



StartCTC Application Guide

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

StartCTC 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, StartCTC creates a TL1 tunnel to transport the TCP traffic through the OSI-based GNE.

This application guide tells you how to:

- Install the program.
- Use StartCTC to start a CTC session to an ONS NE that has an IP connection to the CTC computer.
- Create TL1 tunnels to connect to ONS NEs on the other side of third-party, OSI-based GNEs.
- View and manage TL1 tunnels using CTC.

Install the StartCTC Application

Use the following steps to install the StartCTC application to your computer.

Step 1 Installation of Java 5 JRE is required for StartCTC.exe to run. If JRE 5 has been already installed, skip to [Step 3](#). Otherwise, proceed as follows:



Note

The Java 5 installer for Windows can be downloaded from this location:

http://java.sun.com/javase/downloads/index_jdk5.jsp. Select "Java Runtime Environment (JRE) 5.0 Update xx" (xx= latest revision number) from that page.

- When you install the JRE you can decide to install the java plug-ins or not. If your browsers are used to launch older versions of CTC which require certain versions of Java plug-ins, it is not recommended to install the Java 5 plug-ins (unless this plug-in version is required for other purposes).
-



Corporate Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2007 Cisco Systems, Inc. All rights reserved.

- Step 2** Make sure to select the Custom installation (not the Typical installation) and unselect any browser from the list in the Java plug-ins installation step.
- Step 3** Insert the Cisco ONS Software Release 8.0 CD into your CD drive.
- Step 4** Navigate to the CtcLauncher directory.
- Step 5** Copy the StartCTC.exe file to your local hard drive. Any location that is convenient for you to access, such as the Windows desktop, may be used.
- Stop. You have completed this procedure.**
-

Using StartCTC

You can use StartCTC to connect to ONS NEs that have an IP connection to the CTC computer without using a web browser. To use this connection option, the following prerequisites must be met:

- The StartCTC application file, StartCTC.exe, must be copied from the ONS software CD to the CTC computer. (See the [“Install the StartCTC Application” task on page 1.](#))
- The ONS NEs must be running CTC Software Release 3.3 or higher.
- The CTC Software Release 8.0 Java Archive (JAR) files must be on the CTC computer. CTC JAR files are downloaded to your computer when one of the following occurs:
 - You connect to a Software R8.0 NE using a web browser.
 - You use the LDCACHE utility on a Software R8.0 software CD to copy the JAR files to the CTC computer.

Connect to ONS NEs with an IP Connection

Use the following steps to connect to an ONS NE that has an IP connection to the CTC computer. Before you begin, verify the following:

- The ONS NE is running CTC Software R3.3 or higher.
- The CTC Software Release 8.0 JAR files have been downloaded to your CTC computer through one of the following:
 - You connected to a Software R8.0 NE using a web browser.
 - You used the LDCACHE utility on a Software R8.0 CD to copy the JAR files to the CTC computer.

-
- Step 1** If the StartCTC application has not been installed, complete the [“Install the StartCTC Application” task on page 1.](#) Otherwise, continue with [Step 4.](#)
- Step 2** Navigate to the directory containing the StartCTC.exe file and double-click it. (You can also use the Windows Start menu Run command.)
- Step 3** Enter the IP address of the desired ONS NE node in the **Use IP Node** under Connection Mode. (If the address was entered previously, you can choose it from the drop-down list.)
- Step 4** If the NE node that you are connecting to is using a different software version than 8.0, select the version in the **CTC Version Selection** dialog box. It is recommended to always use the Same version as the login node" unless the use of newer CTC versions is desired.



Note To connect to a CTC NE running a different software version than 8.0 see the [“Customization” section on page 4](#)

Step 5 Click **Launch CTC...** After the connection is made, the CTC Login dialog box appears.

Step 6 Log into the ONS NE. Refer to the ONS NE user documentation for login procedures.

Stop. You have completed this procedure.

Connect to ONS NEs with a TL1 Tunnel

Use the following steps to create a TL1 tunnel and log into an ONS NE.

- Step 1** If the StartCTC.exe file is located on your computer hard drive, continue with [Step 2](#). If not, complete the [“Install the StartCTC Application” task on page 1](#).
- Step 2** Double-click the StartCTC.exe file.
- Step 3** Click the TL1 Tunnel radio button.
- Step 4** Enter the following in the dialog box that appears:
- **Far End TID**—Enter the TID of the ONS ENE at the far end of the tunnel. The ENE must be a Cisco ONS 15454, Cisco ONS 15454 SDH, Cisco ONS 15327, or Cisco ONS 15310-CL running CTC Software Release 6.0. The TID is the name entered in the Node Name field on the node view Provisioning > General tab.
 - **Host Name/IP Address**—Enter the DNS host name or the IP address of the GNE through which the tunnel will established. This is the third-party vender GNE that is connected to an ONS 15454, ONS 15454 SDH, ONS 15327, or ONS 15310-CL through an OSI DCC network. CTC uses TCP/IP over a DCN to reach the GNE. The GNE accepts TL1 connections from the network and can forward TL1 traffic to the ENes.
 - **Choose a port option:**
 - **Use Default TL1 Port**—Choose this option if you want to use the default TL1 Port 3081 or 3082.
 - **Use Other TL1 Port**—Choose this option if the GNE uses a different TL1 port. Enter the port number in the box next to the User Other TL1 Port radio button.
 - **TL1 Encoding Mode**—Choose the TL1 encoding:
 - **LV + Binary Payload**— TL1 messages are delimited by length value (LV) headers and TCP traffic is encapsulated in binary form. Cisco recommends this option because it is the most efficient encoding mode. However, you must verify that the GNE supports LV + Binary Payload encoding.
 - **LV + Base64 Payload**—TL1 messages are delimited by LV headers and TCP traffic is encapsulated using Base64 encoding.
 - **Raw**—TL1 messages are delimited by semicolons only, and the TCP traffic is encapsulated using Base64 encoding.
 - **GNE Login Required**—Check this box if the GNE requires a a local TL1 ACT-USER login before forwarding TL1 traffic to ENes.

- TID—If the GNE Login Required box is checked, enter the GNE TID.

Step 5 Click **OK**.

Step 6 If the GNE Login Required box is checked, complete the following steps. If not, continue with [Step 7](#).

- In the Login to Gateway NE dialog box UID field, enter the TL1 user name.
- In the PID field, enter the TL1 user password.
- Click **OK**.

Step 7 When the CTC Login dialog box appears, complete the CTC login. Refer to login procedures in the user documentation for the ONS ENE.

Stop. You have completed this procedure.

Customization

The StartCTC.exe program accepts optional launching arguments. The normal way to start CtcLauncher is without arguments.

The following arguments can be passed on the command line in order to skip the StartCTC window and directly launch CTC on a given node with a given CTC version :

```
-latest nodename
-sameasnode nodename
nodename
```

For example to start CTC on node 10.1.1.28 and use the same version of CTC as the login node:

```
StartCTC.exe -sameasnode 10.1.1.28
```

To start the latest version of CTC available on node "star17" (-latest is the default CT version selection mode) :

```
StartCTC.exe -latest star17
```

Using these launching arguments, it is possible in Windows to create shortcuts to the StartCTC.exe program and assign parameters to the shortcut. For example, to create an icon to start CTC on node "vikings4" using the same version of CTC as that node (assuming that StartCTC.exe has been installed on the Desktop), you would proceed as follows:

Step 1 Right-click the StartCTC.exe icon on the Desktop.

Step 2 Click **Create Shortcut** to create a shortcut icon.

Step 3 Right click the shortcut icon and click **Properties**.

Step 4 You can change the name of the shortcut to **vikings4**, for example in the General tab,

Step 5 in the **Target** field of the Shortcut tab, add the parameters to the program name.

Step 6 Click **OK**.

You can create any number of shortcuts using the above procedure, for different node names or version selection modes.

Previous CTC Versions

StartCTC can launch multiple CTC versions. Because each CTC version requires a particular JRE version, StartCTC asks you for the location of a suitable JRE whenever a new CTC version is launched for the first time. That JRE information then persists in your preferences file.

When StartCTC needs to use a new JRE, a dialog box appears, from which you can select any appropriate JRE directory; for example, the JRE installation directory or its bin directory.

After the JRE version is selected, the CTC is launched. The required jar files are downloaded into the new cache if they are missing.

The Settings button in the StartCTC window lets you delete the cache containing all CTC versions or specify a different cache directory. The default cache directory is located in the your home directory, under the %HOME%\Application Data\Cisco\CTC directory. Deleting the cache via the Settings dialog deletes only the cached files from the new cache directory (used by StartCTC). It does not delete cache files used by the CTC Applets for versions 3.30 to 7.X. Note that this new cache is completely separate and independent from the older CTC cache (which resides in your system temporary directory), so deleting the new cache does not impact jar files saved in the old cache. The old cache can still be used when launching CTC directly from the browser.

TL1 Tunnels

StartCTC can be used to connect to ONS NEs residing behind OSI-based, third-party GNEs. To do this, StartCTC creates a TL1 tunnel, and the tunnel transports the TCP traffic to and from ONS end network elements (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-Connectionless Network Service (CLNS) tunnels. However, unlike the static IP-over-CLNS tunnels, TL1 tunnels require no provisioning at the ONS ENE, the third-party GNE, or data communications network (DCN) routers. All provisioning occurs at the CTC computer when StartCTC is started.

[Figure 1](#) shows examples of two static IP-over-CLNS tunnels. A static Cisco IP tunnel is created from ENE 1 through the 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 1 Static IP-Over-CLNS Tunnels

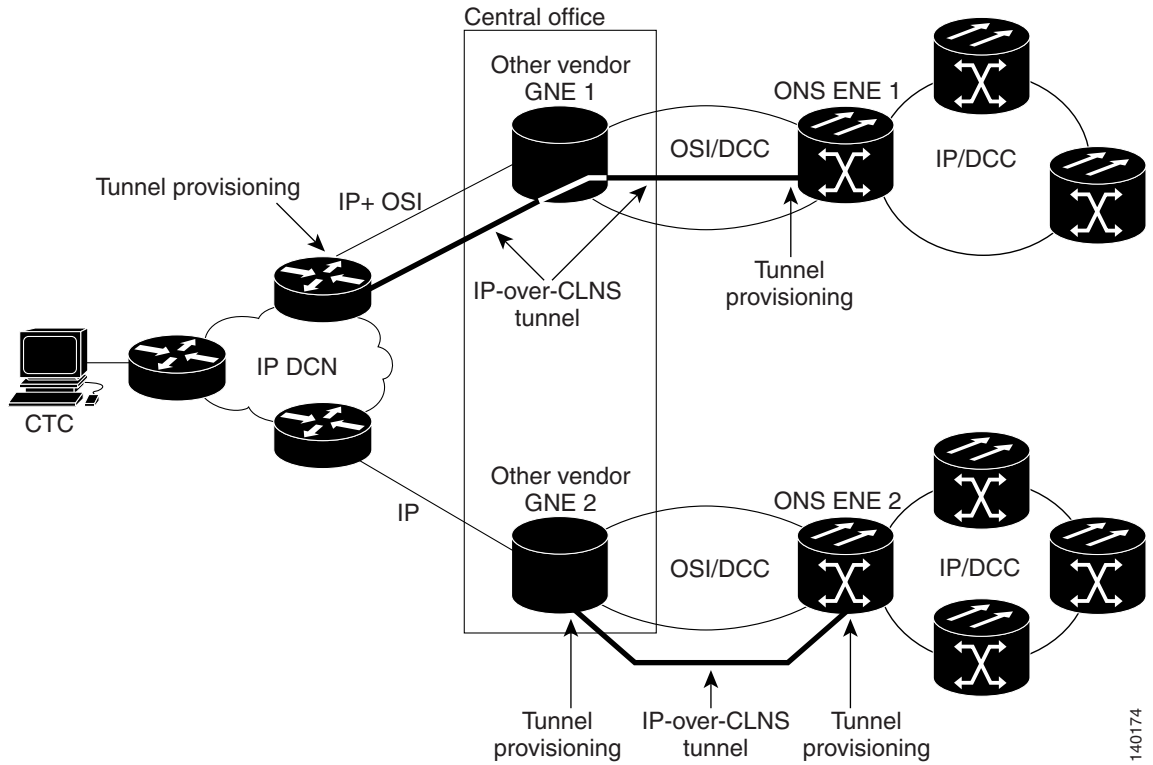
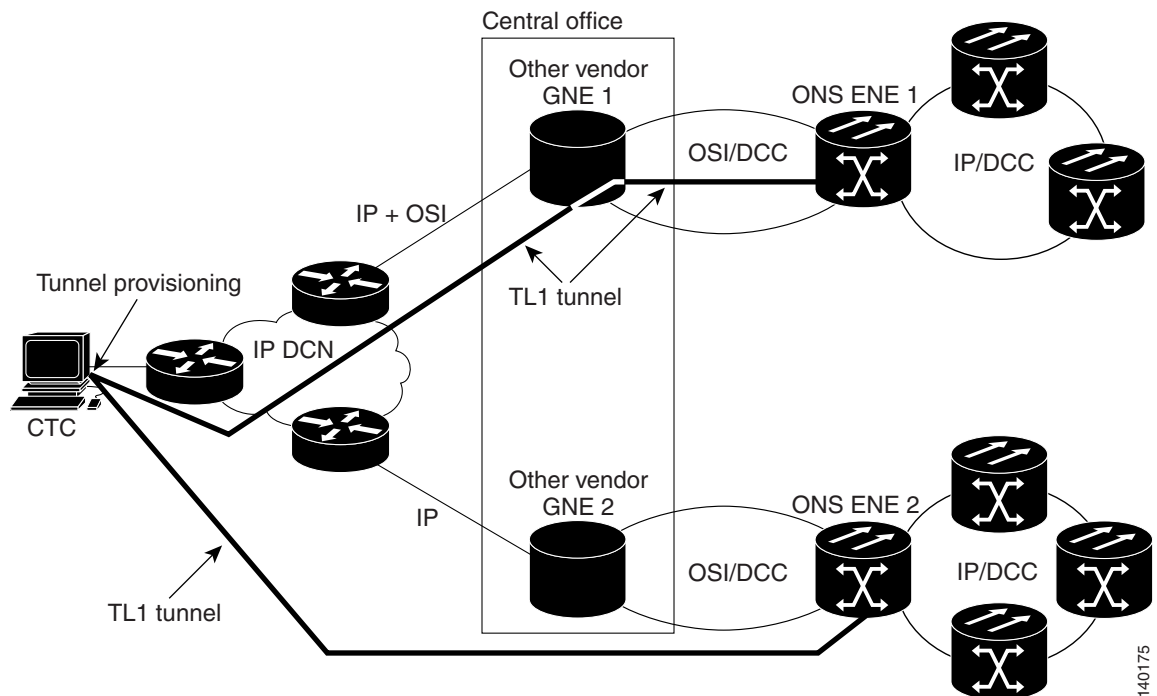


Figure 2 shows the same network using TL1 tunnels. Tunnel provisioning occurs at the CTC computer when the tunnel is created with StartCTC. No provisioning is needed at ONS NEs, GNEs, or routers.

Figure 2 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 Simple Network Management Protocol (SNMP) and Remote Authentication Dial In User Service (RADIUS). Table 1 shows a comparison between the two types of tunnels.

Table 1 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 1 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 session duration	Fixed	CTC session	TL1 tunnel sessions terminate when the CTC session ends. Static IP-over-CLNS tunnels remain up until they are deleted.

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.
- TL1 tunnels attempt to reconnect automatically after a tunnel goes down.
- Each ONS NE can support at least 16 concurrent tunnels.

View TL1 Tunnel Information

Use the following steps to view TL1 tunnel information.

- Step 1** Log into an ONS node using either the [“Connect to ONS NEs with a TL1 Tunnel” procedure on page 3](#) or login procedures provided in the ONS user documentation.
- Step 2** From the Tools menu, choose **Manage TL1 Tunnels**.
- Step 3** In the TL1 Tunnels window, view the information shown in [Table 2](#).

Table 2 TL1 Tunnels Window

Item	Description
Far End TID	The Target ID of the NE at the far end of the tunnel. This NE is an ONS 15454, ONS 15454 SDH, ONS 15327, or ONS 15310-CL. (The far-end NEs must run CTC Software R6.0.) It is typically connected with an OSI DCC to a third-party vender GNE. CTC manages this NE.
GNE Host	The GNE host or IP address through which the tunnel is established. This is generally a third-party vender GNE that is connected to an ONS 15454, ONS 15454, ONS 15327, or ONS 15310-CL with an OSI DCC. CTC uses TCP/IP over a DCN to reach the GNE. The GNE accepts TL1 connections from the network and can forward TL1 traffic to the ENEs.
Port	The TCP port number where the GNE accepts TL1 connections coming from the DCN. These port numbers are standard (such as 3081 and 3082) unless custom port numbers are provisioned on the GNE.

Table 2 TL1 Tunnels Window (Continued)

Item	Description
TL1 Encoding	<p>Defines the TL1 encoding used for the tunnel:</p> <ul style="list-style-type: none"> • LV + Binary Payload—TL1 messages are delimited by an LV header. TCP traffic is encapsulated in binary form. • LV + Base64 Payload—TL1 messages are delimited by an LV header. TCP traffic is encapsulated using the base 64 encoding. • Raw—TL1 messages are delimited by semicolons only, and the TCP traffic is encapsulated using Base64 encoding.
GNE TID	The GNE TID is shown when the GNE requires a local TL1 ACT-USER login before forwarding TL1 traffic to ENEs. If present, CTC asks the user for the ACT-USER user ID and password when the tunnel is opened.
State	<p>Indicates the tunnel state:</p> <ul style="list-style-type: none"> • OPEN—A tunnel is currently open and carrying TCP traffic. • RETRY PENDING—The TL1 connection carrying the tunnel has been disconnected and a retry to reconnect it is pending. (CTC automatically attempts to reconnect the tunnel at regular intervals. During that time all ENEs behind the tunnel are unreachable.) • (empty)—No tunnel is currently open.
Far End IP	The IP address of the ONS NE that is at the far end of the TL1 tunnel. This information is retrieved from the NE when the tunnel is established.
Sockets	The number of active TCP sockets that are multiplexed in the tunnel. This information is automatically updated in real time.
Retries	Indicates the number of times CTC tried to reopen a tunnel. If a network problem causes a tunnel to go down, CTC automatically tries to reopen it at regular intervals. This information is automatically updated in real time.
Rx Bytes	Shows the number of bytes of management traffic that were received over the tunnel. This information is automatically updated in real time.
Tx Bytes	Shows the number of bytes of management traffic that were transmitted over the tunnel. This information is automatically updated in real time.

Stop. You have completed this procedure.

Create a TL1 Tunnel Using CTC

Use the following steps to create a TL1 tunnel using CTC.

- Step 1** Log into an ONS node using the [“Connect to ONS NEs with a TL1 Tunnel” procedure on page 3.](#)
- Step 2** From the Tools menu, choose **Manage TL1 Tunnels**.
- Step 3** In the TL1 Tunnels window, click **Create**.

- Step 4** In the Create CTC TL1 Tunnel dialog box, enter the following:
- **Far End TID**—Enter the TID of the ONS ENE at the far end of the tunnel. The ENE must be a Cisco ONS 15454, Cisco ONS15454 SDH, Cisco ONS 15327, or Cisco ONS 15310-CL running CTC Software R6.0. The TID is the name entered in the Node Name field on the node view Provisioning > General tab.
 - **Host Name/IP Address**—Enter the GNE DNS host name or IP address through which the tunnel will be established. This is the third-party vendor GNE that is connected to an ONS 15454, ONS 15454 SDH, ONS 15327, or ONS 15310-CL with an OSI DCC. CTC uses TCP/IP over a DCN to reach the GNE. The GNE accepts TL1 connections from the network and can forward TL1 traffic to the ENEs.
 - Choose a port option:
 - **Use Default TL1 Port**—Choose this option if you want to use the GNE default TL1 port. TL1 uses standard ports, such as 3081 and 3082, unless custom TL1 ports are defined.
 - **Use Other TL1 Port**—Choose this option if the GNE uses a different TL1 port. Enter the port number in the box next to the User Other TL1 Port radio button.
 - **TL1 Encoding Mode**—Choose the TL1 encoding:
 - **LV + Binary Payload**—TL1 messages are delimited by LV headers and TCP traffic is encapsulated in binary form. Cisco recommends this option because it is the most efficient. However, you must verify that the GNE supports LV + Binary Payload encoding.
 - **LV + Base64 Payload**—TL1 messages are delimited by LV headers and TCP traffic is encapsulated using Base64 encoding.
 - **Raw**—TL1 messages are delimited by semicolons only, and the TCP traffic is encapsulated using Base64 encoding.
 - **GNE Login Required**—Check this box if the GNE requires a local TL1 ACT-USER login before forwarding TL1 traffic to ENEs.
 - **TID**—If the GNE Login Required box is checked, enter the GNE TID.
- Step 5** Click **OK**.
- Step 6** If the GNE Login Required box is checked, complete the following steps. If not, continue [Step 7](#).
- a. In the Login to Gateway NE dialog box UID field, enter the TL1 user name.
 - b. In the PID field, enter the TL1 user password.
 - c. Click **OK**.
- Step 7** After the CTC Login dialog box appears, complete the CTC login. Refer to login procedures in the user documentation for the ONS ENE.
- Stop. You have completed this procedure.**
-

Edit a TL1 Tunnel

Use the following steps to edit a TL1 tunnel using CTC.

- Step 1** Login into an ONS node using the [“Connect to ONS NEs with a TL1 Tunnel” procedure on page 3](#).
- Step 2** From the Tools menu, choose **Manage TL1 Tunnels**.

- Step 3** In the TL1 Tunnels window, click the tunnel that you want to edit.
- Step 4** Click **Edit**.
- Step 5** In the Edit CTC TL1 Tunnel dialog box, edit the following:
- Use Default TL1 Port—Choose this option if you want to use the GNE default TL1 port. TL1 uses standard ports, such as 3081 and 3082, unless custom TL1 ports are defined.
 - Use Other TL1 Port—Choose this option if the GNE uses a different TL1 port. Enter the port number in the box next to the User Other TL1 Port radio button.
 - TL1 Encoding Mode—Choose the TL1 encoding:
 - **LV + Binary Payload**—TL1 messages are delimited by LV headers and TCP traffic is encapsulated in binary form. Cisco recommends this option because it is the most efficient. However, you must verify that the GNE supports LV + Binary Payload encoding.
 - **LV + Base64 Payload**—TL1 messages are delimited by LV headers and TCP traffic is encapsulated using Base64 encoding.
 - **Raw**—TL1 messages are delimited by semicolons only, and the TCP traffic is encapsulated using Base64 encoding.
 - GNE Login Required—Check this box if the GNE requires a local TL1 ACT-USER login before forwarding TL1 traffic to ENEs.
 - TID—If the GNE Login Required box is checked, enter the GNE TID.
- Step 6** Click **OK**.
- Step 7** If the GNE Login Required box is checked, complete login in the Login to Gateway NE dialog box. If not, continue [Step 8](#).
- a. In the UID field, enter the TL1 user name.
 - b. In the PID field, enter the TL1 user password.
 - c. Click **OK**.
- Step 8** When the CTC Login dialog box appears, complete the CTC login. Refer to login procedures in the user documentation for the ONS ENE.
- Stop. You have completed this procedure.**
-

Delete a TL1 Tunnel

Use the following steps to delete a TL1 tunnel.

- Step 1** Login into an ONS node using the [“Connect to ONS NEs with a TL1 Tunnel” procedure on page 3](#).
- Step 2** From the Tools menu, choose **Manage TL1 Tunnels**.
- Step 3** In the TL1 Tunnels window, click the tunnel that you want to delete.
- Step 4** Click **Delete**.
- Step 5** In the confirmation dialog box, click **OK**.
- Stop. You have completed this procedure.**
-

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/en/US/support/tsd_documentation.html

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

Cisco Marketplace:

<http://www.cisco.com/go/marketplace/>

Cisco Optical Networking Product Documentation CD-ROM

Optical networking-related documentation, including Cisco ONS 15xxx product documentation, is available in a CD-ROM package that ships with your product. The Optical Networking Product Documentation CD-ROM is updated periodically and may be more current than printed documentation.

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

<http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on>

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>



Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

<http://www.cisco.com/ipj>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0612R)

Copyright © 2007 Cisco Systems, Inc. All rights reserved.