



Cisco Transport Controller Operation

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



Note

Unless otherwise specified, “ONS 15454” refers to both ANSI and ETSI shelf assemblies.

Chapter topics include:

- [12.1 CTC Software Delivery Methods, page 12-1](#)
- [12.2 CTC Installation Overview, page 12-4](#)
- [12.3 PC and UNIX Workstation Requirements, page 12-4](#)
- [12.4 ONS 15454 Connections, page 12-6](#)
- [12.5 CTC Window, page 12-7](#)
- [12.6 Using the CTC Launcher Application to Manage Multiple ONS Nodes, page 12-19](#)
- [12.7 TCC2/TCC2P Card Reset, page 12-22](#)
- [12.8 TCC2/TCC2P Card Database, page 12-22](#)
- [12.9 Software Revert, page 12-23](#)

12.1 CTC Software Delivery Methods

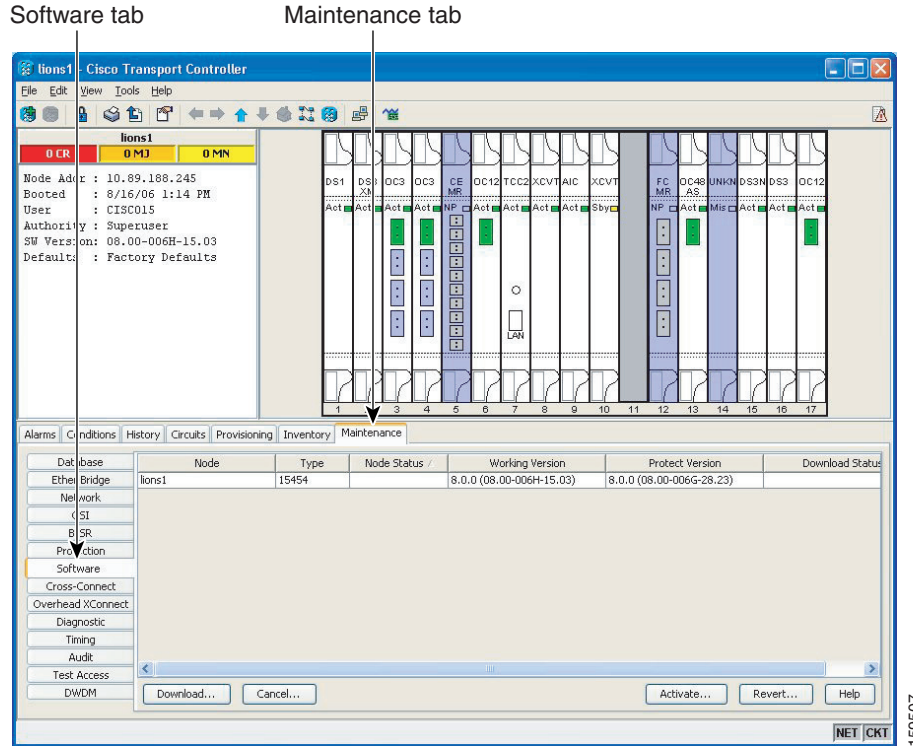
ONS 15454 provisioning and administration is performed using the CTC software. CTC is a Java application that is installed in two locations: it is stored on the TCC2 or TCC2P card and it is downloaded to your workstation the first time you log into the ONS 15454 with a new software release. You can also log into CTC using the CTC launcher application (StartCTC.exe). Refer to the “[12.6 Using the CTC Launcher Application to Manage Multiple ONS Nodes](#)” section on [page 12-19](#) for more information.

12.1.1 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 card.

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 (single-shelf mode) or multishelf view (multishelf mode) (Figure 12-1).

Figure 12-1 CTC Software Versions, Node View (Single-Shelf Mode)



Select the Maintenance > Software tabs in network view to display the software versions installed on all the network nodes (Figure 12-2).

Figure 12-2 CTC Software Versions, Network View

Maintenance tab

Software	Node	Type	Node Status	Working Version	Protect Version	Download Status
Diagnostic	lions2	15454		8.0.0 (08.00-006H-15.03)	8.0.0 (08.00-006G-28.23)	
APC	lions1	15454		8.0.0 (08.00-006H-15.03)	8.0.0 (08.00-006G-28.23)	
	lions4	15454		8.0.0 (08.00-006H-15.03)	8.0.0 (08.00-006G-28.23)	
	lions5	15454		8.0.0 (08.00-006H-15.03)	8.0.0 (08.00-006H-04.15)	

159505

12.1.2 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. After the node view appears, you can upgrade CTC by using the **Tools > Update CTC** menu option. 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.

12.2 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 upon 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* or *Cisco ONS 15454 SDH and Cisco ONS 15600 SDH TL1 Command Guide* for a comprehensive list of TL1 commands.

12.3 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.

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 12-1](#) shows JRE compatibility with ONS 15454 software releases.

Table 12-1 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 4.5	No	Yes	No	No
ONS 15454 Release 4.6	No	Yes	Yes	No
ONS 15454 Release 4.7	No	No	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 ¹

Table 12-1 JRE Compatibility (continued)

ONS Software Release	JRE 1.2.2 Compatible	JRE 1.3 Compatible	JRE 1.4 Compatible	JRE 5.0 Compatible
ONS 15454 Release 7.2	No	No	Yes	Yes ¹
ONS 15454 Release 8.0	No	No	No	Yes

1. JRE 1.4.2 is the preferred version which is included in the 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 15454 DWDM 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 DWDM Procedure Guide*.

[Table 12-2](#) lists the requirements for PCs and UNIX workstations. In addition to the JRE, the Java plug-in is also included on the ONS 15454 software CD.

Table 12-2 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 MG RAM optimum	—
Hard drive	20 GB hard drive with 50 MB of space available	—
Operating System	<ul style="list-style-type: none"> PC: Windows 98 (1st and 2nd editions), Windows ME, 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, 9, or 10 	—

Table 12-2 Computer Requirements for CTC (continued)

Area	Requirements	Notes
Java Runtime Environment	JRE 5.0	JRE 5.0 is installed by the CTC Installation Wizard included on the Cisco ONS 15454 software and CD. JRE 5.0 provides enhancements to CTC performance, especially for large networks with numerous circuits. If CTC must be launched directly from nodes running software earlier than Software Release 4.6, uninstall JRE 1.4.2 and reinstall JRE 1.3.1_02. Then, to run Software R8.0, uninstall JRE 1.3.1_02 and reinstall JRE 5.0.
Web browser	PC: Internet Explorer 6.x or Netscape 7.x UNIX: Mozilla 1.7 or Netscape 7.x	For the PC, Cisco recommends Internet Explorer 6.x. Internet Explorer 6.x is available at the following site: http://www.microsoft.com Netscape 7.x is available at the following site: http://channels.netscape.com/ns/browsers/default.jsp
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. User-supplied cross-over CAT-5 cable to the DCN port on the ONS 15454 patch panel or to the Catalyst 2950 (multishelf mode).	—

12.4 ONS 15454 Connections

You can connect to the ONS 15454 in multiple ways. You can connect your PC directly to the ONS 15454 (local craft connection) using the RJ-45 port on the TCC2/TCC2P card or, for the ANSI shelf, using the LAN pins on the backplane (the ETSI shelf provides a LAN connection via the RJ-45 jack on the MIC-T/C/P Front Mount Electrical Connection [FMEC]). Alternatively, you can 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 12-3](#) lists the ONS 15454 connection methods and requirements.

Table 12-3 ONS 15454 Connection Methods

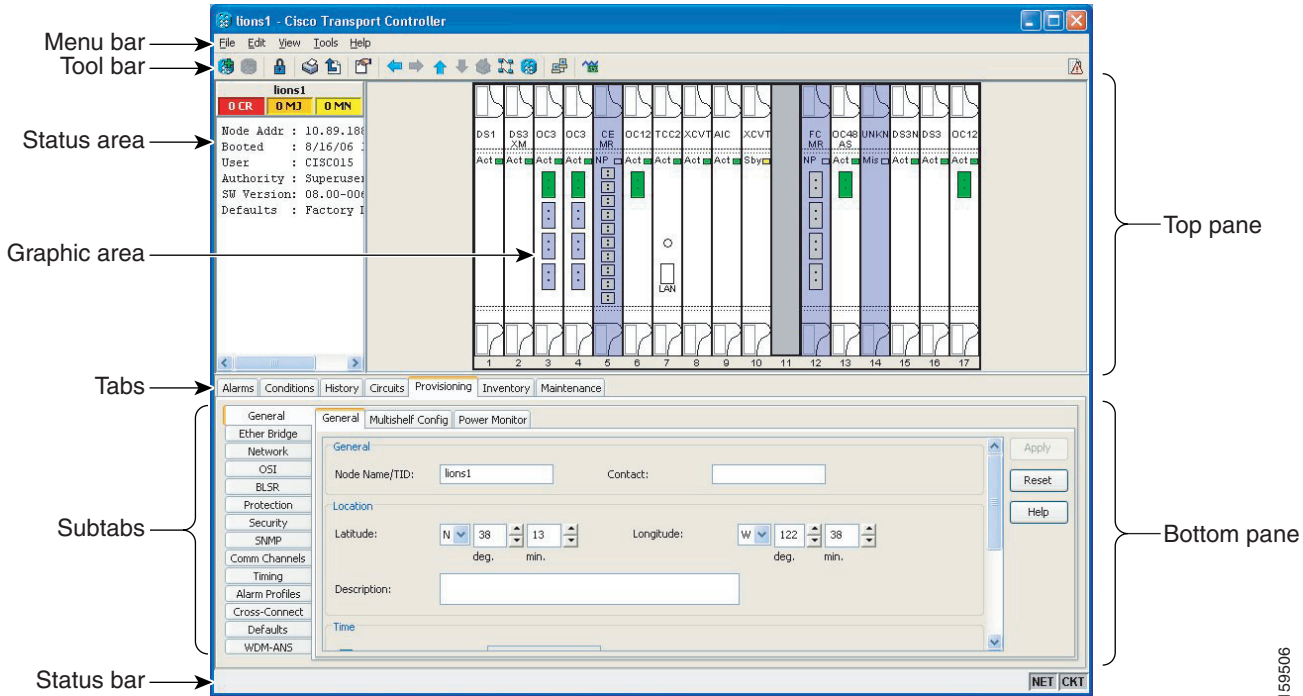
Method	Description	Requirements
Local craft	Refers to onsite network connections between the CTC computer and the ONS 15454 using one of the following: <ul style="list-style-type: none"> • The RJ-45 (LAN) port on the TCC2/TCC2P card • The RJ-45 (LAN) port on the patch panel (multishelf mode) • Port 23 or 24 of the Catalyst 2950 (multishelf mode) • The LAN pins on the ONS 15454 backplane (ANSI) • The RJ-45 jack on the MIC-T/C/P FMEC (ETSI) • 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.	<ul style="list-style-type: none"> • 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 <i>Cisco ONS SONET TL1 Reference Guide</i> or the <i>Cisco ONS 15454 SDH and Cisco ONS 15600 SDH TL1 Reference Guide</i> .
Remote	Refers to a connection made to the ONS 15454 using a modem.	<ul style="list-style-type: none"> • 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.

12.5 CTC Window

When you log into a single-shelf ONS 15454, the CTC window appears in node view (Figure 12-3). When you log into a multishelf ONS 15454, meaning that two or more ONS 15454 shelves are configured to operate as one node, the multishelf view (Figure 12-4) appears in the CTC window. The

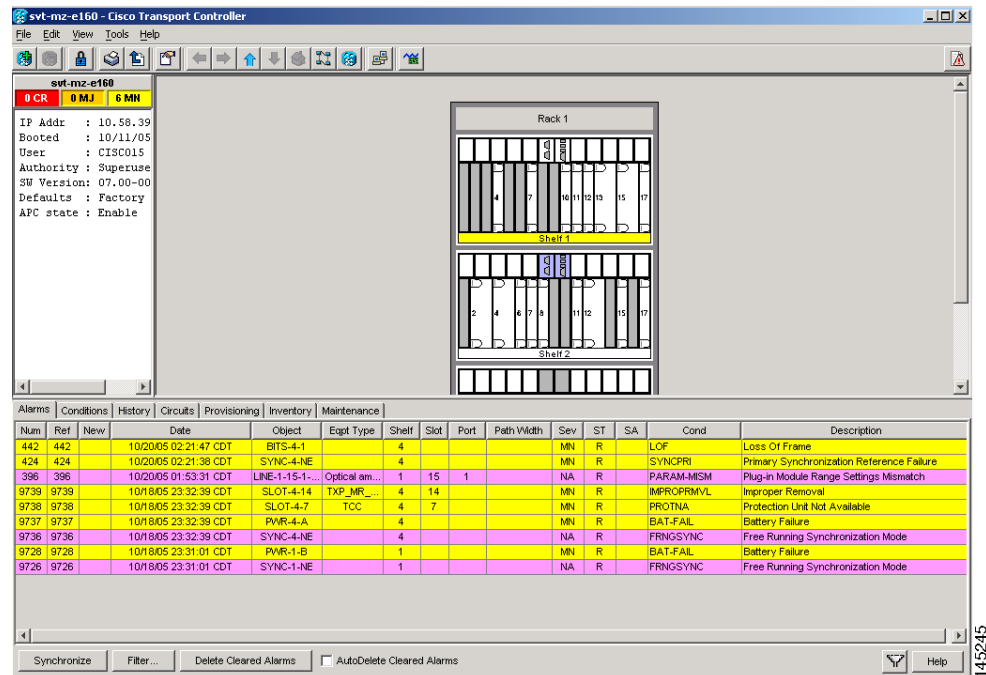
window includes a menu bar, a toolbar, and a top and bottom pane. The top pane provides status information about the selected objects and a graphic of the current view. The bottom pane provides tabs and subtabs to view ONS 15454 information and perform ONS 15454 provisioning and maintenance tasks. From the CTC window, you can display the other ONS 15454 views. In single-shelf mode, these are the network, node, and card views. In multishelf mode, these are the network, multishelf, shelf, and card views.

Figure 12-3 Node View (Default Login View for Single-Shelf Mode)



159506

Figure 12-4 Multishelf View (Default Login View for Multishelf Mode)



12.5.1 Summary Pane

The Summary pane on the left has the following fields:

- Node Addr—IP address of the node.
- Booted—The Booted field indicates one of the following:
 - Date and time of the node reboot. The node reboot is caused by complete power cycle, software upgrade, or software downgrade.
 - Date and time of reset of the control cards one after the other.
- User—Login user name.
- Authority—Security level of users. The possible security levels are Retrieve, Maintenance, Provisioning, and Superuser.
- SW Version—CTC software version.
- Defaults—Name provided to identify the defaults list.

12.5.2 Node View (Multishelf Mode), Node View (Single-Shelf Mode), and Shelf View (Multishelf Mode)

Node view, shown in Figure 12-3, is the first view that appears after you log into a single-shelf ONS 15454. Multishelf view, shown in Figure 12-4, is the first view that appears after you log into a multishelf ONS 15454. The login node is the first node shown, and it is the “home view” for the session. Multishelf view and node view allow 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; name and security level of the current logged-in user; software version; and network element default setup.

In a multishelf mode, up to eight shelves operate as a single node. When you open a shelf from multishelf view, shelf view appears, which looks similar to node view but does not contain the tabs and subtabs that are used for node-level operations.

12.5.2.1 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 12-4](#)).

Table 12-4 *Multishelf View (Multishelf Mode), Node View (Single-Shelf Mode), and Shelf View (Multishelf Mode) 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.

On the ONS 15454 ETSI, the colors of the FMEC cards reflect the real-time status of the physical FMEC cards. [Table 12-5](#) lists the FMEC card colors. The FMEC ports shown in CTC do not change color.



Note

You cannot preprovision FMECs.

Table 12-5 *Multishelf View (Multishelf Mode) and Node View (Single-Shelf Mode) FMEC Color*

Upper Shelf FMEC Color	Status
White	Functioning card is installed.
Yellow	Minor alarm condition exists.
Orange (Amber)	Major alarm condition exists.
Red	Critical alarm exists.

The wording on a card in node view (single-shelf mode) or shelf view (multishelf mode) shows the status of a card (Active, Standby, Loading, or Not Provisioned). [Table 12-6](#) lists the card statuses.

Table 12-6 *Node View (Single-Shelf Mode) or Shelf View (Multishelf Mode) Card Statuses*

Card Status	Description
Act	Card is active.
Sty	Card is in standby mode.

Table 12-6 Node View (Single-Shelf Mode) or Shelf View (Multishelf Mode) Card Statuses

Ldg	Card is resetting.
NP	Card is not present.

Port color in card view, node view (single-shelf mode), and shelf view (multishelf mode) indicates the port service state. [Table 12-7](#) lists the port colors and their service states. For more information about port service states, see [Appendix B, “Administrative and Service States.”](#)

Table 12-7 Node View (Single-Shelf Mode) or Shelf View (Multishelf Mode) Card Port Colors and Service States

Port Color	Service State	Description
Cyan (blue)	Out-of-Service and Management, Loopback (OOS-MA,LPBK) (ANSI) Locked-enabled,loopback (ETSI)	Port is in a loopback state. On the card in node or shelf view, a line between ports indicates that the port is in terminal or facility loopback (see Figure 12-5 and Figure 12-6). 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.
Cyan (blue)	Out-of-Service and Management, Maintenance (OOS-MA,MT) (ANSI) Locked-enabled,maintenance (ETSI)	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 this service state for testing or to suppress alarms temporarily. Change the state to IS-NR/Unlocked-enabled; OOS-MA,DSBLD/Locked-enabled,disabled; or OOS-AU,AINS/Unlocked-disabled,automaticInService when testing is complete.
Gray	Out-of-Service and Management, Disabled (OOS-MA,DSBLD) (ANSI) Locked-enabled,disabled (ETSI)	The port is out-of-service and unable to carry traffic. Loopbacks are not allowed in this service state.
Green	In-Service and Normal (IS-NR) (ANSI) Unlocked-enabled (ETSI)	The port is fully operational and performing as provisioned. The port transmits a signal and displays alarms; loopbacks are not allowed.
Violet	Out-of-Service and Autonomous, Automatic In-Service (OOS-AU,AINS) (ANSI) Unlocked-disabled,automaticInService (ETSI)	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 this service state for the duration of the soak period. After the soak period ends, the port service state changes to IS-NR/Unlocked-enabled. 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/Unlocked-enabled when a signal is received for the length of time provisioned in the soak field.

Figure 12-5 Terminal Loopback Indicator**Figure 12-6 Facility Loopback Indicator**

12.5.2.2 Multishelf View Card Shortcuts

If you move your mouse over cards in the multishelf view 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); the alarm profile used by the card; and for transponder (TXP) or muxponder (MXP) cards, the wavelength of the dense wavelength division multiplexing (DWDM) port.

12.5.2.3 Node View (Single-Shelf Mode) or Shelf View (Multishelf Mode) Card Shortcuts

If you move your mouse over cards in the node view (single-shelf mode) or shelf view (multishelf mode) 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); the alarm profile used by the card; and for TXP or MXP cards, the wavelength of the DWDM port. 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).

12.5.2.4 Multishelf View Tabs

Table 12-8 lists the tabs and subtabs available in the multishelf view. The actions on these tabs apply to the multishelf node and its subtending shelves.

Table 12-8 Multishelf View Tabs and Subtabs

Tab	Description	Subtabs
Alarms	Lists current alarms (CR, MJ, MN) for the multishelf node and updates them in real time.	—
Conditions	Displays a list of standing conditions on the multishelf node.	—
History	Provides a history of multishelf node alarms including the 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	Creates, deletes, edits, and maps circuits.	Circuits, Rolls
Provisioning	Provisions the ONS 15454 multishelf node.	General, Network, OSI, Security, SNMP, Comm Channels, Alarm Profiles, Defaults, WDM-ANS

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

Tab	Description	Subtabs
Inventory	Provides inventory information (part number, serial number, and Common Language Equipment Identification [CLEI] codes) for cards installed on all shelves in the multishelf node. Allows you to delete and reset cards and change the card service state.	—
Maintenance	Performs maintenance tasks for the multishelf node.	Database, Network, OSI, Software, Diagnostic, Audit, DWDM

12.5.2.5 Node View (Single-Shelf Mode) or Shelf View (Multishelf Mode) Tabs

Table 12-9 lists the tabs and subtabs available in node view (single-shelf mode) or shelf view (multishelf mode).

Table 12-9 Node View (Single-Shelf Mode) or Shelf View (Multishelf Mode) Tabs and Subtabs

Tab	Description	Subtabs
Alarms	Lists current alarms (CR, MJ, MN) for the node or shelf and updates them in real time.	—
Conditions	Displays a list of standing conditions on the node or shelf.	—
History	Provides a history of node or shelf alarms including the 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	Creates, deletes, edits, and maps circuits.	Circuits, Rolls
Provisioning	Provisions the ONS 15454 single-shelf or multishelf node.	Single-shelf mode: General, Network, OSI, Security, SNMP, Comm Channels, Alarm Profiles, Defaults, WDM-ANS Multishelf mode: General, Protection, Timing, Alarm Profiles

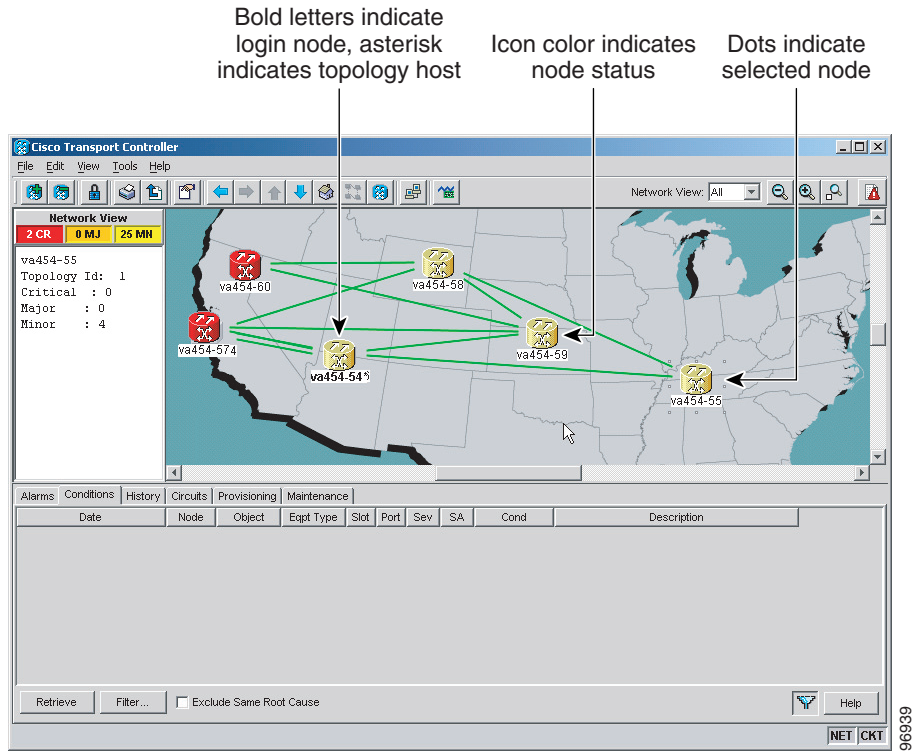
Table 12-9 Node View (Single-Shelf Mode) or Shelf View (Multishelf Mode) Tabs and Subtabs

Tab	Description	Subtabs
Inventory	<p>Provides inventory information (part number, serial number, and CLEI codes) for cards installed in the single-shelf or multishelf node. Allows you to delete and reset cards and change the card service state.</p> <p>Note Each card has bootstrap and boot code. After the card is upgraded using the boot code upgrade procedure, the bootstrap version is displayed in the Inventory tab in CTC; However, the boot code version is not displayed in the Inventory tab.</p>	—
Maintenance	Performs maintenance tasks for the single-shelf or multishelf node.	<p>Single-shelf mode: Database, Network, OSI, Software, Diagnostic, Audit, DWDM</p> <p>Multishelf mode: Protection, Overhead XConnect, Diagnostic, Timing</p>

12.5.3 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 12-7).

Figure 12-7 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.

12.5.3.1 Network View Tabs

Table 12-10 lists the tabs and subtabs available in network view.

Table 12-10 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.	—

Table 12-10 Network View Tabs and Subtabs (continued)

Tab	Description	Subtabs
Provisioning	Provisions security, alarm profiles, bidirectional line switched rings (BLSRs) (ANSI), multiplex section-shared protection rings (MS-SPRing) (ETSI), and overhead circuits.	Security, Alarm Profiles, BLSR (ANSI), MS-SPRing (ETSI), Overhead Circuits, Provisionable Patchcords
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

12.5.3.2 CTC Node Colors

The color of a node in network view, shown in [Table 12-11](#), indicates the node alarm status.

Table 12-11 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)

12.5.3.3 DCC Links

The lines show DCC connections between the nodes ([Table 12-12](#)). 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. Selecting a node or span in the graphic area displays information about the node and span in the status area.

Table 12-12 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

12.5.3.4 Link Consolidation

CTC provides the ability to consolidate the DCC, generic communications channel (GCC), optical transmission section (OTS), and PPC links shown in the network view into a more streamlined view. Link consolidation allows you to condense multiple inter-nodal links into a single link. The link

consolidation sorts links by class, meaning that all DCC links are consolidated together, for example. You can access individual links within consolidated links using the right-click shortcut menu. Each link has an associated icon (Table 12-13).

Table 12-13 Link Icons

Icon	Description
	DCC icon
	GCC icon
	OTS icon
	PPC icon



Note

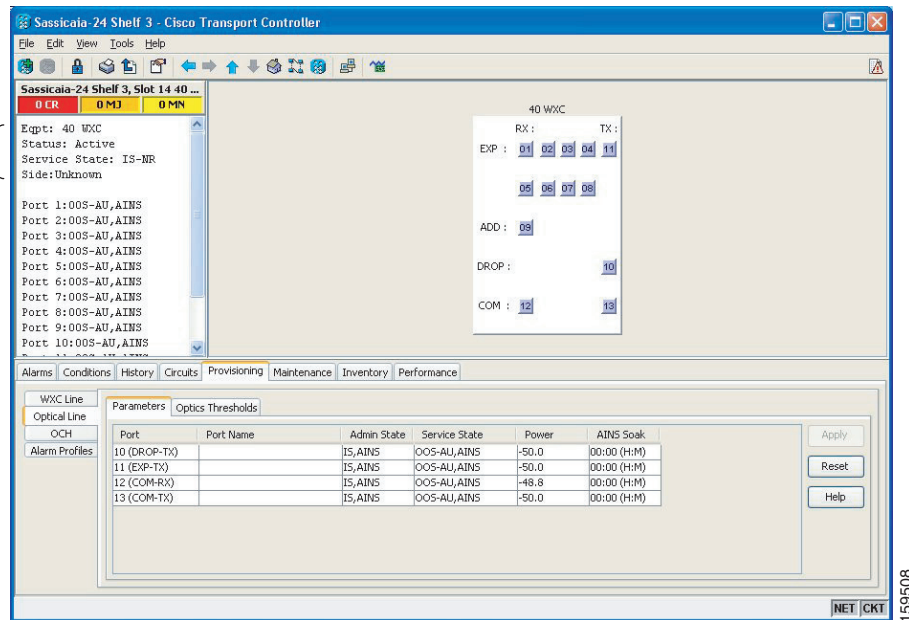
Link consolidation is only available on non-detailed maps. Non-detailed maps display nodes in icon form instead of detailed form, meaning that the nodes appear as rectangles with ports on the sides. Refer to the *Cisco ONS 15454 DWDM Procedure Guide* for more information about consolidated links.

12.5.4 Card View

The card view provides information about individual ONS 15454 cards. Use this window to perform card-specific maintenance and provisioning (Figure 12-8). 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, card status (active or standby), card service state if the card is present, and port service state (described in Table 12-7 on page 12-11). The information that appears and the actions that you can perform depend on the card. For more information about card service states, refer to Appendix B, “Administrative and Service States.”

Figure 12-8 CTC Card View Showing a 40-WXC-C Card

Card identification and status

**Note**

CTC provides a card view for all ONS 15454 cards except the TCC2/TCC2P card.

Use the card view tabs and subtabs shown in Table 12-14 to provision and manage the ONS 15454. The subtabs, fields, and information shown under each tab depend on the card type selected.

Table 12-14 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.	—

Table 12-14 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 DS-N and OC-N cards), Elect Path Thresholds, SONET Thresholds, SONET STS, Alarm Profiles TXP and MXP cards: Card, Line, Line Thresholds, Optics Thresholds, OTN, Alarm Profiles DWDM cards (subtabs depend on card type): Optical Line, Optical Chn, Optical Amplifier, Parameters, Optics Thresholds, Alarm Profiles
Maintenance	Performs maintenance tasks for the card.	Loopback, Info, Protection, J1 Path Trace, AINS Soak (options depend on the card type), Automatic Laser Shutdown
Performance (Not available for the AIC-I cards)	Performs performance monitoring for the card.	DS-N and OC-N cards: no subtabs TXP and MXP cards: Optics PM, Payload PM, OTN PM DWDM cards (subtabs depend on card type): Optical Line, Optical Chn, Optical Amplifier Line, OC3 Line, Parameters, Optics Thresholds
Inventory	(40-WSS, 40-WXC, OPT-PRE and OPT-BST cards) Displays an Inventory screen of the ports.	—

12.6 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. The CTC launcher application provides an advantage particularly when you have more than one NE version on the network, because it allows you to pick from all available CTC software versions. It also starts more quickly than the browser version of CTC and has a dedicated node history list.

CTC Launcher provides two connection options. The first option is used to connect to ONS 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 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 12-9 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 vendor, 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 12-9 Static IP-Over-CLNS Tunnels

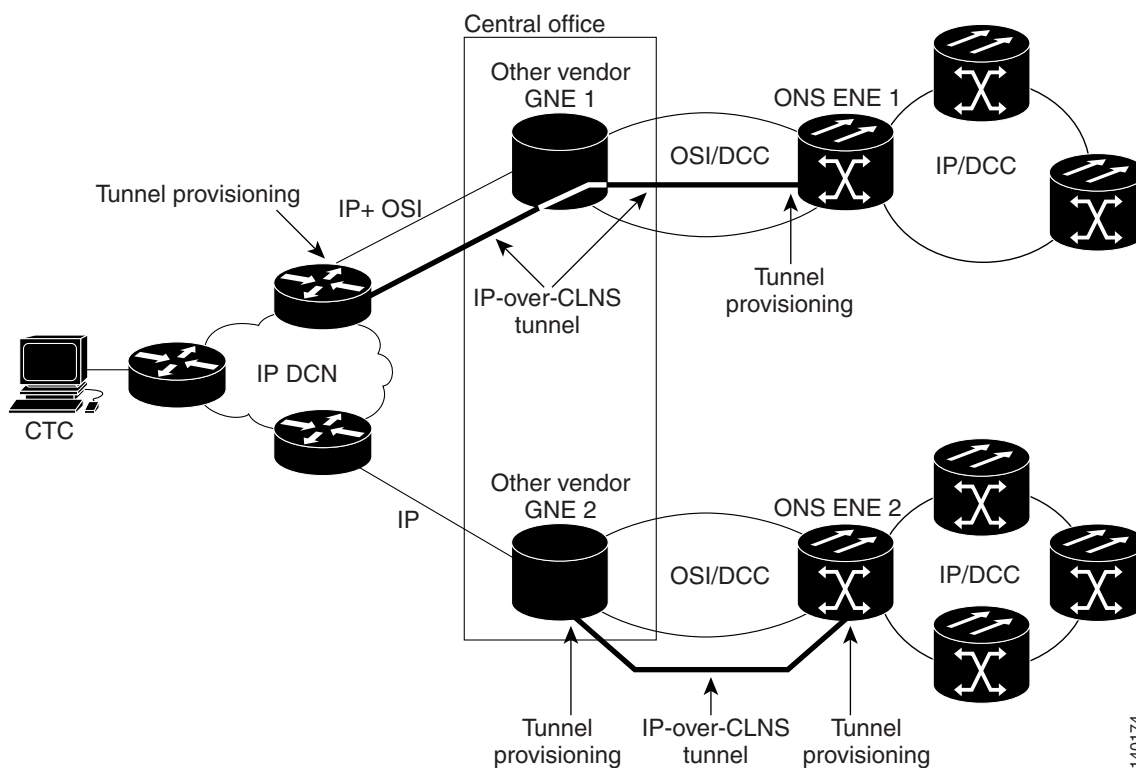
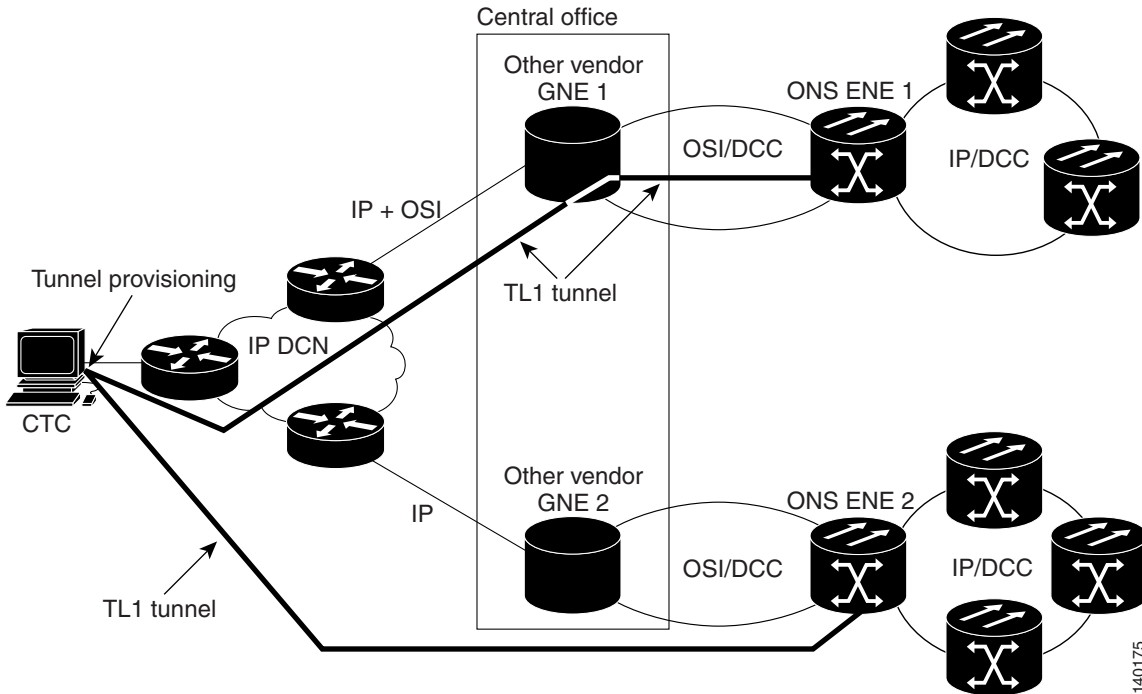


Figure 12-10 shows the same network using TL1 tunnels. Tunnel provisioning occurs at the CTC computer when the tunnel is created with the CTC Launcher. No provisioning is needed at ONS NEs, GNEs, or routers.

Figure 12-10 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 12-15 shows a comparison between the two types of tunnels.

Table 12-15 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 12-15 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.

12.7 TCC2/TCC2P Card Reset

You can reset the ONS 15454 TCC2/TCC2P card by using CTC (a soft reset) or by physically reseating the 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 card goes through an initialization process and also resets because it is controlled by the active TCC2/TCC2P card.

12.8 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.

**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.

12.9 Software Revert

When you click the Activate button after a software upgrade, the TCC2/TCC2P card copies the current working database and saves it in a reserved location in the TCC2/TCC2P card flash memory. If later during the upgrade you 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.

The revert feature is useful if the maintenance window in which you were performing an upgrade closes while you are still upgrading CTC software. You can revert to the protect software load without losing traffic. During the next maintenance window, you can complete the upgrade and activate the new software load.

Circuits created or provisioning done after you activate a new software load (upgrade to a higher 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, such as Software R5.0.1 to Software R5.0.2, because maintenance releases retain the database during activation.)

**Caution**

Cisco does not recommend reverting after changing provisioning on the node. Depending upon the particular provisioning, reverting in this case can be traffic affecting.

To perform a supported (non-service-affecting) revert from a software release that you have just activated, the release you revert to must have been working at the time you first activated the new software 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 the software release that you are upgrading to 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 will reset, but will not be traffic affecting and will not change your database).

**Note**

To perform a supported software upgrade or revert, you must consult the specific upgrade document and release notes for the release you are upgrading to (or reverting from).

