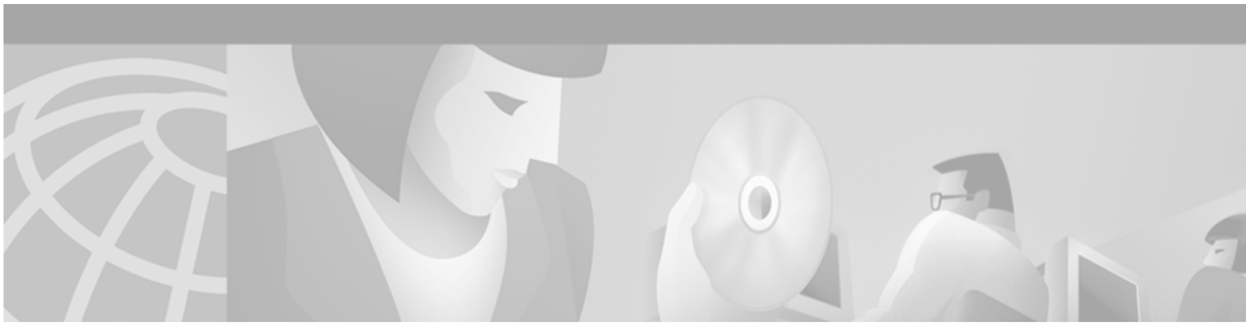


Cisco Content Transformation Engine 1400 Series Configuration Note Release 2.5

Product Number: CTE-1400

This publication contains the procedures for configuring the Cisco Content Transformation Engine 1400 Series (CTE).

For information on installing the CTE, refer to the *Cisco CTE 1400 Hardware Installation Guide*.

Note Throughout this publication, the *Cisco CTE 1400 Series* is referred to as the *CTE*.

Contents

This publication consists of these sections:

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

Important Security Information

Improper configuration of the CTE can result in a security risk. Before you deploy the CTE, verify that the CTE does not have access to protected intranet sites.

By default, the CTE proxies only the web pages that it has identified (transcoded in Design Studio) to prevent access to protected servers that are on the same subnet as the CTE. If you choose to override that default, do not put the CTE on the same subnet as the protected servers.

Note If you configure the CTE to proxy all web pages, the CTE provides access to computers on the same subnet as the web servers that are configured to work with the CTE. For example, suppose a CTE has an external IP address of 24.221.1.1 and an internal IP address of 192.168.1.31. On the same subnet, you have an intranet server, protected from outside access, with an IP address of 192.168.1.20. It is possible to access all ports on the protected intranet server through the CTE by using the URL *http://24.221.1.1/http://192.168.1.20*.

Overview

The CTE transforms and delivers back-end website content to a variety of mobile devices, including Wireless Application Protocol (WAP) phones, Personal Digital Assistants (PDAs), and the Cisco IP phone. The CTE is a 1U device that installs into any network infrastructure without requiring changes to the existing hardware or back-end software. The CTE sits in front of content servers and works with other networking products such as server load balancers, cache engines, web servers, firewalls, Virtual Private Network (VPN) solutions, routers, and IEEE 802.11 broadband wireless devices.

Design Studio is a PC-based application that you can use to create transformation rules for a set of content and to upload the rules to a CTE. Assisting in the management of configuration files sent between Design Studio and a CTE is Services Manager, which is a centralized configuration management tool.

These sections describe the CTE:

- Features, page 3
- Licensing, page 5
- Security, page 5
- Sessions and Connections, page 6
- Operation Modes, page 7
- CTE Traffic Flow, page 9
- Input and Output Encoding, page 10

Features

Table 1 summarizes the features of the CTE.

Table 1 CTE Features

Feature	Description
Performance and Scalability	• Each CTE supports up to 1400 simultaneous connections. • Each CTE supports 1000 user sessions. • Add CTEs anywhere in your network to scale up.
Back-end content transformation	• Supports any HTML content (web server, enterprise application, etc.). • Supports raw XML data sources through XSL transformations (XSLT). • Transforms content through XSL, allowing for open standards and extensibility. • Supports advanced programming by allowing direct upload of XSL style sheets. XSL provides easy integration with existing technologies such as application servers, if needed. • Automatically removes content not supported by mobile devices or IP phones during transformation. This includes Java Applets and Flash programs. • Prepends the CTE IP address to all links on transformed pages.
Support for Multiple Devices	Mobile devices and Cisco IP phones use a variety of operating system platforms, presentation languages, and screen sizes and have different bandwidth constraints. The CTE manages these requirements on many devices automatically. Supported devices include the following: • Cisco IP Phone (XML) • Wireless phones (WAP 1.1-enabled phones using WML[1] version 1.1) • Handspring devices and Palm VII (Palm HTML) • Compaq iPAQ, Hewlett Packard Jornada, and RIM[2] devices (cHTML[3]) • Desktop computers (HTML/XML) Supports website content in the following formats: • HTML versions 4.0, 3.2, and 2.0 • XHTML versions 1.1 and 1.0 • XML version 1.0 • WML, version 1.1 • XSL[4] version 1.0 • GIF, JPEG, BMP, and WBMP image formats

Table 1 CTE Features (continued)

Feature	Description
Conversion features	• Automatically recognizes devices and provides device-specific rendering of content. Devices send a device ID with requests; the CTE uses the device ID to determine the correct formatting for the requesting device. • Transcodes images (GIF and JPEG to BMP and WBMP) and reduces color depth for bandwidth conservation. • Provides real-time content parsing for best performance. Automatically splits large page documents into smaller documents for small devices. Adds a More soft key to the page for navigation. • Issues pages in transit, while they are still being transformed and transcoded, for lower latency. • Supports dynamic content, malformed and overlapping HTML, and large forms in HTML content. • Supports up to 512-KB content size, not including images. • Supports web pages that use any standard encoding and transcodes web pages to the formats required by all supported wireless devices: UTF-8, UTR-16, and Shift_JIS character encoding. • Supports JavaScript-dependent form manipulation, even processing, browser redirection, and cookie handling.
Data and Session Management	• Works with any web server and any HTTP gateway (for example, any WAP gateway) and uses standard protocols for communication. Requires no integration effort with existing systems. • Provides load-balancing support with session stickiness. This is a high performance solution when operating with a server load balancer. • Provides server redundancy through the server load balancer and redundancy between two CTEs. • Supports in-line operation where server load balancers are not available. Using proxy ARP, the CTE masquerades as the web server and transforms content nonintrusively. • Supports session data (virtual cookies) for devices that do not natively support cookies. • Handles timeouts automatically. A connection times out after 60 seconds of inactivity (just like clients that use HTTP keepalive). An administrator can configure the session timeout interval. • Supports Design Studio connection to the CTE through a firewall or proxy server.

Table 1 CTE Features (continued)

Feature	Description
Security[5]	• Provides FlexLM licensing. • Fully supports various login authentication mechanisms (such as HTTP 401 authentication). Transcodes authentication protocols for devices that do not natively support authentication (such as Palm handheld devices). • Provides SSL sessions with support for HTTP and HTTPS. Fully supports secure cookies. • Supports full secure mode, where a client device is always secure to the CTE, independent of the connection to the web server. Works with VPN solutions. • Supports digital certificates in PEM[6] format that include a private key. • Requires only three available ports: 80 (for requests from wireless devices), 443 (requests from wireless devices are directed to this secure port during operations), and 9001 (for communication with Design Studio over a secure SSL link).

[1] WML = Wireless Markup Language.

[2] RIM = Research in Motion.

[3] cHTML = Compact HTML.

[4] XSL = Extensible Stylesheet Language.

[5] For more information, see the "Security" section on page 5.

[6] PEM = Privacy Enhanced Mail.

Licensing

The CTE supports FlexLM licensing.

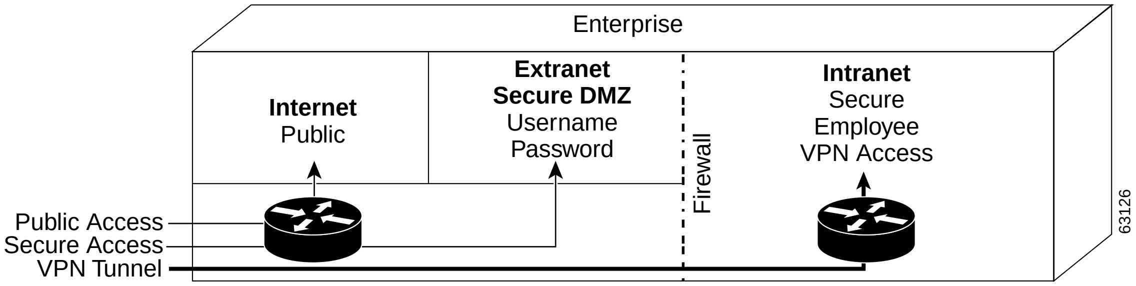
You can upload a new license through the CTE Administration Interface. For more information, see the "Uploads Screen" section on page 46.

Security

Internet, extranet, and intranet sites require different levels of security, all supported by the CTE. As shown in Figure 1, those sites have the following characteristics:

- Internet sites contain external content, are public, and require no authentication for access. All wireless devices supported by the CTE can access Internet sites.
- Extranet sites also contain external content, but they require authentication for access. Extranet sites are in a secure demilitarized zone (DMZ). All wireless devices supported by the CTE can access extranet sites. (Cisco IP phones cannot authenticate, so they are unable to log in to extranet sites.) The CTE supports various login authentication mechanisms (such as HTTP 401 authentication). In addition, the CTE transcodes authentication protocols for devices that do not natively support authentication (such as Palm devices).
- Intranet sites contain internal content that resides inside the enterprise firewall. From outside the firewall, these sites require a VPN client to tunnel through the firewall. Of the wireless devices supported by the CTE, only the Palm and Pocket PC devices with a Certicom VPN client can access intranet sites.

Figure 1 Security in the Enterprise



Security Issue for WAP Phones and Palm 7 Devices

The CTE terminates Secure Sockets Layer (SSL) sessions to provide an endpoint for a secure link. Some PDAs support SSL connections from the device to the CTE. However, WAP phones and the Palm 7 device do not support SSL. WAP phones use Wireless Transport Layer Security (WTLS) and Palm 7 devices use Elliptical Curve Cryptography (ECC). Carrier gateways usually convert WTLS and ECC to SSL; during the conversion, text is not secure.

Sessions and Connections

When a new device user makes a first request through the CTE, the CTE creates a new session for that user. In previous releases, the CTE did not store any session data. Consequently, the CTE could support 10,000 concurrent user sessions. With the introduction of JavaScript, the CTE must store data for each session. Therefore, the number of active sessions is limited by memory.

The CTE supports two configuration options to control the cache that stores session data: maximum and minimum session timeout thresholds. Both of these settings (Session Timeout and Minimum Session Timeout) can be set through the Advanced > General screen in the CTE Administration screens. For more information, see the "General Screen" section on page 37.

When the maximum session timeout is set and a session has not been active for the specified time period, the CTE terminates the session and clears the data from the cache. Any session that has been inactive longer than the maximum session timeout can be removed. Data from a terminated session, which includes authentication information and other sensitive data, is physically removed from memory, preventing unauthorized access.

The minimum session timeout determines the minimum time between two requests that a session is guaranteed to be active. For example, if the minimum session timeout is set for 5 minutes, and a user requests information through the CTE every 4 minutes and 59 seconds, that session will remain active indefinitely. If the user waits more than 5 minutes between requests, the session becomes unprotected and can be replaced by a new session.

If the minimum session timeout is not set, the CTE can support 10,000 sessions. However, not setting a minimum session timeout creates an environment in which each request initiates a new session and there is no guaranteed stability for any session during busy periods.

The only way to increase the number of active sessions is to increase memory (RAM and/or disk) or to lower the amount of memory allocated to each user. If the memory is lowered, however, performance can suffer because the CTE must retrieve and process the data again.

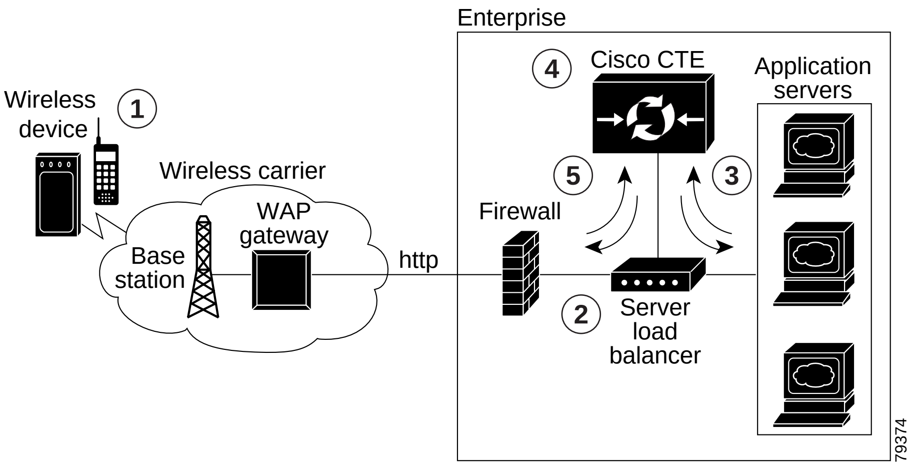
Another variable that can affect CTE performance is the number of simultaneous connections. A connection is used for each request. A session can use several simultaneous connections. For example, when a user requests a web page and that page contains images, frames, and other elements, the user's browser makes one request for each element. If a page has ten elements, the initial request makes one connection to retrieve the main page and the browser makes ten connections to retrieve the ten elements.

Operation Modes

The CTE uses rules supplied by Design Studio to fulfill requests for wireless content. A CTE is typically installed behind a server load balancer. When a wireless device requests a web page, the CTE accepts the request from the wireless device and requests the content from the back-end servers. Functioning as a reverse-proxy, the CTE acts like a web server to the client device and acts like a client device to the web servers.

Figure 2 shows the path that a wireless user request for a web page takes when the CTE is connected to a server load balancer. This configuration is recommended for sites where most of the network traffic intercepted by the CTE uses content supplied by the servers directly connected to the server load balancer.

Figure 2 CTE Connected to a Server Load Balancer



Note The numbers in Figure 2 refer to the following process.

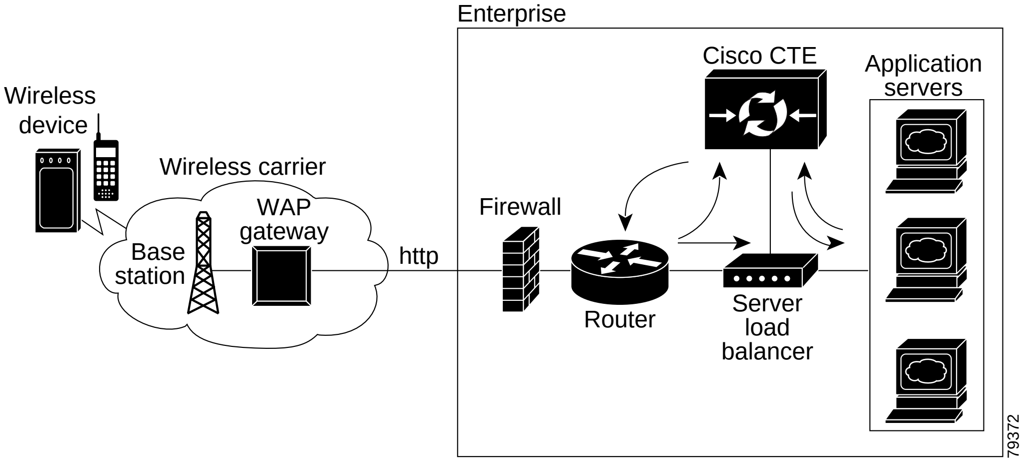
The path the wireless user request takes is as follows:

1. A wireless user requests a URL. A wireless carrier transmits the request to a communications tower, through the WAP carrier gateway, and to the Internet.
2. The server load balancer that receives the request evaluates the request header. The server load balancer directs HTML/XML requests to the web server farm and directs requests from wireless devices to the CTE.
3. The CTE terminates the request and then, acting as a proxy, sends a request to the server load balancer for the HTML/XML page.

4. When the CTE receives the page, it uses the rules in the configuration file to transform the content.
5. The CTE sends the transformed page to the server load balancer for forwarding to the wireless device.

A variation of the preceding configuration is to direct requests from the CTE through a router that sits in front of the server load balancer, as shown in Figure 3. This configuration is recommended for sites where most of the network traffic intercepted by the CTE uses content supplied by servers at other locations. For example, a results page served by a search engine portal contains links to content that resides outside of the domain of the search site.

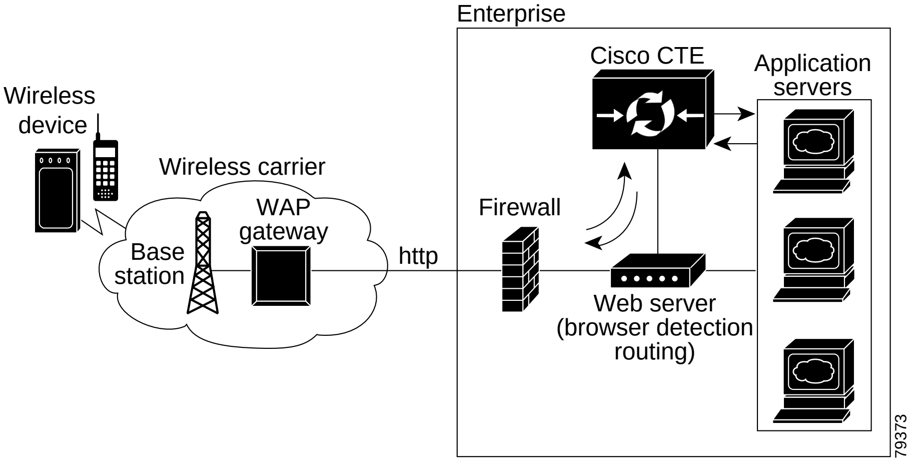
Figure 3 CTE Connected to Router and Server Load Balancer



CTE Connected to Web Server

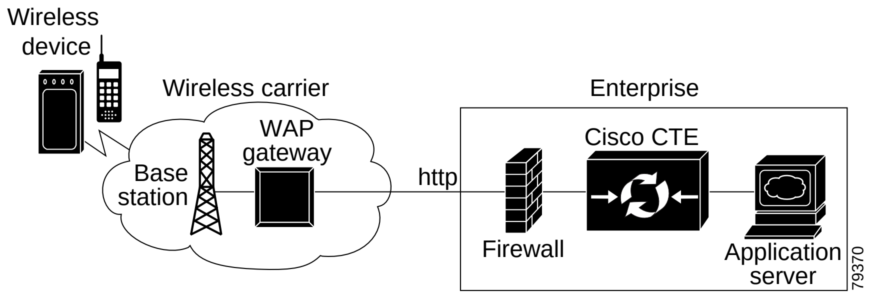
You can connect a CTE to a web server that routes traffic to the CTE or to web servers based on browser detection, as shown in Figure 4.

Figure 4 CTE Connected to a Web Server that Routes



You can also connect a CTE directly to a web server, as shown in Figure 5. In this case, all web traffic goes through the CTE, which passes HTML/XML requests to the web server and handles requests from wireless devices. This configuration is recommended when you designate specific IP addresses for wireless traffic.

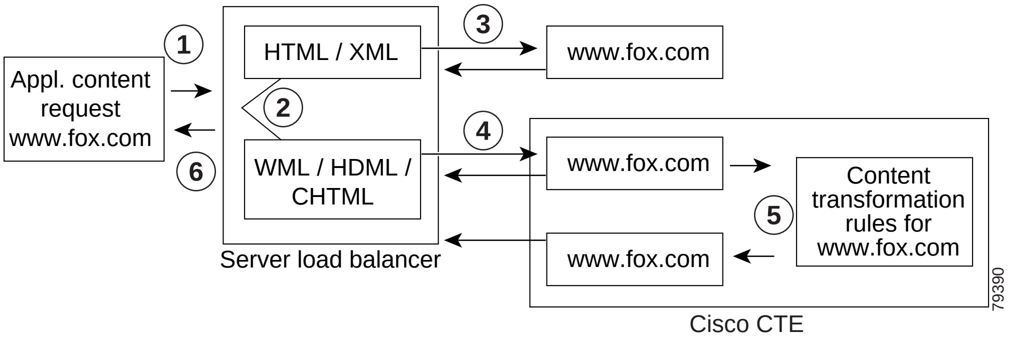
Figure 5 CTE In-line Connection



CTE Traffic Flow

Figure 6 and the following procedure describe how URL requests from a wireless device are handled by the CTE and connected devices.

Figure 6 Traffic Flow for Web Page Requests



Note The numbers in Figure 6 refer to the steps in the following procedure.

When a wireless device sends a URL to a web server, the traffic flow is as follows:

Step 1 A wireless user enters a URL (such as www.fox.com). The request is transmitted to a communications tower, through the carrier gateway, and to the Internet.

Step 2 The server load balancer that receives the request looks at the header.

Step 3 The server load balancer directs HTML/XML requests to the web server farm.

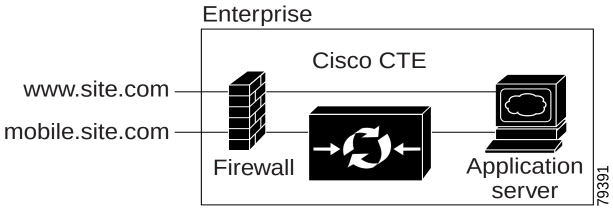
Step 4 The server load balancer directs requests from wireless devices to the CTE.

Step 5 The CTE sends the new request to the server load balancer for the HTML/XML content. The CTE, acting as a proxy, sends a request to the server load balancer for the HTML/XML content. The server load balancer obtains the content from a web server and sends it to the CTE.

Step 6 The CTE uses the rules created by Design Studio to transform the content and then sends the transformed content to the server load balancer. The server load balancer forwards the content to the wireless device.

As shown in Figure 7, you can also route requests based on a URL so that requests from designated URLs (such as mobile.site.com) are passed directly to the CTE.

Figure 7 Requests Directed Based on a URL



Input and Output Encoding

Input encoding, the formats into which information coming to the CTE can be written, is configurable through the Administration Interface. By default, input encoding is set to Western European (ISO-8859-1, Latin-1, ASCII). Only one input encoding format can be active at a time. Other input encoding schemes are listed in Table 10 on page 38.

Output encoding, the formats into which information sent from the CTE can be written, is specified in the DDF file of each device driver. If there is an error in a particular DDF file, each device driver has a hard-coded default value for output encoding. Formats supported for output encoding are listed in Table 2.

Table 2 Output Encoding Formats

Language	Format
Armenian	ARMSCII-8
Chinese	EUC-CN, HZ, GBK, GB18030, EUC-TW, BIG5, CP950, BIG5-HKSCS, ISO-2022-CN, ISO-2022-CN-EXT
European	ASCII, ISO-8859-(1, 2, 3, 4, 5, 7, 9, 10, 13, 14, 15, 16), KO18-R, KO18-U, KO18-RU, CP (850, 866, 1250, 1251, 1252, 1253, 1254, 1257), Mac (Roman, Central Europe, Iceland, Croatian, Romania, Cyrillic, Ukraine, Greek, Turkish)
Full Unicode	UTF-8, UCS-2, UCS-2BE, UCS-2LE, UCS-4, UCS-4BE, UCS-4LE, UTF-16, UTF-16BE, UTF-16LE, UTF-32, UTF-32BE, UTF-32LE, UTF-7
Georgian	Georgian-Academy, Georgian-PS
Japanese	EUC-JP, SHIFT-JIS, CP932, ISO-2022-JP-2, ISO-2022-JP-1
Korean	EUC-KR, CP949, ISO-2022-KR, JOHAB

Table 2 Output Encoding Formats (continued)

Language	Format
Laotian	MuleLao-1, CP1133
Platform-specific	HP-ROMAN8, NEXTSTEP
Semitic	ISO-8859-6, ISO-8859-8, CP1255, CP1256, CP862, Mac (Hebrew, Arabic)
Thai	TIS-620, CP874, MacThai
Vietnamese	VISCII, TCVN, CP1258

Configuring the CTE

The configuration instructions in this publication assume the following setup:

- The CTE is installed and connected to a second computer through a serial port, as described in the *Cisco CTE 1400 Hardware Installation Guide*.
- The devices to which you are connecting the CTE, such as a server load balancer, are already part of a working configuration. This publication does not, for example, cover the steps for configuring web servers or a web server farm with a server load balancer.

The "Operation Modes" section on page 7 covers typical network configurations for the CTE. Use Table 3 as a guide to determine the best location for a CTE, based on network topology and website characteristics.

Table 3 CTE Network Location Guidelines

Network Topology and Website Characteristics	Network Location of CTE
A server load balancer sits in front of one or more web servers. Most of the network traffic to be intercepted by the CTE uses website content supplied by servers directly connected to the server load balancer.	Behind the server load balancer. or In front of a web server that routes traffic to one or more CTEs or to web servers based on browser detection.
A server load balancer sits in front of one or more web servers. Most of the network traffic to be intercepted by the CTE uses website content supplied by servers at other locations. For example, a results page served by a search engine portal contains links to content that resides outside of the domain of the search site.	Behind the server load balancer with requests from one or more CTEs directed through the router.
One web server. All traffic destined for the web server goes through the CTE.	In front of the web server.

The general process for configuring a CTE and connected devices is as follows:

1. Draw a diagram of the data flow for the CTE, including all IP addresses and VLAN numbers.
2. Physically connect the CTE to the network.

   Depending on your network topology, you may need to use one or both of the CTE ports (NICs).
3. Verify that the server load balancer can ping the CTE.

4. If configuring multiple CTEs, associate the various CTE network connections with a CTE server farm.
5. Configure the server load balancer so that the CTE can access web content on the web servers.
6. Configure the server load balancer so that the CTE is accessible by clients requesting web content.
7. Verify that the data flow of the CTE is as planned.
8. If a client does not require in-line data transformation by the CTE, direct its traffic to the web servers if possible.

These sections describe how to configure the CTE and connected devices:

- Preparing to Connect and Configure the CTE, page 12
- Configuring a CTE Connected Directly to a Web Server, page 13
- Configuring a CTE Connected to a Server Load Balancer, page 17

Preparing to Connect and Configure the CTE

Note Before you deploy the CTE, verify that port 9001 is not accessible from outside of your firewall. The CTE communicates with Design Studio through port 9001 using clear-text transmissions. Only ports 80 and 443 should be visible from outside of your firewall.

Most firewalls allow administrators to deny external IP addresses access to specific ports that are set up internally. See your firewall administrator guide for information on setting up rules to block specific ports.

To connect the CTE to a network, you need two network cables. Only one cable may be necessary if you connect the CTE directly to one web server. Before configuring the CTE and connected devices, plan the network information that you want to use for the following, as appropriate:

- VLAN number, port numbers, and IP addresses for the client-side connections between the CTE and a server load balancer, router, or web server (directly connected to the CTE).
- VLAN number, port numbers, and IP addresses for the server-side connections between the CTE and a server load balancer.

  Note The CTE does not work with Dynamic Host Configuration Protocol (DHCP). You must use static IP addresses for the CTE.

- The virtual IP address that you want to assign to a masquerade host.
- CTE server farm names and their virtual IP addresses.

Reopening the CTE Console

The CTE console provides initial access to the CTE, letting you set up the CTE for use. From the console, you can configure network parameters, configure SNMP, set the gateways, manage users, and restart or shut down the CTE.

If you completed the installation procedures described in the *Cisco CTE 1400 Hardware Installation Guide*, you already have a CTE console open on a computer that has a serial connection to the CTE. If the CTE console has been closed, reopen the connection to the CTE console as follows.

To open a CTE console, perform these steps:

Step 1 On the computer with a serial connection to the CTE, start the terminal emulation application and open the connection that you created to the CTE.

Step 2 Log on to the CTE console as **root**. You will be prompted to choose a password.

Step 3 Enter a new root password. You will be prompted to reenter the password for verification.

Step 4 The CTE prompts you for the following:

```
IP address [x.x.x.x] (Enter 0 to clear): ipaddress
Netmask [x.x.x.x] (Enter 0 to clear): 255.255.255.0
Gateway [x.x.x.x]: default gateway ipaddress
```

Step 5 Enter the IP address and netmask of the eth0 port and the IP address of the default gateway.

Step 6 The CTE will ask you to commit the changes. Type **yes** to commit them, and the Main menu of the CTE console appears. If you do not want to commit the changes, type **no**, and then type **0** (Express Setup) to reenter the settings.

Step 7 If the CTE console does not open, check the following:

- Verify that the CTE is powered on.
- Check the settings in the terminal emulation application. Set the serial connection to 9600 bits per second, 8 data bits, no parity, and 1 stop bit.

Configuring a CTE Connected Directly to a Web Server

You can connect a CTE directly to a web server if your site has only one web server and you want all traffic destined for the web server to pass through the CTE. The CTE determines how to handle requests for web content based on the request header, which indicates the type of device making the request. The CTE intercepts requests from supported mobile devices and passes through other requests.

Connecting a CTE directly to a web server does not require any changes to the web server configuration.

The following sections describe how to connect a CTE to a web server and configure the CTE to work with the web server:

- Connecting a CTE to a Web Server, page 13
- Configuring CTE Parameters, page 14

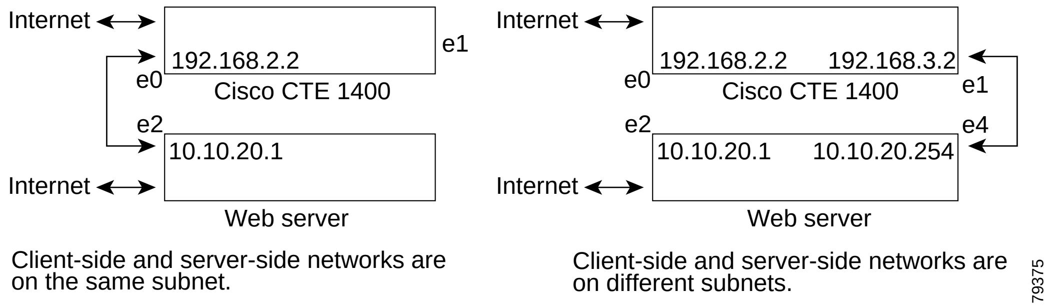
Connecting a CTE to a Web Server

Connecting a CTE to a web server requires either one or two network cables as follows:

- If the CTE can access the web server from the same subnet as it receives client requests, you can use one network cable. Connect the CTE e0 (NIC 1) port to the client-side network.
- If the web server and clients are on different subnets, you must use two network cables and connect the CTE as follows:
  - Connect the CTE e0 (NIC 1) port to the client-side network.
  - Connect the CTE e1 (NIC 2) port to the server-side network, directly or indirectly. In most cases, the gateway IP address will be on the same subnet as the web server.

Figure 8 shows how to connect a CTE to a web server.

Figure 8 CTE Connected to Web Server



Note The IP addresses used throughout this publication are example addresses, not actual ones.

Configuring CTE Parameters

Use the CTE console and the CTE Administration menus to display and configure parameters for the CTE.

When the CTE console first appears, the console displays the Main menu:

```
[0] Express Setup
[1] Configure Network Interface
[2] Manage Administrative Users
[3] View System Information
[4] Restart/Shutdown
[5] Log Out
```

Displaying Current Network Parameters

To display current network parameters, perform these steps:

Step 1 Type **1** (Configure Network Interface) and press **Enter**. The Network Settings menu appears:

```
Network Settings
[0] Configure Interface 0
[1] Configure Interface 1
[2] Set DNS
[3] Set Gateway
[4] Set Gateway Device
[5] Ping
[6] Display Configuration
[7] Return to Main Menu
```

Step 2 Type **6** (Display Configuration), and the console displays all set parameters:

```
eth0 address: 10.0.16.192
eth0 netmask: 255.255.255.0
eth0 duplex mode: auto
eth0 MTU: 1500
eth1 address:
eth1 netmask:
eth1 duplex mode: auto
eth1 MTU: 1500
DNS Server 0: [null]
DNS Server 1: [null]
DNS Server 2: [null]
Domain Name:
Gateway: 10.0.16.1
Gateway Device:
```

Configuring Network Parameters

To configure network parameters, perform these steps:

Step 1 From the Main Menu, type **1** (Configure Network Interface).

Step 2 From the Network Settings menu, type **0** (Configure Interface 0) and press **Enter**. The following menu appears:

```
[0] Set IP Address
[1] Set Netmask
[2] Set Duplex Mode
[3] Set MTU
[4] Display Settings
[5] Return to Network Menu
```

Step 3 Type **0** to set the IP address for Interface 0, and enter the address at the following prompt:

```
IP address [x.x.x.x] (Enter 0 to clear): ip_address
```

Press **Enter** to retain the same value, type **0** to clear the value, or enter a new IP address and press **Enter**.

Step 4 Type **1** to set the netmask for Interface 0, and enter the netmask at the following prompt:

```
Netmask [255.255.255.0] (Enter 0 to clear): netmask
```

Press **Enter** to retain the same value, type **0** to clear the value, or enter a new netmask and press **Enter**.

Step 5 Type **2** to set duplex mode, and the following menu appears:

```
Select Transmission Mode (<Enter> to cancel)
[0] Auto Detect
[1] Full-Duplex Transmission
[2] Half-Duplex Transmission
```

Type **0**, **1**, or **2** depending on the transmission mode you want to specify.

Step 6 Type **3** to set the MTU (maximum transmitted unit), and enter a value at the following prompt, or press **Enter** to retain the default value of 1500.

```
MTU (1500):
```

Step 7 To display the current settings for both Interfaces 0 and 1, type **4**, and the console displays the following:

```
eth0 address: 10.0.16.192
eth0 netmask: 255.255.255.0
eth0 duplex mode: auto
eth0 MTU: 1500
eth1 address:
eth1 netmask:
eth1 duplex mode: auto
eth1 MTU: 1500
```

Step 8 To return to the Network Settings menu, type **5**.

Note When changes are pending, the Network Settings menu contains two additional options: [7] Commit Changes and [8] Cancel Changes. These options are only present on the menu when changes are pending but not yet saved.

Step 9 After you have made any changes, you will need to commit them. To commit your changes, type **7** (Commit Changes) on the Network Settings menu. You can also choose to cancel any changes by typing **8** (Cancel Changes).

Step 10 To configure Interface 1 from the Network Settings menu, type **1** (Configure Interface 1) and press **Enter**. Perform steps 2 through 9 as described for Interface 0.

Step 11 From the Network Settings menu, type **2** (Set DNS) and press **Enter**.

Step 12 Answer the prompts as follows:

```
DNS server [0] : [x.x.x.x]
DNS server [1] : [x.x.x.x]
DNS server [2] : [x.x.x.x]
Domain Name :

DNS server [0] [x.x.x.x] (Enter 0 to clear): ip_address
DNS server [1] [x.x.x.x] (Enter 0 to clear): ip_address
DNS server [2] [x.x.x.x] (Enter 0 to clear): ip_address
Domain Name [ ] (Enter 0 to clear): domain_name
```

Step 13 Type **3** (Set Gateway) and press **Enter** to define the IP address of the default gateway address.

```
Gateway [x.x.x.x]: gateway ip_address
```

Step 14 Type **4** (Set Gateway Device) and press **Enter** to define the default gateway device.

```
Gateway Device (eth0, eth1) [] 0 or 1
```

This display (from the configuration shown in Figure 8 on page 14) shows different subnets and contains the following network parameters:

```
eth0 IP address: 192.168.2.1
eth0 netmask: 255.255.255.0
eth1 IP address: 192.168.3.1    [on separate subnet from eth0]
eth1 netmask: 255.255.255.0
Gateway: 10.10.20.254
Gateway device: 1
```

Step 15 To commit your changes, type **7** (Commit Changes) on the Network Settings menu. You can also choose to cancel any changes by typing **8** (Cancel Changes).

Step 16 After your changes are saved, type **7** to return to the Main menu.

To continue configuring the CTE, perform these steps:

Step 1 From any browser, enter the following URL:

https://<*IP-address*>**:**<*administration-port*>

where:

- <*IP_address*> is the IP address of your CTE
- <*administration-port*> is the administration port of your CTE (usually 9001)

Step 2 Click **Yes** if a Security Information dialog box appears.

Step 3 Log in as **root**, and enter your root password.

Note You can create additional administrative usernames and passwords from the CTE console. For more information, see the description of [2] Manage Administrative Users in Table 4 on page 24.

Step 4 On the Interfaces screen of the Network tab, define the Masquerade Hosts for Interface 0 and Interface 1. The masquerade host is an IP address that can be used for Network Address Translation (NAT).

NAT makes all requests appear to originate from the same client, so that the CTE sends its response to the request back on the correct network connection. If the NAT IP address is not defined, the CTE sends responses out through the NIC where the gateway is identified.

Step 5 On the General screen of the Advanced tab, define a default URL that the CTE will request if you attempt to access the CTE directly (for example, http://*cte_name*). Defining this field allows administrators to configure a default web page to proxy.

Step 6 Click the **Submit** button at the bottom of the window to save your changes.

To configure additional CTEs, repeat the above procedure for each CTE.

Configuring a CTE Connected to a Server Load Balancer

You can connect a CTE to a server load balancer such as the Cisco Content Services Switch (CSS) 11000 or the Catalyst 6000 family Content Switching Module (CSM). Characteristics of this configuration include the following:

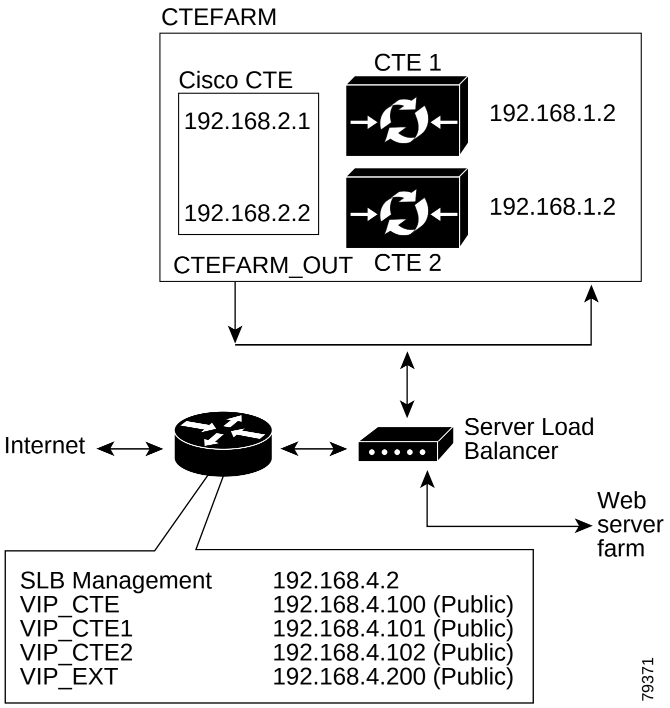
- Incoming web traffic is intercepted by the server load balancer and load balanced between the CTEs (if more than one CTE is in use). All incoming client IP addresses appear as a single IP address through NAT.
- When a CTE receives a request through port 80 for a valid web page, it issues a temporary redirect to the client so that the connection uses HTTPS on port 443. The address to which the client is redirected is determined by the masquerade host IP address set for the CTE.

  If multiple CTEs are in use, each CTE has a different masquerade host IP address. In addition, the CTE modifies all URLs embedded within a page to include the masquerade host IP address. This use of the masquerade host IP address ensures that the redirected client returns to the CTE it first encountered, providing session stickiness. The association between a particular request and the CTE is broken only when the client makes a new connection on port 80.
- The CTEs request content from web servers through the alias IP address set for the server-side VLAN.

  The CTE farm and the web server farm are directly accessible through load-balanced virtual IP (VIP) addresses. This configuration enables you to direct traffic that originates from a wireless device to the CTE farm VIP address.

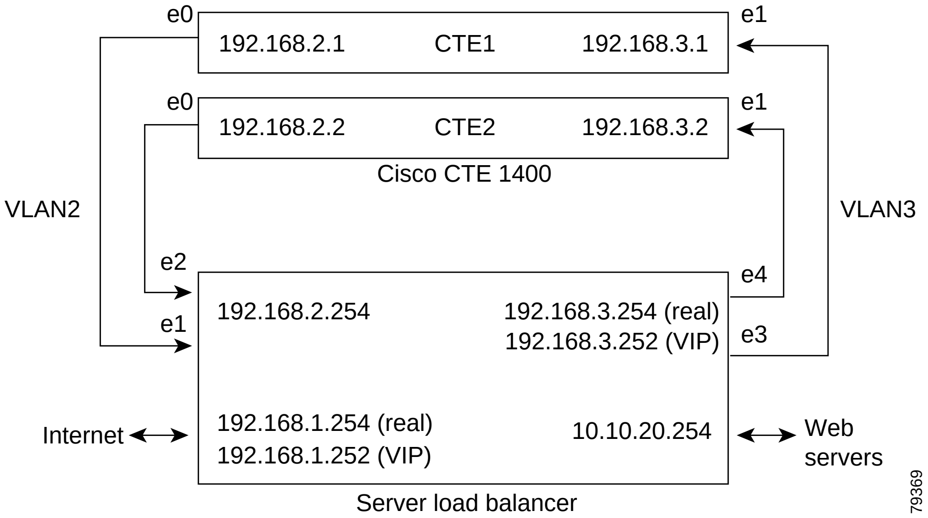
The procedures in this section are specific to the CSS, although the CSM setup is similar. Figure 9 shows a CSM setup in which CTE requests go to the server load balancer, rather than the router.

Figure 9 CTE Connected to Catalyst 6000 Family Switch (Requests Not Directed Through Router)


CTEFARM
Cisco CTE
192.168.2.1
192.168.2.2
CTE 1
192.168.1.2
192.168.1.2
CTEFARM_OUT
CTE 2
Internet
Server Load Balancer
Web server farm
SLB Management 192.168.4.2
VIP_CTE 192.168.4.100 (Public)
VIP_CTE1 192.168.4.101 (Public)
VIP_CTE2 192.168.4.102 (Public)
VIP_EXT 192.168.4.200 (Public)
79371

This section uses the example configuration shown in Figure 10.

Figure 10 CTE Connected to Server Load Balancer



The following sections describe how to configure a CTE with a server load balancer:

- Connecting the CTE to a Server Load Balancer, page 19
- Configuring CTE Parameters, page 19
- Configuring the Server Load Balancer, page 22

Connecting the CTE to a Server Load Balancer

To establish the physical connection, do the following:

- Connect the CTE e0 (NIC 1) port of each CTE to the client-side network.
- Connect the CTE e1 (NIC 2) port of each CTE to the server-side network.

Configuring CTE Parameters

Use the CTE console and the CTE Administration tools to display and configure parameters for the CTE.

When the CTE console first appears, the console displays the Main menu:

```
[0] Express Setup
[1] Configure Network Interface
[2] Manage Administrative Users
[3] View System Information
[4] Restart/Shutdown
[5] Log Out
```

Displaying Current Network Parameters

To display current network parameters, perform these steps:

Step 1 Type **1** (Configure Network Interface) and press **Enter**. The Network Settings menu appears:

```
Network Settings
[0] Configure Interface 0
[1] Configure Interface 1
[2] Set DNS
[3] Set Gateway
[4] Set Gateway Device
[5] Ping
[6] Display Configuration
[7] Return to Main Menu
```

Step 2 Type **6** (Display Configuration), and the console displays all set parameters:

```
eth0 address: 10.0.16.192
eth0 netmask: 255.255.255.0
eth0 duplex mode: auto
eth0 MTU: 1500
eth1 address:
eth1 netmask:
eth1 duplex mode: auto
eth1 MTU: 1500
DNS Server 0: [null]
DNS Server 1: [null]
DNS Server 2: [null]
Domain Name:
Gateway: 10.0.16.1
Gateway Device:
```

Configuring Network Parameters

To configure network parameters, perform these steps:

Step 1 From the Main menu, type **1** (Configure Network Interface).

Step 2 From the Network Settings menu, type **0** (Configure Interface 0) and press **Enter**. The following menu appears:

```
[0] Set IP Address
[1] Set Netmask
[2] Set Duplex Mode
[3] Set MTU
[4] Display Settings
[5] Return to Network Menu
```

Step 3 Type **0** to set the IP address for Interface 0, and enter the address at the following prompt:

```
IP address [x.x.x.x] (Enter 0 to clear): ipaddress
```

Press **Enter** to retain the same value, type **0** to clear the value, or enter a new IP address and press **Enter**.

Step 4 Type **1** to set the netmask for Interface 0, and enter the netmask at the following prompt:

```
Netmask [255.255.255.0] (Enter 0 to clear): netmask
```

Press **Enter** to retain the same value, type **0** to clear the value, or enter a new netmask and press **Enter**.

Step 5 Type **2** to set duplex mode, and the following menu appears:

```
Select Transmission Mode (<Enter> to cancel)
[0] Auto Detect
[1] Full-Duplex Transmission
[2] Half-Duplex Transmission
```

Type **0**, **1**, or **2** depending on the transmission mode that you want to specify.

Step 6 Type **3** to set the MTU (maximum transmitted unit), and enter a value at the following prompt, or press **Enter** to retain the default value of 1500.

```
MTU (1500):
```

Step 7 To display the current settings for both Interfaces 0 and 1, type **4**, and the console displays the following:

```
eth0 address: 10.0.16.192
eth0 netmask: 255.255.255.0
eth0 duplex mode: auto
eth0 MTU: 1500
eth1 address:
eth1 netmask:
eth1 duplex mode: auto
eth1 MTU: 1500
```

Step 8 To return to the Network Settings menu, type **5**.

Note When changes are pending, the Network Settings menu contains two additional options: [7] Commit Changes and [8] Cancel Changes. These options are only present on the menu when changes are pending but not yet saved.

Step 9 After you have made any changes, you will need to commit them. To commit your changes, type **7** (Commit Changes) on the Network Settings menu. You can also choose to cancel any changes by typing **8** (Cancel Changes).

Step 10 To configure Interface 1 from the Network Settings menu, type **1** (Configure Interface 1) and press **Enter**. Perform Steps 2 through 9 as described for Interface 0.

Step 11 From the Network Settings menu, type **2** (Set DNS) and press **Enter**.

Step 12 Answer the prompts as follows:

```
DNS server [0] : [x.x.x.x]
DNS server [1] : [x.x.x.x]
DNS server [2] : [x.x.x.x]
Domain Name :

DNS server [0] [x.x.x.x] (Enter 0 to clear): ip_address
DNS server [1] [x.x.x.x] (Enter 0 to clear): ip_address
DNS server [2] [x.x.x.x] (Enter 0 to clear): ip_address
Domain Name [ ] (Enter 0 to clear): domain_name
```

Step 13 Type **3** (Set Gateway) and press **Enter** to define the IP address of the default gateway address.

```
Gateway [x.x.x.x]: gateway ip_address
```

Step 14 Type **4** (Set Gateway Device) and press **Enter** to define the default gateway device.

```
Gateway Device (eth0, eth1) [] 0 or 1
```

For Figure 10, the network parameters for CTE are as follows:

```
eth0 IP address: 192.168.2.1
eth0 netmask: 255.255.255.0
eth1 IP address: 192.168.3.1    [on separate subnet from eth0]
eth1 netmask: 255.255.255.0
Gateway: 10.10.20.254
Gateway device: 1
```

Step 15 To commit your changes, type **7** (Commit Changes) on the Network Settings menu. You can also choose to cancel any changes by typing **8** (Cancel Changes).

Step 16 After your changes are saved, type **7** to return to the Main menu.

To continue configuring the CTE, go to the CTE Administration Interface, and perform these steps:

Step 1 Make sure that the CTE console is running.

Step 2 From any browser, enter the following URL:

https://<*IP-address*>**:**<*administration-port*>

where:

- <*IP_address*> is the IP address of your CTE
- <*administration-port*> is the administration port of your CTE (usually 9001)

Step 3 Click **Yes** if a Security Information dialog box appears.

Step 4 Log in as **root**, and enter your root password.

Note You can create additional administrative usernames and passwords from the CTE console. For more information, see the description of [2] Manage Administrative Users in Table 4 on page 24.

Step 5 On the Interfaces screen of the Network tab, define the Masquerade Hosts for Interface 0 and Interface 1. The masquerade host is an IP address that can be used for NAT.

NAT makes all requests appear to originate from the same client, so that the CTE sends its response to the request back on the correct network connection. If the NAT IP address is not defined, the CTE sends responses out through the NIC where the gateway is identified.

Step 6 On the General screen of the Advanced tab, define a default URL that the CTE will request if you attempt to access the CTE directly (for example, http://*cte_name*). Defining this field allows administrators to configure a default web page to proxy.

Step 7 Press the **Submit** button at the bottom of the window to save your changes.

To configure additional CTEs, repeat the above procedure for each CTE.

Configuring the Server Load Balancer

The basic process for configuring a server load balancer, such as the CSS, is as follows:

1. Establish a console port connection to the server load balancer.
2. Define the interfaces to the VLANs.
3. Configure the circuits.
4. Define services, owners, and content rules.
5. Check network connectivity.

This section describes the general steps for configuring the CSS, based on the example configuration shown in Figure 10. For the CLI commands needed to complete this configuration, see the "Configuration Example" section on page 47.

To configure a server load balancer for operation with a CTE, perform these steps:

Step 1 On a computer that is connected to the console port of the server load balancer, log into the device's command line interface.

Step 2 Create links between the CTE ports and the server load balancer by adding the client-side and server-side VLANs and defining the interfaces to the VLANs.

In the example configuration in Figure 10, the e1 and e2 ports are the interfaces for VLAN2; e3 and e4 are the interfaces for VLAN3.

Step 3 Specify the IP addresses for the VLAN circuits.

In the sample configuration, the IP address for the VLAN2 circuit is 192.168.2.254. The IP address for the VLAN3 circuit is 192.168.3.254.

Step 4 Create services to identify the two CTEs.

In the sample configuration, the IP address for the CTE1 service is 192.168.2.1 and the IP address for the CTE2 service is 192.168.2.2.

Step 5 Create an owner so that you can define content rules for the CTE1 and CTE2 services.

Step 6 Create a Layer 3 content rule for the services.

In the sample configuration, the content rule is configured with the virtual IP address 192.168.3.252 and is added to the CTE1 and CTE2 services.

Step 7 Check network connectivity.

Using the CTE Console Menu and Administration Interface

The CTE Console menu and Administration Interface allow you to set up and administer your CTE. This section describes both tools:

- CTE Console Menu, page 23
- CTE Administration Interface, page 31

CTE Console Menu

The CTE Console menu lets you set up the CTE initially. From this menu, you can perform the tasks described in Table 4.

Table 4 CTE Console Commands

Command	Description

[0] Express Setup	Allows you to set the IP address, netmask, and gateway for the Ethernet 0 port.
	Type **0**, press **Enter**, and enter the requested information at the following prompts:
	`IP address [x.x.x.x] (Enter 0 to clear):`
	Type the IP address of the Ethernet 0 port, and press **Enter**. To clear the value, type **0** and press **Enter**.
	`Netmask [255.255.255.0] (Enter 0 to clear):`
	Press **Enter** to retain the default netmask value of 255.255.255.0. To clear the value, type **0** and press **Enter**.
	`Gateway [x.x.x.x]:`
	Type the IP address of the gateway device that you want to be the default, and press **Enter**.

[1] Configure Network Interface	Allows you to display the Network Settings menu.
	Type **1** and the following menu appears:
	`Network Settings`
	`[0] Configure Interface 0`
	`[1] Configure Interface 1`
	`[2] Set DNS`
	`[3] Set Gateway`
	`[4] Set Gateway Device`
	`[5] Ping`
	`[6] Display Configuration`
	`[7] Return to Main Menu`
	Note When changes are pending, the Network Settings menu contains two more options to commit or cancel your changes. When changes have been saved or canceled, these extra options go away.

Table 4 CTE Console Commands (continued)

Command	Description
[1] Configure Network Interface	Allows you to configure network settings for Interface 0.

[0] Configure Interface 0	On the Network Settings menu, type **0**, and the following submenu appears:
	`[0] Set IP Address`
	`[1] Set Netmask`
	`[2] Set Duplex Mode`
	`[3] Set MTU`
	`[4] Display Settings`
	`[5] Return to Network Menu`
	To set the IP address for Interface 0, type **0**, and enter a value at the following prompt:
	`IP address [x.x.x.x] (Enter 0 to clear):`
	To set the netmask for Interface 0, type **1**, and enter a value at the following prompt:
	`Netmask [255.255.255.0] (Enter 0 to clear):`
	To set the Duplex Mode for Interface 0, type **2**, and select a transmission mode from the following submenu:
	`Select Transmission Mode (<Enter> to cancel)`
	`[0] Auto Detect`
	`[1] Full-Duplex Transmission`
	`[2] Half-Duplex Transmission`
	The console will display the mode that you select and return you to the previous menu.
	To set the Maximum Transmission Unit (MTU) for Interface 0, type **3**, and enter a value at the following prompt, or press **Enter** to accept the default value:
	`MTU [1500]:`
	The console will display the value that you specified and return you to the previous menu.

Table 4 CTE Console Commands (continued)

Command	Description

[1] Configure Network Interface
[0] Configure Interface 0 (continued)
	To display the current network settings for Interfaces 0 and 1, type **4**, and the console displays the following settings:
	`eth0 address: –`
	Displays the IP address of Interface 0 if defined.
	`eth0 netmask: –`
	Displays the subnet mask of Interface 0 if defined.
	`eth0 duplex mode: auto`
	Displays the transmission mode for Interface 0 if defined.
	`eth0 MTU: 1500`
	Displays the MTU setting for Interface 0.
	`eth1 address: –`
	Displays the IP address of Interface 1 if defined.
	`eth1 netmask: –`
	Displays the subnet mask of Interface 1 if defined.
	`eth1 duplex mode: auto`
	Displays the transmission mode for Interface 1 if defined.
	`eth1 MTU: 1500`
	Displays the MTU setting for Interface 1.
	To return to the Network Settings menu, type **5**.

[1] Configure Network Interface
[1] Configure Interface 1
	Allows you to configure the network settings for Interface 1.
	Type **1**, and the following submenu appears:
	`[0] Set IP Address`
	`[1] Set Netmask`
	`[2] Set Duplex Mode`
	`[3] Set MTU`
	`[4] Display Settings`
	`[5] Return to Network Menu`
	Configure values for Interface 1 as described for Interface 0.

Table 4 CTE Console Commands (continued)

Command	Description

[1] Configure Network Interface
[2] Set DNS
	Allows you to define up to three DNS servers and an associated domain name.
	Type **2**, press **Enter**, and enter the requested information at the following prompts:
	`DNS server[0] [x.x.x.x] (Enter 0 to clear):`
	Type the IP address of the first DNS server, or press **Enter** to leave the value blank.
	`DNS server[1] [x.x.x.x] (Enter 0 to clear):`
	Type the IP address of the second DNS server, or press **Enter** to leave the value blank.
	`DNS server[2] [x.x.x.x] (Enter 0 to clear):`
	Type the IP address of the third DNS server, or press **Enter** to leave the value blank.
	`Domain Name (Enter 0 to clear):`
	Type the domain name, or press **Enter** to leave the value blank.

[1] Configure Network Interface [3] Set Gateway	Allows you to specify the default gateway address. Type **3**, press **Enter**, and enter the requested information at the following prompt: `Gateway [x.x.x.x]:` Type the IP address of the gateway device that you want to be the default, or press **Enter** to leave the value blank. If the gateway is unset, the CTE will only be able to access content on the local network.
[1] Configure Network Interface [4] Set Gateway Device	Allows you to specify the default gateway address and device. Type **4**, press **Enter**, and enter the requested information at the following prompt: `Gateway Device (eth0, eth1) []` Type **eth0** or **eth1** to specify Interface 0 or Interface 1 as the default gateway device. (If a gateway device is currently selected, its value will appear between the two brackets at right.)

Table 4 CTE Console Commands (continued)

Command	Description
[1] Configure Network Interface [5] Ping	Allows you to verify that your machine can see another machine on the network. This feature is particularly useful when you have set up a static route to make sure that the route was successfully set. Type **5**, press **Enter**, and type a machine name or IP address. Status messages will appear on your screen. You will know that you can see the other machine if the messages say that the same number of packets were transmitted and received, and zero packets were lost. You will know that you cannot see the other machine if the messages say that zero packets were received and all the packets were lost.

Table 4 CTE Console Commands (continued)

Command	Description

[1] Configure Network Interface
[6] Display Configuration (continued)
	Allows you to display the current configuration.
	Type **6**, and the console displays the following settings:
	`eth0 address: –`
	Displays the IP address of the Interface 0 if defined.
	`eth0 netmask: –`
	Displays the subnet mask of Interface 0 if defined.
	`eth0 duplex mode: auto`
	Displays the transmission mode for Interface 0 if defined.
	`eth0 MTU: 1500`
	Displays the MTU setting for Interface 0.
	`eth1 address: –`
	Displays the IP address of the Interface 1 if defined.
	`eth1 netmask: –`
	Displays the subnet mask of Interface 1 if defined.
	`eth1 duplex mode: auto`
	Displays the transmission mode for Interface 1 if defined.
	`eth1 MTU: 1500`
	Displays the MTU setting for Interface 1.
	`DNS Server 0:`
	Displays the IP address of DNS server 0 if defined.
	`DNS Server 1:`
	Displays the IP address of DNS server 1 if defined.
	`DNS Server 2:`
	Displays the IP address of DNS 2 server if defined.
	`Domain Name: –`
	Displays the domain name if defined.
	`Gateway:`
	Displays the IP address of the gateway if defined.
	`Gateway Device:`
	Displays eth0 or eth1 if defined.
	To return to the Main menu, type **7**.

Table 4 CTE Console Commands (continued)

Command	Description

[2] Manage Administrative Users	Allows you to list, add, and delete administrative users, and define their passwords.
	Type **2**, press **Enter**, and the following submenu appears:
	`[0] Change Password`
	`[1] Add User`
	`[2] Delete User`
	`[3] List Users`
	`[4] Return to Main Menu`
	[0] Change Password lets you change a password for an existing user.
	[1] Add User lets you enter a username and password for a new user. Usernames must be at least 6 characters, and passwords must be at least 8 characters.
	[2] Delete User lets you delete users. Enter the complete username when prompted and press **Enter**. The name is deleted from the list.
	[3] List Users lists current administrative users.
	Type **4** to return to the Main menu.

[3] View System Information	Allows you to view the FlexLM host ID.
	Type **3**, press **Enter**, and you will see the following prompts:
	`[0] Get Host ID`
	`[1] Return to Main Menu`
	Type **0** to display the host ID information.
	Type **1** to return to the Main menu.

[4] Restart/Shutdown	Allows you to restart or shut down the CTE.
	Type **4**, press **Enter**, and you will see the following prompts:
	`[0] Restart`
	`[1] Shutdown`
	To restart the CTE, type **0** or **R**.
	To shut down the CTE, type **1** or **S**.
	Press any other key to exit this function without restarting or shutting down the device.

[5] Log Out	Allows you to log out of the console. Type **5** to log out.

CTE Administration Interface

The CTE Administration Interface lets you monitor and maintain the activity on your CTE from any browser on the Internet. Through this interface, you can specify or display information in the following four categories:

- Network, which lets you define interfaces, ports, DNS settings, static routes, and proxies.
- Advanced, which lets you define the default URL and host, session timeout, minimum session time, maximum buffer size, security, browser masquerade, input character encoding method, external caching, and the ability to enable JavaScript emulation, keepalive messages, and unrestricted proxy.
- Logging, which lets you define the SNMP location, contact, community, and port, and to enable logging of SNMP, system, and system health messages.
- Administration, which lets you specify files to upload, such as secure certificates, server upgrades, and licenses, and also manage users.

Logging On to the Administration Interface

To access the CTE Administration Interface, perform these steps:

Step 1 Make sure that the CTE console is running.

Step 2 From any browser, enter the URL:

https://<*IP-address*>**:**<*administration-port*>

where:

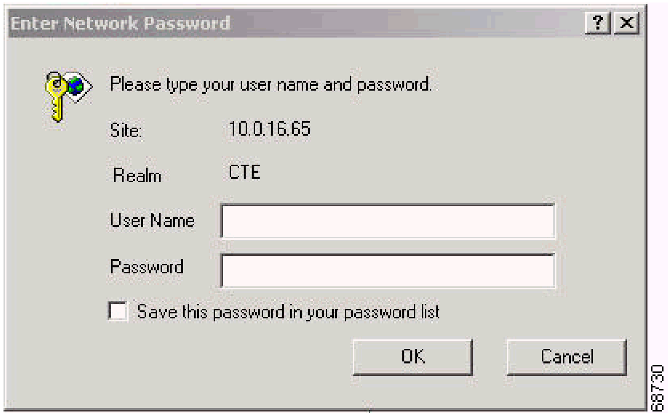
– <*IP_address*> is the IP address of your CTE

– <*administration-port*> is the administration port of your CTE (usually 9001)

Step 3 Click **Yes** on the Security Information dialog box.

The CTE Administration Interface login dialog, shown in Figure 11, appears.

Figure 11 Administration Interface Login


Enter Network Password

Please type your user name and password.

Site: 10.0.16.65

Realm CTE

User Name

Password

□ Save this password in your password list

Step 4 Log in as **root**, and enter your root password.

Note You can create additional administrative usernames and passwords from the CTE console. For more information, see the description of [2] Manage Administrative Users in Table 4 on page 24.

The initial CTE Administration screen appears. These screens are described in the following sections.

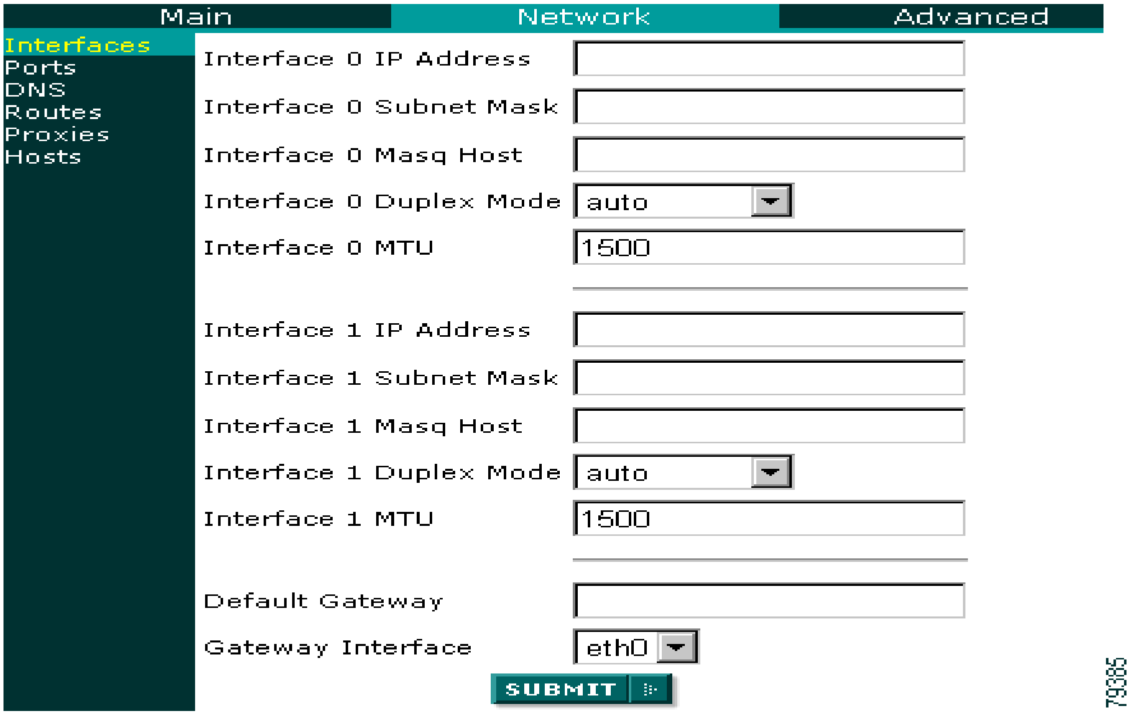
Specifying Network Settings

The first tab on the Administration screen, Network, is divided into the following screens:

- Interfaces Screen, page 33
- Ports Screen, page 34
- DNS Screen, page 35
- Routes Screen, page 35
- Proxy Screen, page 36

When you first open the CTE Administration screen, it appears as shown in Figure 12.

Figure 12 CTE Administration Screen



Interface 0 IP Address
Interface 0 Subnet Mask
Interface 0 Masq Host
Interface 0 Duplex Mode auto
Interface 0 MTU 1500

Interface 1 IP Address
Interface 1 Subnet Mask
Interface 1 Masq Host
Interface 1 Duplex Mode auto
Interface 1 MTU 1500

Default Gateway
Gateway Interface eth0

The CTE Administration screen has four tabs across the top representing the four areas of information that you can display and define. When the initial screen appears, the Network tab is displayed. There are five different Network administration screens, which are listed in the left column. The Interfaces screen is in view initially. To move between screens, click a screen name in the left column and the screen display will change to reflect your choice.

To save changes you make on any of the Administration screens, click the **Submit** button at the bottom of each screen.

Interfaces Screen

From the Interfaces screen, you can view and set the values shown in Table 5.

Table 5 Interfaces Screen Settings

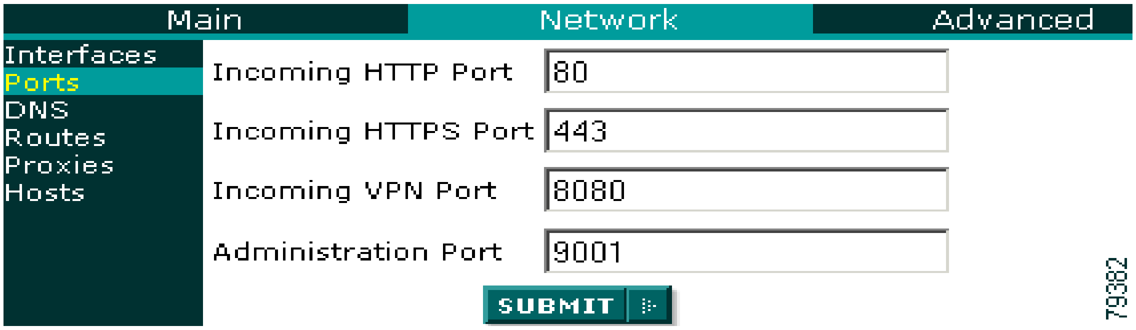
Setting	Description
Interface 0 IP Address	Specifies the IP address for Interface 0.
Interface 0 Subnet Mask	Specifies the subnet mask for Interface 0 (usually 255.255.255.0).
Interface 0 Masquerade Host	Specifies the current IP address for NAT for Interface 0, which makes all requests appear to originate from the same client. The current setting is displayed when the screen appears.
Interface 0 Duplex Mode	Specifies the duplex mode for Interface 0, which can be auto, full duplex, or half duplex.
Interface 0 MTU	Specifies the Maximum Transmission Unit (MTU) for Interface 0. The MTU defines the maximum size of each transmitted packet. The default value is 1500.
Interface 1 IP Address	Specifies the IP address for Interface 1.
Interface 1 Subnet Mask	Specifies the subnet mask for Interface 1 (usually 255.255.255.0).
Interface 1 Masquerade Host	Specifies the current IP address for NAT for Interface 1, which makes all requests appear to originate from the same client. The current setting is displayed when the screen appears.
Interface 1 Duplex Mode	Specifies the duplex mode for Interface 1, which can be auto, full duplex, or half duplex.
Interface 1 MTU	Specifies the MTU for Interface 1. The MTU defines the maximum size of each transmitted packet. The default value is 1500.
Default Gateway	Specifies the IP address of the default gateway device.
Gateway Interface	Specifies the gateway interface, which can be either eth0 or eth1.

Click the **Submit** button to save your changes.

Ports Screen

When you choose **Ports** in the left column of the Network screen, the information shown in Figure 13 appears:

Figure 13 Ports Screen



Incoming HTTP Port: 80

Incoming HTTPS Port: 443

Incoming VPN Port: 8080

Administration Port: 9001

Values for many of these items are already defined and displayed on the screen. You can change them to reflect changes in your configuration.

From the Ports screen, you can view and set values for each item on the screen, as shown in Table 6.

Table 6 Ports Screen Settings

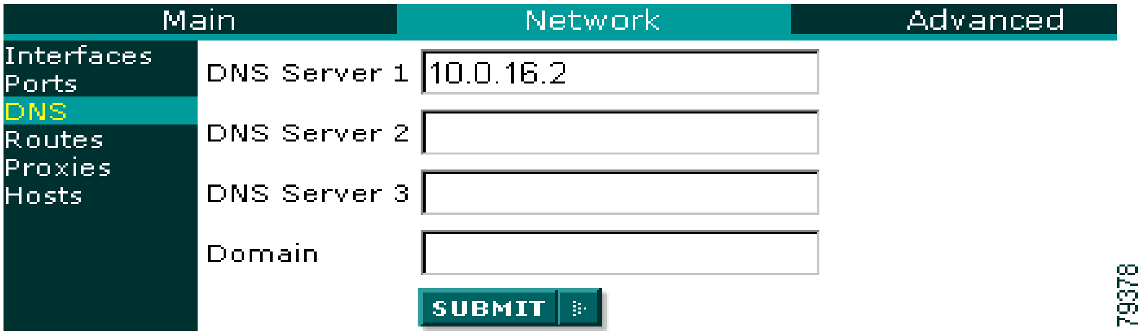
Setting	Description
Listen on Interface	Specifies the IP address of the HTTP Listener. The CTE will listen to one or more ports, depending on how you define the HTTP Listener: • If you accept the default value of 0.0.0.0 as the HTTP Listener IP address, no HTTP Listener is defined and the CTE will listen to both the eth0 and eth1 ports. • If the HTTP Listener is defined as an address that is similar to one of the Ethernet ports but dissimilar to the other—for example, 10.0.16.95 when eth0 is 10.0.16.65 and eth1 is 12.4.20.8, the CTE will listen to both the defined HTTP Listener machine and eth0. • If the HTTP Listener IP address is similar to both eth0 and eth1—for example, 10.0.16.95 when eth0 is 10.0.16.65 and eth1 is 10.0.16.98, the CTE will listen to all three IP addresses. • If the HTTP Listener is defined as an IP address that is dissimilar from the eth0 and eth1 ports, the CTE will listen to the defined HTTP Listener IP address only.
Incoming HTTP Port	Specifies the incoming HTTP port number.
Incoming HTTPS Port	Specifies the incoming HTTPS port number.
Administration Port	Specifies the ADMIN port number.

Click the **Submit** button to save your changes.

DNS Screen

When you choose **DNS** in the left column of the Network screen, the information shown in Figure 14 appears.

Figure 14 DNS Screen



DNS Server 1 10.0.16.2

DNS Server 2

DNS Server 3

Domain

From the DNS screen, you can view and set values for each item on the screen, as shown in Table 7.

Table 7 DNS Screen Settings

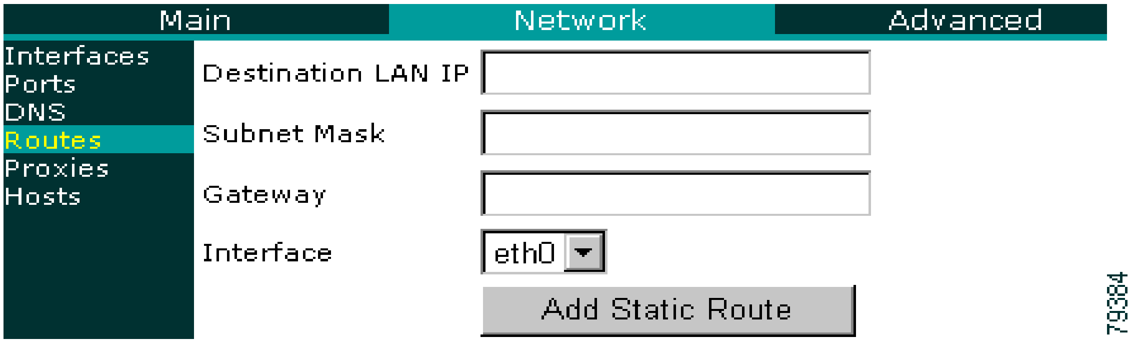
Setting	Description
DNS Server 1	Specifies the IP address of the first DNS server.
DNS Server 2	Specifies the IP address of the second DNS server.
DNS Server 3	Specifies the IP address of the third DNS server.
Domain	Specifies the DNS domain name.

Click the **Submit** button to save your changes.

Routes Screen

When you choose **Routes** in the left column of the Network screen, the information shown in Figure 15 appears.

Figure 15 Routes Screen



Destination LAN IP

Subnet Mask

Gateway

Interface eth0

From the Routes screen, you can view and set values for each item on the screen, as shown in Table 8.

Table 8 Routes Screen Settings

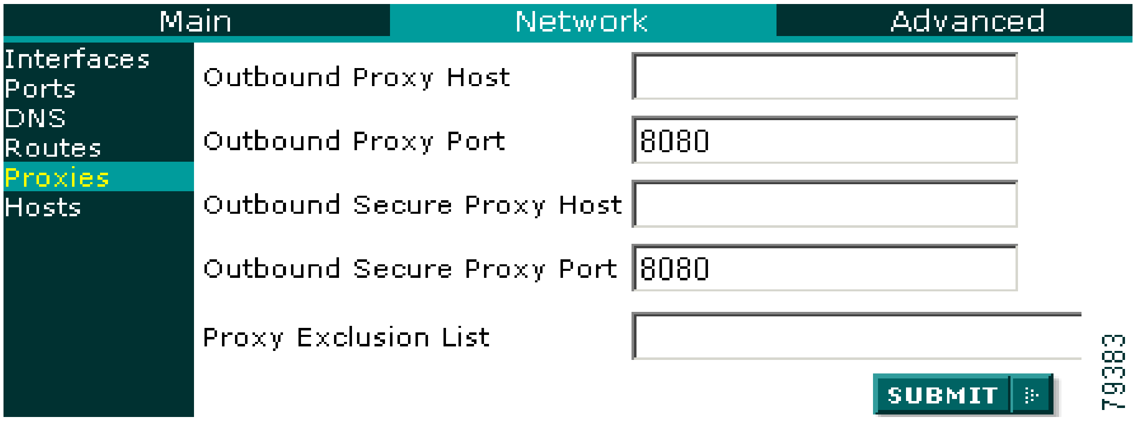
Setting	Description
Destination LAN IP	Specifies the IP address of the destination LAN.
Subnet Mask	Specifies the netmask for the gateway device.
Default Gateway	Specifies the IP address of the default gateway.
Interface	Specifies the interface that the default gateway uses, either eth0 or eth1. The default value is eth0.

When you have defined the route, click the **Add Static Route** button to save your changes.

Proxy Screen

When you choose **Proxy** in the left column of the Network screen, the information shown in Figure 16 appears.

Figure 16 Proxy Screen



Outbound Proxy Host

Outbound Proxy Port 8080

Outbound Secure Proxy Host

Outbound Secure Proxy Port 8080

Proxy Exclusion List

From the Proxy screen, you can view and set values for each item on the screen, as shown in Table 9.

Table 9 Proxy Screen Settings

Setting	Description
Outbound Proxy Host	Specifies the IP address of an outbound proxy server. This setting sets a proxy server for HTTP (nonsecure requests). If your CTE is behind a firewall or proxy server, the CTE will use these settings for HTTP requests.
Outbound Proxy Port	Specifies the outbound port number on the outbound proxy server.
Outbound Secure Proxy Host	Specifies the IP address of an outbound secure proxy server, which sets a proxy server for HTTPS (secure requests).
Outbound Secure Proxy Port	Specifies the outbound port number on the outbound secure proxy server.

Table 9 Proxy Screen Settings (continued)

Setting	Description
Local Proxy Exclusion	If checked, specifies that the defined proxy server is ignored in the local domain.
Proxy Exclusion List	Specifies any IP addresses, host names, or domain names that should not use the defined proxy server. Use a space between each item in the list to separate them.

Click the **Submit** button to save your changes.

Specifying Advanced Settings

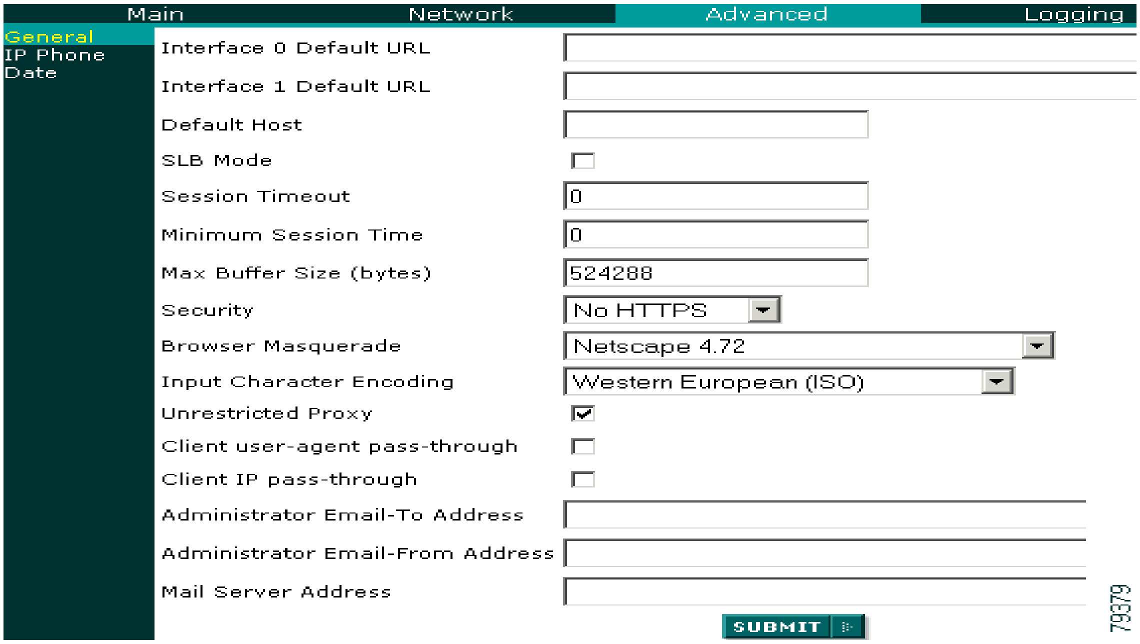
The second tab on the Administration screen, Advanced, is divided into the following screens:

- General Screen, page 37
- IP Phone Screen, page 40

General Screen

When you choose **General** in the left column of the Advanced screen, the information shown in Figure 17 appears.

Figure 17 General Screen



Interface 0 Default URL	
Interface 1 Default URL	
Default Host	
SLB Mode	□
Session Timeout	0
Minimum Session Time	0
Max Buffer Size (bytes)	524288
Security	No HTTPS
Browser Masquerade	Netscape 4.72
Input Character Encoding	Western European (ISO)
Unrestricted Proxy	☑
Client user-agent pass-through	□
Client IP pass-through	□
Administrator Email-To Address	
Administrator Email-From Address	
Mail Server Address	

From the General screen, you can view and set values for each item on the screen, as shown in Table 10.

Table 10 General Screen Settings

Setting	Description
Default URL	Specifies a default URL that the CTE will request if you attempt to access the CTE directly (for example, http://*cte_name*). Defining this field allows administrators to configure a default web page to proxy.
Default Host	Specifies a default host that the CTE uses if a request includes a relative link, such as http://*cte_address*. For any relative address received, the CTE will substitute the IP address of the default host that you specify.
Session Timeout	Specifies in minutes the session timeout interval, which is the amount of time a session is allowed to last. The default value for this setting is 30 minutes. For more information about sessions, see the "Sessions and Connections" section on page 6.
Minimum Session Time	Specifies in minutes the minimum session timeout interval, which is the period of time a session is guaranteed to remain active. Setting a minimum session time protects current users when the CTE has many active sessions. New users are denied, rather than evicting current users. The default value for this setting is 5 minutes. For more information about sessions, see the "Sessions and Connections" section on page 6.
Max Buffer Size (bytes)	Specifies the maximum buffer size. The default value is 524288.
Security	Specifies whether you are using secure connections. You can select either No HTTPS (none of your connections will be secure) or Force HTTPS (all of your connections will be secure).
Browser Masquerade	Specifies Netscape, Internet Explorer, or Content Mobility Engine. Because some application servers behave differently with one browser than the other, the first two options give you the ability to make the display look like a different browser. If you select Content Mobility Engine, this option specifies that the CTE will act as its own user agent.

Table 10 General Screen Settings (continued)

Setting	Description
Input Character Encoding	Specifies the input character encoding method, as follows: Western European (iso-8859-1, Latin-1, ASCII), Central/Eastern Europe (iso-8859-2, Latin-2), Esperanto (iso-8859-3, Latin-3), Baltic/Latvian/Lithuanian (iso-8859-4, Latin-4), Cyrillic (iso-8859-5), Greek (iso-8859-7), Turkish (iso-8859-9, Latin-5), Nordic (iso-8859-10, Latin-6), Latvian (iso-8859-13, Latin-7), Celtic (iso-8859-14, Latin-8), Western European (iso-8859-15, Latin-9), Romanian (iso-8859-16, Latin-10), Windows Eastern European (windows-1250, cp1250), Windows Cyrillic (windows-1251, cp1251), Windows Western European (windows-1252, cp1252), Windows Greek (windows-1253, cp1253), Windows Turkish (windows-1254, cp1254), Windows Baltic (windows-1257, cp1257), Western European (cp850, DOS Latin-1), Russian (cp866, DOS Russian), Russian (KO18-R), Ukranian (KO18-R), Russian/Ukranian (KO18-RU), MacRoman, MacCentralEurope, MacIceland, MacCroatian, MacRomania, MacCyrillic, MacUkraine, MacGreek, MacTurkish, Arabic (iso-8859-6), Hebrew (iso-8859-8), Windows Hebrew (windows-1255, cp1255), Windows Arabic (windows-1256, cp1256), Hebrew (cp862, DOS Hebrew), MacHebrew, MacArabic, Japanese (EUC-JP), Japanese (SHIFT-JIS), Japanese (cp932), Japanese (ISO-2022-JP), Japanese (ISO-2022-JP-2), Japanese (ISO-2022-JP-1), Chinese (GB2312, EUC-CN), Chinese (HZ), Chinese (GBK), Chinese (GB18030), Chinese (EUC-TW), Chinese (BIG5), Chinese (CP950), Chinese (BIG5-HKSCS), Chinese (ISO-2022-CN), Chinese (ISO-2022-CN-EXT), Korean (EUC-KR), Korean (CP949), Korean (ISO-2022-KR), Korean (JOHAB), Georgian-Academy, Georgian-PS, Thai (TIS-620), Thai (cp874), MacThai, Laotian (MuleLao-1), Vietnamese (cp1133), Vietnamese (VISCII), Vietnamese (TCVN), Vietnamese (windows-1258, cp1258), HP Western European (HP-ROMAN8), NEXTSTEP Western European, UTF-8, UCS-2, UCS-2BE, UCS-2LE, UCS-4, UCS-4BE, UCS-4LE, UTF-16, UTF-16BE, UTF-16LE, UTF-32, UTF-32BE, UTF-32LE, UTF-7, JAVA
JavaScript Emulation	Enables or disables JavaScript emulation. When this function is enabled, the CTE requires additional memory for each page, even if the page does not contain JavaScript. Unless a site requires JavaScript support, you should disable it.

Table 10 General Screen Settings (continued)

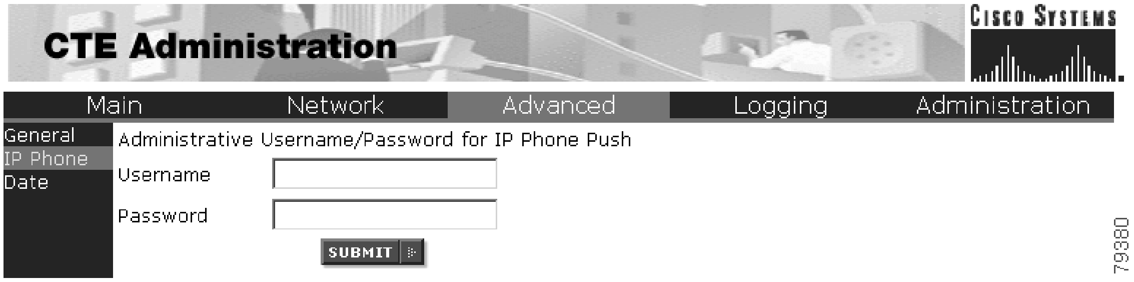
Setting	Description
Outbound KeepAlive	Enables or disables outbound keepalive messaging. When enabled, outgoing keepalive holds the connection to the server open for further requests.
Incoming KeepAlive	Enables or disables incoming keepalive messaging. When enabled, incoming keepalive holds the connection to the client open for further requests.
Unrestricted Proxy	Enables or disables unrestricted proxy support. When this function is enabled, the CTE proxies only the web pages that it has transformed to prevent access to protected servers that are on the same subnet as the CTE.

Click the **Submit** button to save your changes.

IP Phone Screen

When you choose **IP Phone** in the left column of the Advanced screen, the information shown in Figure 18 appears.

Figure 18 IP Phone Screen



Administrative Username/Password for IP Phone Push

Username

Password

From the IP Phone screen, you can define a default IP phone username and password, as shown in Table 11.

Table 11 IP Phone Screen Settings

Setting	Description
Username	Specifies a username to be used as the default IP phone username. This setting is necessary because some IP phones require a default username.
Password	Specifies a password to be associated with the default IP phone username.

Click the **Submit** button to save your changes.

Specifying Logging Settings

The third tab on the Administration screen, Logging, is divided into the following screens:

- Configure Screen, page 41
- System Log Screen, page 42
- Health Log Screen, page 43
- SNMP Screen, page 45

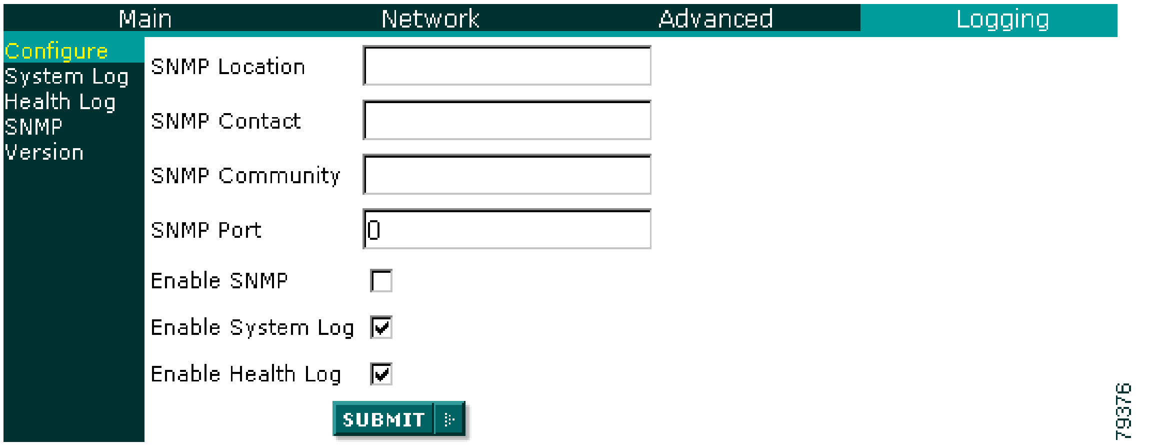
The logging features allow you to enable or disable the logging of system performance information and view the information collected during the logging. By reviewing the information provided, you can track unusual changes that can affect the stability and performance of the CTE.

Configure Screen

The Configure screen lets you define SNMP settings and enable all logging methods.

When you choose **Configure** in the left column of the Logging screen, the information shown in Figure 19 appears.

Figure 19 Configure Screen



SNMP Location

SNMP Contact

SNMP Community

SNMP Port 0

Enable SNMP □

Enable System Log ☑

Enable Health Log ☑

From the Configure screen, you can view and set values for each item on the screen, as shown in Table 12.

Table 12 Configure Screen Settings

Setting	Description
SNMP Location	Specifies the SNMP location, such as a rack, building, or network.
SNMP Contact	Specifies the name of the SNMP contact person.
SNMP Community	Specifies the password of the string that is used to read statistics from the CTE.
SNMP Port	Specifies the SNMP port number.
Enable SNMP	Enables or disables the logging of SNMP messages, which you can view from the SNMP screen of the Logging tab.

Table 12 Configure Screen Settings (continued)

Setting	Description
Enable System Log	Enables or disables the logging of system messages, which you can view from the System Log screen of the Logging tab.
Enable Health Log	Enables or disables the logging of health data, which you can view from the Health Log screen of the Logging tab.

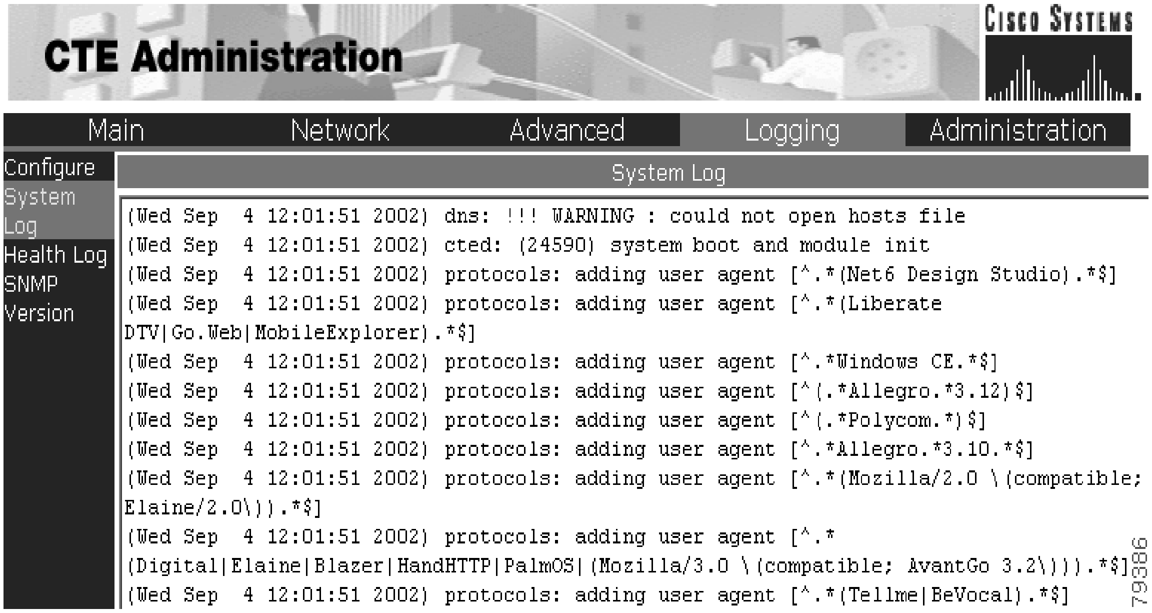
Click the **Submit** button to save your changes.

System Log Screen

Note Before you can view the System Log, make sure that you have enabled the logging of system messages on the Configure screen of the Logging tab.

When you choose **System Log** in the left column of the Advanced screen, you can view a log of system messages, as shown in Figure 20.

Figure 20 System Log Example



```
(Wed Sep  4 12:01:51 2002) dns: !!! WARNING : could not open hosts file
(Wed Sep  4 12:01:51 2002) cted: (24590) system boot and module init
(Wed Sep  4 12:01:51 2002) protocols: adding user agent [^.*(Net6 Design Studio).*$]
(Wed Sep  4 12:01:51 2002) protocols: adding user agent [^.*(Liberate
DTV|Go.Web|MobileExplorer).*$]
(Wed Sep  4 12:01:51 2002) protocols: adding user agent [^.*Windows CE.*$]
(Wed Sep  4 12:01:51 2002) protocols: adding user agent [^(.*Allegro.*3.12)$]
(Wed Sep  4 12:01:51 2002) protocols: adding user agent [^(.*Polycom.*)$]
(Wed Sep  4 12:01:51 2002) protocols: adding user agent [^.*Allegro.*3.10.*$]
(Wed Sep  4 12:01:51 2002) protocols: adding user agent [^.*(Mozilla/2.0 \(compatible;
Elaine/2.0\)).*$]
(Wed Sep  4 12:01:51 2002) protocols: adding user agent [^.*
(Digital|Elaine|Blazer|HandHTTP|PalmOS|(Mozilla/3.0 \(compatible; AvantGo 3.2\))).*$]
(Wed Sep  4 12:01:51 2002) protocols: adding user agent [^.*(Tellme|BeVocal).*$]
```

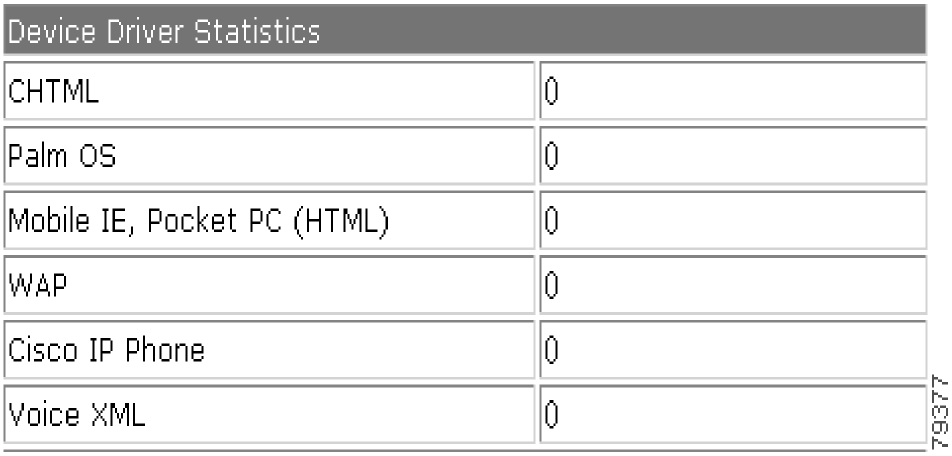
Health Log Screen

Note Before you can view health data, make sure that you have enabled the Health Log setting on the Configure screen of the Logging tab.

When you choose **Health Log** in the left column of the Advanced screen, the administration interface displays two types of information:

- Device Driver Statistics, shown in Figure 21 on page 43
- Load Statistics, shown in Figure 22 on page 44

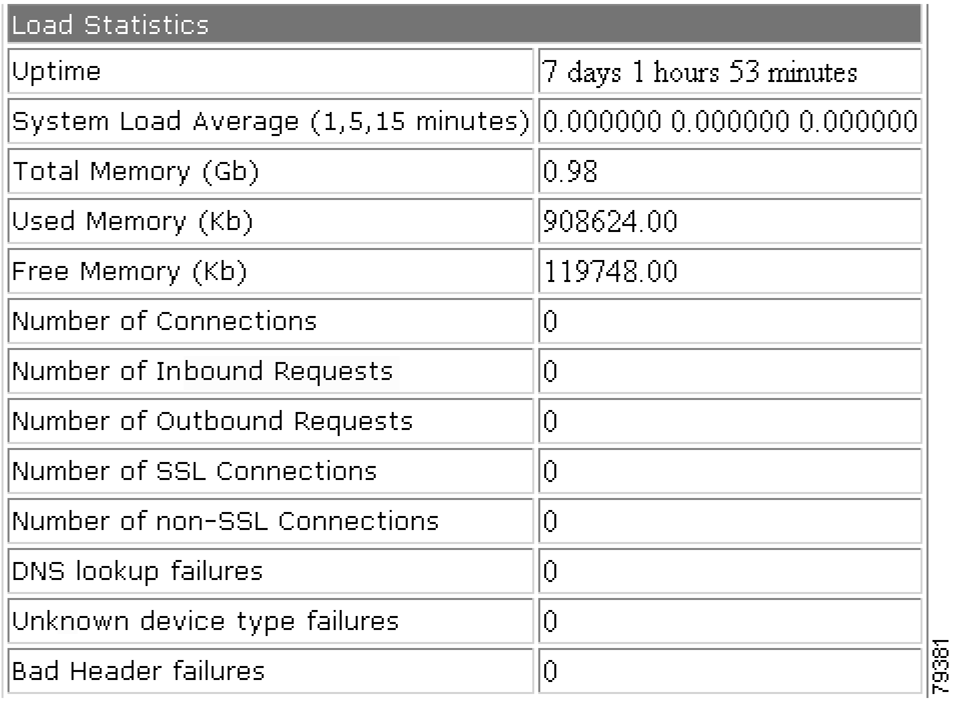
Figure 21 Device Driver Statistics



Device Driver Statistics	
CHTML	0
Palm OS	0
Mobile IE, Pocket PC (HTML)	0
WAP	0
Cisco IP Phone	0
Voice XML	0

The fields in this portion of the screen display the number of requests received from each listed device.

Figure 22 Load Statistics



Load Statistics	
Uptime	7 days 1 hours 53 minutes
System Load Average (1,5,15 minutes)	0.000000 0.000000 0.000000
Total Memory (Gb)	0.98
Used Memory (Kb)	908624.00
Free Memory (Kb)	119748.00
Number of Connections	0
Number of Inbound Requests	0
Number of Outbound Requests	0
Number of SSL Connections	0
Number of non-SSL Connections	0
DNS lookup failures	0
Unknown device type failures	0
Bad Header failures	0

The fields in this portion of the screen display:

- Up Time—Displays how long the CTE has been running in the current session, in days, hours, and minutes.
- System Load Average—Displays the average system load, measured for the past 1, 5, and 15 minutes.
- Total Memory (Gb)—Displays the total memory capacity.
- Used Memory (Kb)—Displays the amount of memory used.
- Free Memory (Kb)—Displays the amount of free memory.
- Number of Connections—Displays the number of connections serviced.
- Number of Inbound Requests—Displays the number of requests coming to the CTE.
- Number of Outbound Requests—Displays the number of requests going out from the CTE.
- Number of SSL Connections—Displays the number of Secure Sockets Layer connections.
- Number of non-SSL Connections—Displays the number of non-Secure Sockets Layer connections.
- DNS lookup failures—Displays the number of requests that failed because of DSN lookup failure.
- Unknown device type—Displays the number of requests that failed because the device type was unknown.
- Bad header failures—Displays the number of requests that failed because of bad header addresses.

SNMP Screen

Note Before you can view the SNMP Log, make sure that you have enabled the logging of SNMP messages on the Configure screen of the Logging tab.

When you choose **SNMP** in the left column of the Advanced screen, you can view a log of SNMP messages.

Specifying Administration Settings

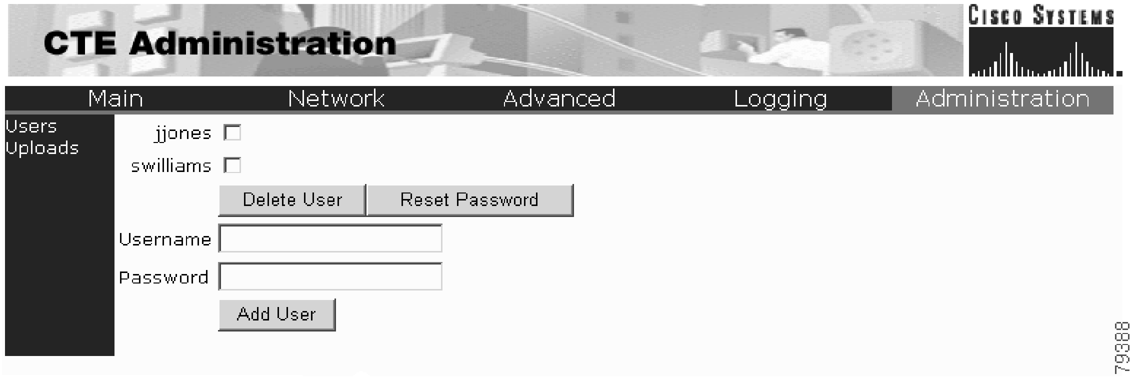
The fourth tab on the Administration screen, Administration, is divided into the following screens:

- Users Screen, page 45
- Uploads Screen, page 46

Users Screen

When you choose **Users** in the left column of the Administration screen, the information shown in Figure 23 appears.

Figure 23 Users Screen



From the Users screen, you can create new Design Studio users, delete users, and change user passwords. The fields for Username and Password are shown in Table 13.

Table 13 Users Screen Settings

Setting	Description
Username	Specifies a username. Usernames must be at least 6 characters.
Password	Specifies the password to be associated with the username. Passwords must be at least 8 characters.

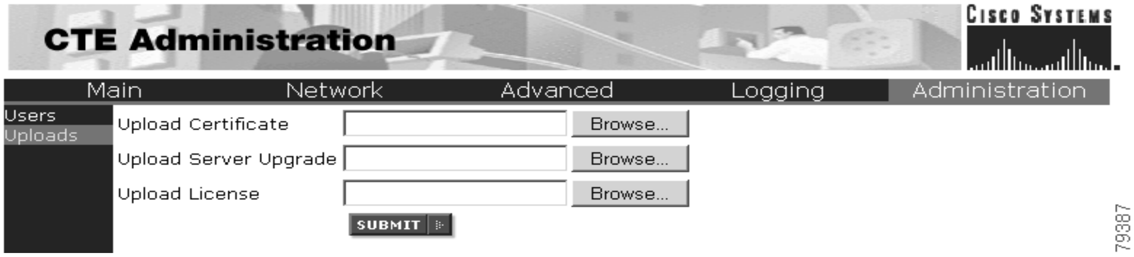
Use the buttons on the Users screen as follows:

- Add User—To add a user, click the **Add User** button after you have defined a username and password. Once added, the new username appears in the upper left corner of the window with a checkbox in front of it. When you delete or change the password for a username, click the checkbox to indicate the username with which you are working.
- Delete User—To delete a user, click the checkbox next to the username that you want to delete, and click the **Delete User** button.
- Reset Password—To reset the password of an existing user, click the checkbox next to the username, enter the new password, and click the **Reset Password** button.

Uploads Screen

When you choose **Uploads** in the left column of the Administration screen, the information shown in Figure 24 appears.

Figure 24 Uploads Screen



From the Uploads screen, you can view and set values for each item on the screen, as shown in Table 14.

Table 14 Uploads Screen Settings

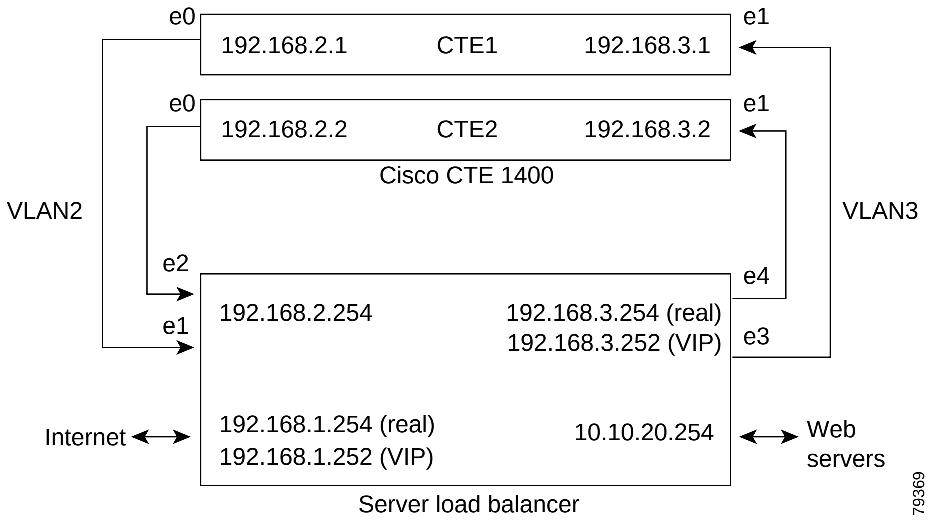
Setting	Description
Upload Certificate	Specifies a secure certificate file to upload. To upload the file, click the **Browse** button, and locate the file you want to upload.
Upload Server Upgrade	Specifies a server upgrade file to upload. To upload the file, click the **Browse** button, and locate the file you want to upload.
Upload License	Specifies a license file to upload. To upload the file, click the **Browse** button, and locate the file you want to upload.

Click the **Submit** button to save your changes.

Configuration Example

This section contains the CTE console/administration and CLI commands needed to configure two CTEs with a Cisco CSS 11000, as shown in Figure 25.

Figure 25 CTE Connected to Server Load Balancer



To configure network parameters for CTE1, perform these steps from the CTE console and CTE Administration Interface:

	Task	Application	Command/Field

Step 1	Display the current configuration.	Console	`[1] Configure Network Interface`
			`[6] Display Configuration`

Step 2	Specify the IP address and netmask for eth0.	Console	`[1] Configure Network Interface`
			`[0] Configure Interface 0`
			`[0] Set IP Address`
			`IP address [x.x.x.x]`
			`[Enter 0 to clear]` **`192.168.2.1`**
			`[1] Set Netmask`
			`Netmask [x.x.x.x]`
			`(Enter 0 to clear)` **`255.255.255.0`**
			`[5] Return to Network Menu`

Step 3	Specify the IP address and netmask for eth1.	Console	`[1] Configure Interface 1`
			`[0] Set IP Address`
			`IP address [x.x.x.x]`
			`[Enter 0 to clear]` **`192.168.3.1`**
			`[1] Set Netmask`
			`Netmask [x.x.x.x]`
			`(Enter 0 to clear)` **`255.255.255.0`**
			`[5] Return to Network Menu`

Step 4	Specify eth1/NIC 2 as the gateway device.	Console	`[3] Set Gateway`
			`Gateway [x.x.x.x]` **`192.168.2.1`**
			`[4] Set Gateway Device`
			`Gateway Device (eth0,eth1) []` **`eth1`**

Step 5	Review your changes.	Console	`[6] Display Configuration`

	Task	Application	Command/Field
Step 6	Save your changes.	Console	When prompted to commit your changes, type **yes**.

Step 7	Open the CTE Administration interface.	Web browser	`Enter the URL:`
			`https://ip-address:administration-port`
			`Enter your administrative username and password.`

Step 8	Set the subnet mask for the CTE.	CTE Administration	`Network tab`
			`Interfaces screen`
			`Interface 0 Subnet Mask` **`255.255.255.0`**

Step 9	Specify the IP address of the default web server.	CTE Administration	`Advanced tab`
			`General screen`
			`Default URL` **`10.10.20.22`**

Step 10	Specify the IP address for NAT.	CTE Administration	`Network tab`
			`Interfaces screen`
			`Interface 0 Masquerade Host` **`192.168.2.1`**

Step 11	Save any changes made in the CTE Administration screens.	CTE Administration	`Click the` **`Submit`** `button.`

To configure network parameters for additional CTEs, perform the same steps as you did for CTE1, specifying the following unique information for each CTE:

- IP addresses for eth0 and eth1 on the Console menu
- IP address for the masquerade host in the Administration interface

To configure the server load balancer, perform these steps from a computer that is connected to the console port of the server load balancer and logged into the CSS:

Note The following steps are representative of what is required to configure a server load balancer. The specific commands that you need to use are based on your network topology.

	Task	Command
Step 1	Enter configuration mode.	`#` **`config`**

Step 2	Enter interface mode for each interface you want to configure, and then bridge the interface to the VLAN.
	Note These commands establish the interfaces between the server load balancer and VLANs 2 and 3.
		`(config)#` **`interface ethernet-1`**
		`(config-if[e1])#` **`bridge vlan 2`**
		`(config-if[e1])#` **`exit`**
		`(config)#` **`interface ethernet-2`**
		`(config-if[e2])#` **`bridge vlan 2`**
		`(config-if[e2])#` **`exit`**
		`(config)#` **`interface ethernet-3`**
		`(config-if[e3])#` **`bridge vlan 3`**
		`(config-if[e3])#` **`exit`**
		`(config)#` **`interface ethernet-4`**
		`(config-if[e4])#` **`bridge vlan 3`**
		`(config-if[e4])#` **`exit`**

	Task	Command
Step 3	Assign an IP address and subnet mask to each circuit.	(config)# **circuit VLAN2** (config-circuit[VLAN2])# **ip address 192.168.2.254 255.255.255.0** (config-circuit-ip [VLAN2-192.168.2.254])# **exit** (config-circuit[VLAN2])# **exit** (config)# **circuit VLAN3** (config-circuit[VLAN3])# **ip address 192.168.3.254 255.255.255.0** (config-circuit-ip [VLAN3-192.168.3.254])# **exit** (config-circuit[VLAN3])# **exit**
Step 4	Create services for CTE1 and CTE2, assign an IP address to the services, and activate the services.	(config)# **service cte** (config-service[cte1])# **ip address 192.168.2.1** (config-service[cte1])# **active** (config-service[cte1])# **service cte2** (config-service[cte2])# **ip address 192.168.2.2** (config-service[cte2])# **active** (config-service[cte2])# **exit**
Step 5	Create an owner.	(config)# **owner cte**
Step 6	Create and configure a Layer 3 content rule for the CTE1 and CTE2 services using the owner just created.	(config-owner[cte])# **content L3Rule1** (config-owner-content[cte-L3Rule1])# **vip address 192.168.1.252** (config-owner-content[cte-L3Rule1])# **balance roundrobin** (config-owner-content[cte-L3Rule1])# **add service cte1** (config-owner-content[cte-L3Rule1])# **add service cte2** (config-owner-content[cte-L3Rule1])# **active** (config-owner-content[cte-L3Rule1])# **exit**

Creating Logins for Design Studio Users

Upon startup, Design Studio prompts for a username, password, CTE IP address, and server upload port. The username and password are created through the CTE Administration screens.

To create a login for a Design Studio user, perform these steps:

Step 1 In the CTE Administration screens, click the **Administration** tab at the top of the screen.

Step 2 Click **Users** in the left column.

Step 3 In the Username field, type a username of at least six characters.

Step 4 In the Password field, type a password of at least eight characters.

Step 5 Click the **Add User** button.

Shutting Down and Restarting the CTE Server Software

Always use the CTE console to shut down the CTE. Never shut down the CTE by powering off the CTE.

To shut down the CTE server software, perform these steps:

Step 1 In the CTE console, type **4** (Restart/Shutdown) and press **Enter**.

Step 2 Type **1** or **S** and press **Enter**.

To restart the CTE server software, perform these steps:

Step 1 In the CTE console, type **4** (Restart/Shutdown) and press **Enter**.

Step 2 Type **0** or **R** and press **Enter**.

Uploading a Secure Certificate to the CTE

The CTE Design Studio accepts by default a Privacy Enhanced Mail (PEM) format certificate file for upload to the CTE. PEM is a text format that is the Base 64 encoding of the Distinguished Encoding Rules (DER) binary format. The PEM format specifies the use of text BEGIN and END lines that indicate the type of content that is being encoded.

The certificate must have the following characteristics:

- It must be in PEM format and include a private key.
- The private key must be unencrypted.

  If the private key is encrypted, you must use the CTE console to start the CTE each time the appliance powers up.

This section describes how to perform the tasks associated with uploading a secure certificate:

- Generating the Certificate Signing Request, page 51
- Unencrypting the Private Key, page 51
- Combining the Private Key with the Signed Certificate, page 52
- Generating Trusted Certificates for Multiple Levels, page 52

Generating the Certificate Signing Request

To generate a certificate signing request (CSR), perform these steps:

Step 1 Open the CertMaker.exe file, provided on the Design Studio CD.

Step 2 Follow the instructions to create your request, naming the CSR file and specifying where it will reside.

The program will create two files:

- The CSR file, which is saved with a .csr extension
- The private key file, which is saved with a .pvk extension

Step 3 Submit your CSR to the Certificate Authority (CA), as instructed by the CertMaker program.

The CA will return a Signed Certificate to you by e-mail within several days.

Unencrypting the Private Key

To unencrypt the private key, perform these steps:

Step 1 In Linux, enter the **openssl rsa** command.

If you enter this command without arguments, you will be prompted as follows:

```
read RSA key
```

Step 2 Enter the name of the password to be encrypted.

You can enter the **openssl rsa** command with arguments if you know the name of the private key and the unencrypted PEM file.

In the following example, if the private key filename is cte_keytag_key.pvk, and the unencrypted filename is keyout.pem, you would enter the **openssl rsa -in cte_keytag_key.pvk -out keyout.pem** command.

For more information, refer to the following URL:

http://www.openssl.org/docs/apps/rsa.html#EXAMPLES

For information on downloading OpenSSL for Windows, refer to the following URL:

http://sourceforge.net/project/showfiles.php?group_id=23617&release_id=48801

Combining the Private Key with the Signed Certificate

When you have received the Signed Certificate from the CA, before you can upload it to the CTE, you must combine it with the Private Key. To do this, perform these steps:

Step 1 Combine the unencrypted Private Key with the Signed Certificate in the PEM file format. The file contents will look similar to the following:

```
-----BEGIN RSA PRIVATE KEY-----
    <Unencrypted Private Key>
-----END RSA Private KEY-----
-----BEGIN CERTIFICATE-----
    <Signed Certificate>
-----END CERTIFICATE-----
```

Step 2 Save and name the PEM file. For example, you can name the file CTE.pem.

Step 3 In the CTE Administration interface, go to the Network tab, and from the Interfaces screen, set the value for Interface 0 Masq Host to the DNS name for which the certificate was registered.

Step 4 In the CTE Administration interface, go to the Administration tab, click the **Uploads** screen, and choose **Upload Certificate**.

Step 5 Browse to the certificate file and select it.

Step 6 Click the **Submit** button.

Generating Trusted Certificates for Multiple Levels

Caution Any certificate that has more than one level *must* include all intermediate certificates, or the system may become unusable.

To see if your certificate has more than one level, and if it does, to handle the intermediate certificates properly, perform these steps:

Step 1 Do not exit Design Studio.

Step 2 Open Internet Explorer, and access a page through the CTE. For example, enter a URL similar to the following:

https://<*IP_address*>**:**<*http_port*>**//www.google.com**

where:

- <*IP_address*> is the IP address of your CTE
- <*http_port*> is the four-digit port HTTP port number

Step 3 Double-click the Lock symbol in the bottom right corner of the browser.

Step 4 Switch to the Certificate Path window pane at the top of the screen.

Step 5 Double-click the first path level to bring up the Certificate information for the first level and go to the Details screen.

Step 6 Click the **Copy to File** button at the bottom. A Certificate Export Wizard appears. Click **Next**.

Step 7 Make sure that the format selected is: "DER encoding binary X.509(.CER)"

Step 8 Click **Next**.

Step 9 Enter a filename. For example, you can enter **G:\tmp\root.cer**.

Step 10 Review the information and note the complete filename. Click **Finish**.

Step 11 Click **OK** to close the Certificate information window for the first level.

Step 12 Repeat Steps 5–11 for all levels except the last level.

Step 13 Insert all certificates into one file, and make sure that any intermediate certificates are part of any certificate file you upload.

The format of the uploaded file should be the following:

private key
Server Certificate
Intermediate Certificate 0
Intermediate Certificate 1
Intermediate Certificate 2

Proxy Settings for Design Studio and CTE

The CTE and Design Studio each have proxy settings that you will want to set if your network does not allow your computer access to HTTP or HTTPS traffic.

You will need to set up proxy settings in the following circumstances:

- **CTE:** If your CTE is behind a firewall or proxy server, you will need to set up CTE proxy settings through the Administration Interface. For more information, see the "Proxy Screen" section on page 36.
- **Design Studio:** If there is a firewall or proxy server between the computer on which Design Studio is installed and the CTE, Design Studio users will need to set up proxy settings. When they are starting Design Studio, users can set up proxy settings by clicking Use Proxy and specifying the host and port for HTTP and HTTPS connections. For more information, see the "Starting Design Studio" section of the *Design Studio User Guide*.

Using Static Routes

When setting up communication with another host or network, you will sometimes need to create a static route from the CTE to the new destination. Static routes are set up on the CTE port not being used by the default gateway. To create a static route, use the Set Routes option on the CTE console.

Creating a Static Route

To create a static route, perform these steps:

Step 1 From the CTE Administration screens, go to the Network tab, and click **Routes** in the left column.

Step 2 Enter the IP address of the destination LAN.

Step 3 Enter the subnet mask for the gateway device. The default is 255.255.255.0.

Step 4 Enter the IP address for the default gateway.

Step 5 Enter the gateway device when prompted: **eth0** or **eth1** (eth0 is the default).

Step 6 Click the **Add Static Route** button.

Step 7 From the CTE console, select [**1**] Configure Network Interfaces.

Step 8 Select [**5**] Ping.

Step 9 Enter the host IP address for the device you want to ping, and press **Enter**.

If you are successfully communicating with the other machine, messages will appear saying that the same number of packets were transmitted and received, and zero packets were lost. If you are not communicating with the other machine, these status messages will indicate that zero packets were received and all the packets were lost.

If you are not communicating with the other machine, return to step 1 and create the static route again.

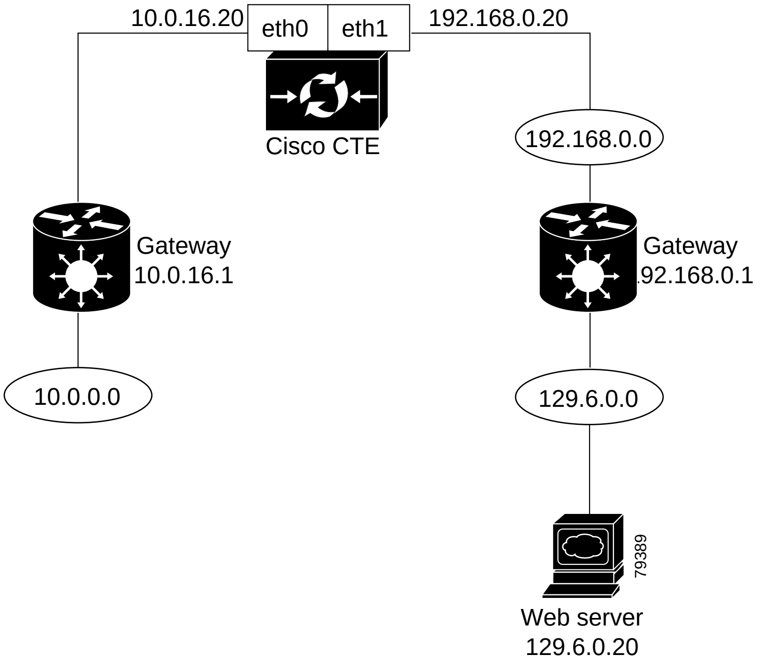
If you are communicating with the other machine, the route was created successfully.

Static Route Example

When the CTE receives a request that requires access to an IP address to which it is not currently connected, creating a static route creates a path to the new destination.

Suppose that the IP address of the eth0 port on your CTE is 10.0.16.20 and there has been a request to access information at 129.6.0.20 to which you currently have no path. You can create a static route through the Ethernet port that is not set as your CTE's default gateway and out to the requested network address, as shown in Figure 26.

Figure 26 Building a Static Route



In Figure 26, you can see the following connections:

- The eth0 port (IP address 10.0.16.20) leads to the default gateway (IP address 10.0.16.1), which connects to the rest of the 10.0.0.0 network.
- The eth1 port (IP address 192.168.0.20) is set to communicate with the 192.168.0.0 network and its gateway (IP address 192.168.0.1). Through this gateway, the eth1 port can communicate with the 129.6.00 network and the web server at IP address 129.6.0.20.

To set up this static route you need to establish the path between the eth1 port and IP address 129.6.0.20.

To set up the static route, perform these steps:

Step 1 From the CTE Administration screens, go to the Network tab, and click **Routes** in the left column.

Step 2 Define the IP address of the destination LAN as **129.6.0.0**.

Step 3 Define the subnet mask for the gateway device as the default value, 255.255.255.0.

Step 4 Define the IP address of the default gateway as **192.168.0.1**.

Step 5 Define the gateway device as **eth1**.

Step 6 Click the **Add Static Route** button.

Recovering from a CTE Crash

If the CTE device fails, follow the instructions in the *CTE Hardware Installation Guide* for diagnosing and recovering from a hardware failure. Once the hardware is operational, reinstall the CTE from the CD provided with the device.

To reinstall the CTE, perform these steps:

Step 1 Insert the installation CD in the CD-ROM drive of the CTE to start the installer.

Step 2 When the installation completes, power off the CTE.

Step 3 Power on the CTE. As the device starts, eject the CD.

The CTE console menu displays a message informing you whether the installation was successful.

Troubleshooting a CTE

The following information explains how to deal with problems you might encounter when setting up and using the CTE.

The CTE does not start and the CTE console is blank.

Verify that the following are correctly set up:

- The serial console is using the correct port and the physical and logical ports match.
- The cable is a null-modem cable.
- The COM settings in your serial communication software are set to 9600 bits per second, 8 data bits, no parity, and 1 stop bit.

Wireless devices or device simulators cannot communicate with the CTE.

Verify that the following are correctly set up:

- The masquerade IP address specified in the CTE Administration Interface (Network tab, Interfaces screen) is available outside of your firewall.
- Any changes made in the CTE console have been committed.
- The devices are configured to access the correct IP address and port number.

Rules created in Design Studio are not in effect on wireless devices or device simulators.

If you are sure that the rules are correctly created and applied in Design Studio and that they have been uploaded to the CTE, verify the CTE configuration as follows:

- The server load balancer or switch connected to the CTE is set up to recognize wireless devices.
- Wireless device traffic is directed through the CTE.
- The CTE is intercepting traffic from wireless devices.

I tried using Ctrl-Alt-Delete to reboot the CTE, but nothing happened.

The reboot function on the CTE is disabled. You must use the CTE console to start and stop the device.

The CTE does not work with European-made phones.

By default, the CTE redirects traffic from HTTP to HTTPS. European-made phones do not support those secure redirects, so if you are using this type of phone you must disable secure redirects for the CTE. To do that, go to the CTE Administration interface, and under the General screen on the Advanced tab, set the Security field to No HTTPS, and click the **Submit** button to commit the change. (Be aware that no HTTPS sites can be proxied when you set this field to No HTTPS.)

SSLV2 sessions do not work with a multi-level certificate chain

If intermediate (multi-level) certificates are part of your secure certificate upload, you need to make sure that the intermediate certificates are part of the certificate file that you are uploading. Any certificate that has more than one level must include all intermediate certificates, or the system may become unusable. For information about how to add intermediate certificates to the uploaded certificate file, see the "Uploading a Secure Certificate to the CTE" section on page 50.

Because SSLV2 does not support certificate chaining, if you have a multi-level certificate, it will not work to support SSLV2 sessions.

Related Documentation

For more information about the CTE, refer to the following publications:

- *CTE and Design Studio Quick Start Guide*
- *CTE Hardware Installation Guide*
- *Release Notes for CTE and Design Studio*

For information about using Design Studio, see the *Cisco CTE Design Studio User Guide*.

Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following URL:

http://www.cisco.com

Translated documentation is available at the following URL:

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

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

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

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click the **Fax** or **Email** option under the “Leave Feedback” section at the bottom of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408 527-0730.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

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

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to the following URL to register:

http://www.cisco.com/register/

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.

This document is to be used in conjunction with the documents listed in the “Related Documentation” section.