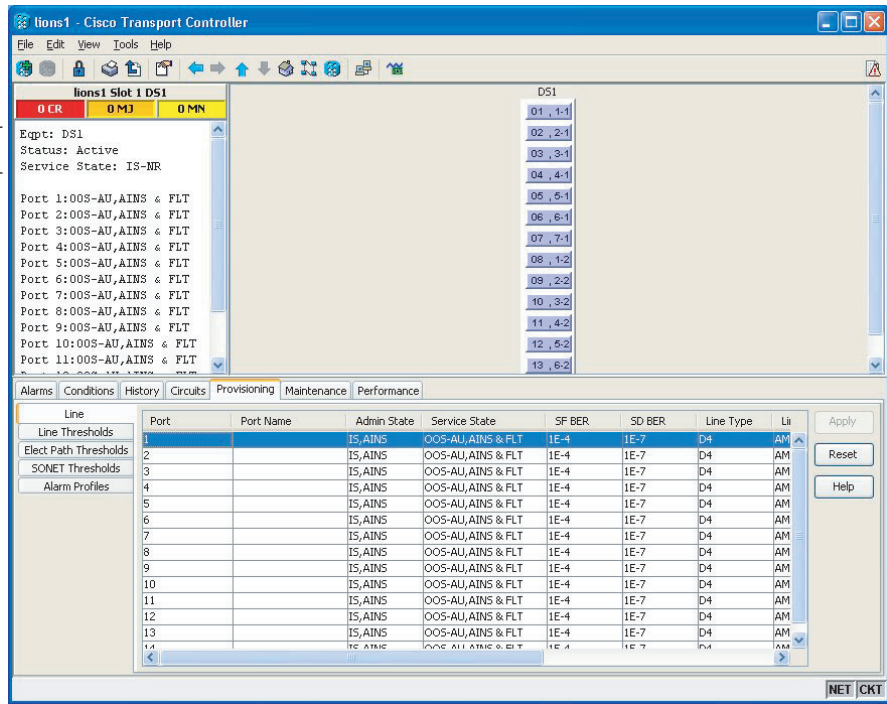
Note   CTC provides a card view for all ONS 15454 cards except the TCC2, TCC2P, XCVT, XC10G, and XC-VXC-10G cards. Provisioning for these common control cards occurs at the node view; therefore, no card view is necessary.

Use the card view tabs and subtabs shown in Table 8-12 to provision and manage the ONS 15454. The subtabs, fields, and information shown under each tab depend on the card type selected. The Performance tab is not available for the Alarm Interface Controller-International (AIC-I) cards.

Table 8-12   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	Creates, deletes, edits, and search circuits and rolls.	Circuits, Rolls

Table 8-12 Card View Tabs and Subtabs (continued)

Tab	Description	Subtabs
Provisioning	Provisions an ONS 15454 card.	DS-N and OC-N cards: Line, Line Thresholds (different threshold options are available for electrical and optical cards), Elect Path Thresholds, SONET Thresholds, Alarm Profiles
		Ethernet cards (subtabs depend on the card type): Line, Line Thresholds, Electrical Path Thresholds, SONET Thresholds, Port, RMON Thresholds, VLAN, Card, Alarm Profiles
Maintenance	Performs maintenance tasks for the card.	DS-N and OC-N cards: Loopback, ALS, Info, Protection, Path Trace, Bandwidth, AINS Soak
		Ethernet cards (subtabs depend on the card type): Path Trace, Loopback, Allocation, AINS Soak, Ether Port Soak, RPR Span Soak
Performance	Performs performance monitoring for the card.	DS-N and OC-N cards: no subtabs
		Ethernet cards: Statistics, Utilization, History
Inventory	Displays an Inventory screen of the ports (TXP and MXP cards only).	—

8.6.4 Print or Export CTC Data

You can use the File > Print or File > Export options to print or export CTC provisioning information for record keeping or troubleshooting. The functions can be performed in card, node, or network views. The File > Print function sends the data to a local or network printer. File > Export exports the data to a file where it can be imported into other computer applications, such as spreadsheets and database management programs.

Whether you choose to print or export data, you can choose from the following options:

- Entire frame—Prints or exports the entire CTC window including the graphical view of the card, node, or network. This option is available for all windows.

- Tabbed view—Prints or exports the lower half of the CTC window containing tabs and data. The printout includes the selected tab (on top) and the data shown in the tab window. For example, if you print the History window Tabbed view, you print only history items appearing in the window. This option is available for all windows.

- Table Contents—Prints or exports CTC data in table format without graphical representations of shelves, cards, or tabs. The Table Contents option prints all the data contained in a table with the same column headings. For example, if you print the History window Table Contents view, you print all data included in the table whether or not items appear in the window.

The Table Contents option does not apply to all windows; for a list of windows that do not support print or export, see the *Cisco ONS 15454 Procedure Guide*.

8.7 Using the CTC Launcher Application to Manage Multiple ONS Nodes

The CTC Launcher application is an executable file, StartCTC.exe, that is provided on Software Release 8.0 CDs for Cisco ONS products. You can use CTC Launcher to log into multiple ONS nodes that are running CTC Software Release 3.3 or higher, without using a web browser.

CTC Launcher provides two connection options. The first option is used to connect to ONS network elements (NEs) that have an IP connection to the CTC computer. The second option is used to connect to ONS NEs that reside behind third party, OSI-based gateway network elements (GNEs). For this option, CTC Launcher creates a TL1 tunnel to transport the TCP traffic through the OSI-based GNE.

The TL1 tunnel transports the TCP traffic to and from ONS ENEs through the OSI-based GNE. TL1 tunnels are similar to the existing static IP-over-CLNS tunnels, GRE and Cisco IP, that can be created at ONS NEs using CTC. (Refer to the Cisco ONS product documentation for information about static IP-over-CLNS tunnels.) However, unlike the static IP-over-CLNS tunnels, TL1 tunnels require no provisioning at the ONS ENE, the third-party GNE, or DCN routers. All provisioning occurs at the CTC computer when the CTC Launcher is started.

Figure 8-8 shows examples of two static IP-over-CLNS tunnels. A static Cisco IP tunnel is created from ENE 1 through other vendor GNE 1 to a DCN router, and a static GRE tunnel is created from ONS ENE 2 to the other vender, GNE 2. For both static tunnels, provisioning is required on the ONS ENEs. In addition, a Cisco IP tunnel must be provisioned on the DCN router and a GRE tunnel provisioned on GNE 2.
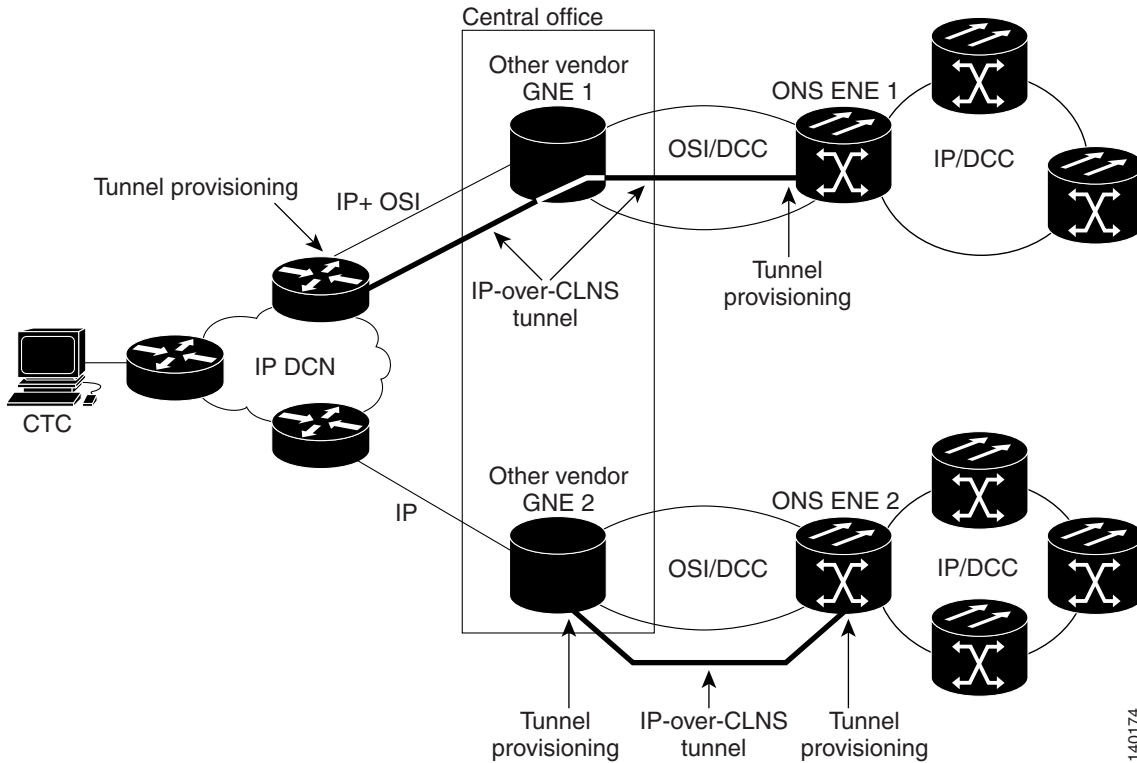
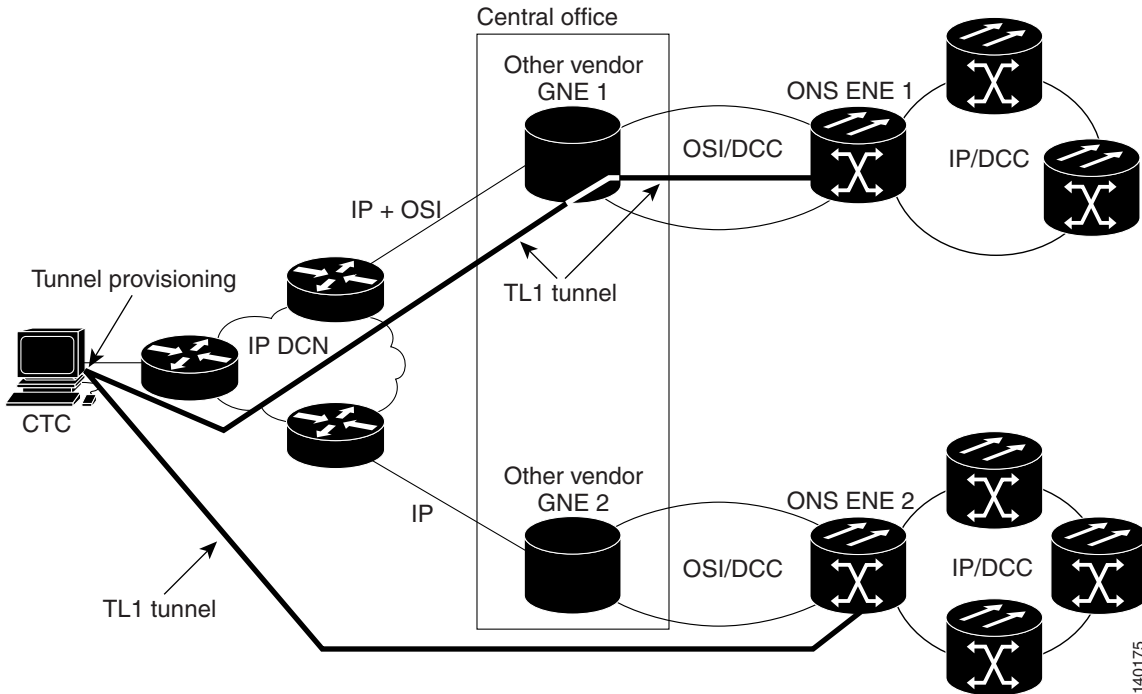*Figure 8-8   Static IP-Over-CLNS Tunnels*

Figure 8-9 shows the same network using TL1 tunnels. Tunnel provisioning occurs at the CTC computer when the tunnel is created with the CTC Launcher. No provisioning is needed at ONS NEs, GNEs or routers.

Figure 8-9   TL1 Tunnels

TL1 tunnels provide several advantages over static IP-over-CLNS tunnels. Because tunnel provisioning is needed only at the CTC computer, they are faster to set up. Because they use TL1 for TCP transport, they are more secure. TL1 tunnels also provide better flow control. On the other hand, IP over CLNS tunnels require less overhead and usually provide a slight performance edge over TL1 Tunnels (depending on network conditions). TL1 tunnels do not support all IP applications such as SNMP and RADIUS Authentication. Table 8-13 shows a comparison between the two types of tunnels.

Table 8-13   TL1 and Static IP-Over-CLNS Tunnels Comparison

Category	Static IP-Over-CLNS	TL1 Tunnel	Comments
Setup	Complex	Simple	Requires provisioning at ONS NE, GNE, and DCN routers. For TL1 tunnels, provisioning is needed at CTC computer.
Performance	Best	Average to good	Static tunnels generally provide better performance than TL1 tunnels, depending on TL1 encoding used. LV+Binary provides the best performance. Other encoding will produce slightly slower TL1 tunnel performance.
Support all IP applications	Yes	No	TL1 tunnels do not support SNMP or RADIUS Server IP applications.
ITU Standard	Yes	No	Only the static IP-over-CLNS tunnels meet ITU standards. TL1 tunnels are new.
Tunnel traffic control	Good	Very good	Both tunnel types provide good traffic control
Security setup	Complex	No setup needed	Static IP-over-CLNS tunnels require careful planning. Because TL1 tunnels are carried by TL1, no security provisioning is needed.

Table 8-13   TL1 and Static IP-Over-CLNS Tunnels Comparison (continued)

Category	Static IP-Over-CLNS	TL1 Tunnel	Comments
Potential to breach DCN from DCC using IP.	Possible	Not possible	A potential exists to breach a DCN from a DCC using IP. This potential does not exist for TL1 tunnels.
IP route management	Expensive	Automatic	For static IP-over-CLNS tunnels, route changes require manual provisioning at network routers, GNEs, and ENEs. For TL1 tunnels, route changes are automatic.
Flow control	Weak	Strong	TL1 tunnels provide the best flow control.
Bandwidth sharing among multiple applications	Weak	Best	—
Tunnel lifecycle	Fixed	CTC session	TL1 tunnels are terminated when the CTC session ends. Static IP-over-CLNS tunnels exist until they are deleted in CTC.

TL1 tunnel specifications and general capabilities include:

- Each tunnel generally supports between six to eight ENEs, depending on the number of tunnels at the ENE.
- Each CTC session can support up to 32 tunnels.
- The TL1 tunnel database is stored locally in the CTC Preferences file.
- Automatic tunnel reconnection when the tunnel goes down.
- Each ONS NE can support at least 16 concurrent tunnels.

8.8 TCC2/TCC2P Card Reset

You can reset the ONS 15454 TCC2/TCC2P card by using CTC (a soft reset) or by physically reseating a TCC2/TCC2P card (a hard reset). A soft reset reboots the TCC2/TCC2P card and reloads the operating system and the application software. Additionally, a hard reset temporarily removes power from the TCC2/TCC2P card and clears all buffer memory.

You can apply a soft reset from CTC to either an active or standby TCC2/TCC2P card without affecting traffic. If you need to perform a hard reset on an active TCC2/TCC2P card, put the TCC2/TCC2P card into standby mode first by performing a soft reset.

Note   When a CTC reset is performed on an active TCC2/TCC2P card, the AIC-I cards go through an initialization process and also reset because AIC-I cards are controlled by the active TCC2/TCC2P.

8.9 TCC2/TCC2P Card Database

When dual TCC2/TCC2P cards are installed in the ONS 15454, each TCC2/TCC2P card hosts a separate database; therefore, the protect card database is available if the database on the working TCC2/TCC2P fails. You can also store a backup version of the database on the workstation running CTC. This

operation should be part of a regular ONS 15454 maintenance program at approximately weekly intervals, and should also be completed when preparing an ONS 15454 for a pending natural disaster, such as a flood or fire.

A database backup may be restored in two ways, partial or complete. A partial database restore operation restores only the provisioning data. A complete database restore operation restores both system and provisioning data. For more information on restoring a database, refer to the *Cisco ONS 15454 Procedure Guide*.

Note The following parameters are not backed up and restored: node name, IP address, mask and gateway, and Internet Inter-ORB Protocol (IIOP) port. If you change the node name and then restore a backed up database with a different node name, the circuits map to the new node name. Cisco recommends keeping a record of the old and new node names.

Note To avoid a node IP and secure IP ending up in the same domain after restoring a database, ensure that the node IP stored in the database differs in domain from that of the node in repeater mode. Also, after restoring a database, ensure that the node IP and secure IP differ in domain.

8.10 Software Revert

When you click the Activate button after a software upgrade, the TCC2/TCC2P copies the current working database and saves it in a reserved location in the TCC2/TCC2P flash memory. If you later need to revert to the original working software load from the protect software load, the saved database installs automatically. You do not need to restore the database manually or recreate circuits.

Note The TCC2/TCC2P card does not carry any software earlier than Software R4.0. You will not be able to revert to a software release earlier than Software R4.0 with TCC2/TCC2P cards installed.

The revert feature is useful if a maintenance window closes while you are upgrading CTC software. You can revert to the protect software load without losing traffic. When the next maintenance window opens, complete the upgrade and activate the new software load.

Circuits created and provisioning done after a software load is activated (upgraded to a higher software release) will be lost with a revert. The database configuration at the time of activation is reinstated after a revert. This does not apply to maintenance reverts (for example, 4.6.2 to 4.6.1), because maintenance releases use the same database.

To perform a supported (non-service-affecting) revert from Software R8.0, the release you want to revert to must have been working at the time you first activated Software R8.0 on that node. Because a supported revert automatically restores the node configuration at the time of the previous activation, any configuration changes made after activation will be lost when you revert the software. Downloading Release 8.0 a second time after you have activated the new load ensures that no actual revert to a previous load can take place (the TCC2/TCC2P card will reset, but will not be traffic affecting and will not change your database).