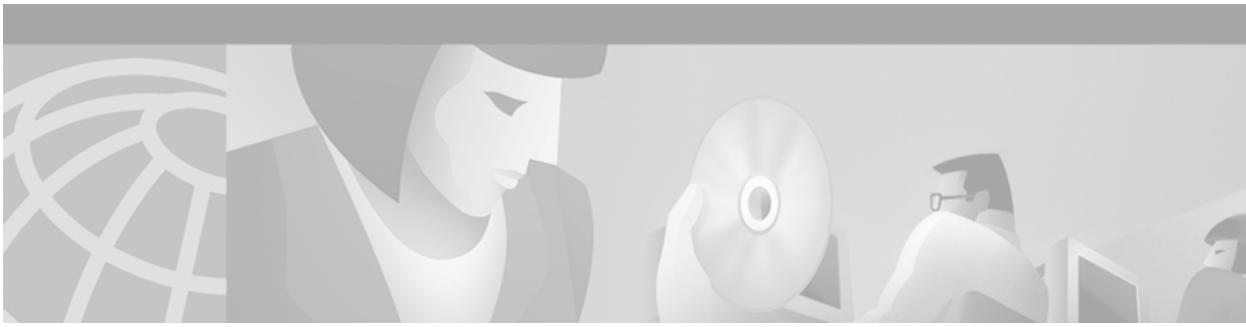


Cisco Content Transformation Engine 1400 Configuration Note

Product Number: 74-2552-01

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

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

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 Cisco CTE 1400 can result in a security risk. Before you deploy the Cisco CTE 1400, verify the configuration as follows:

- Verify that the CTE does not have access to protected intranet sites.

  By default, the CTE proxies only the web pages it has transformed in order to prevent access to protected servers that are on the same subnet as the CTE. If you choose to override that default, as described in the "Configuring the Cisco CTE 1400 to Proxy All Web Pages" section on page 17, do not put the CTE on the same subnet as 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 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*.

- 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. To assure secure operations, you must block access to CTE port 9001 from outside of your firewall.

Overview

The Cisco CTE 1400 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, firewall, Virtual Private Network (VPN) solutions, routers, and IEEE 802.11 broadband wireless devices.

Use the CTE Design Studio, a PC-based application, to create transformation rules for a set of content and to upload the rules to a CTE.

These sections describe the Cisco CTE 1400:

Features

Table 1 summarizes the features of the Cisco CTE 1400.

Table 1 Cisco CTE 1400 Features

Feature	Description
Performance and Scalability	• Each CTE supports up to 1400 simultaneous connections. • Each CTE supports 10,000 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 Javascript, 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 all of those requirements on many devices automatically. Supported devices include: • Cisco IP Phone (XML) • Wireless phones (WAP 1.1-enabled phones using WML[1] version 1.1) • Handspring devices and Palm VII (Palm HTML) • Compact iPAQ, Hewlett Packard Jornada, and RIM[2] devices (cHTML[3]) • Desktop computers (HTML/XML) Supports web site 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 • XSL[4] version 1.0 • GIF, JPEG, BMP, and WBMP image formats

Table 1 Cisco CTE 1400 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” button 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.
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 in conjunction 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 10 seconds of inactivity (just like clients that use HTTP Keep-Alive).

Table 1 Cisco CTE 1400 Features (continued)

Feature	Description
Security[5]	• 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. • Has only three available ports: 80 (for requests from wireless devices), 443 (requests from wireless devices are directed to this secure port during operations), 9001 (for communication with Design Studio).

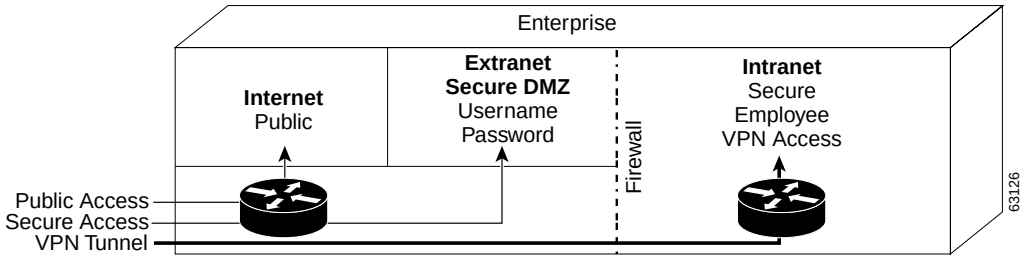
1. WML = Wireless Markup Language.
2. RIM = Research in Motion.
3. cHTML = Compact HTML.
4. XSL = Extensible Stylesheet Language.
5. For more information, see the "Security" section on page 5.
6. PEM = Privacy Enhanced Mail.

Security

Internet, extranet, and intranet sites require different levels of security, all supported by the Cisco CTE 1400. 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

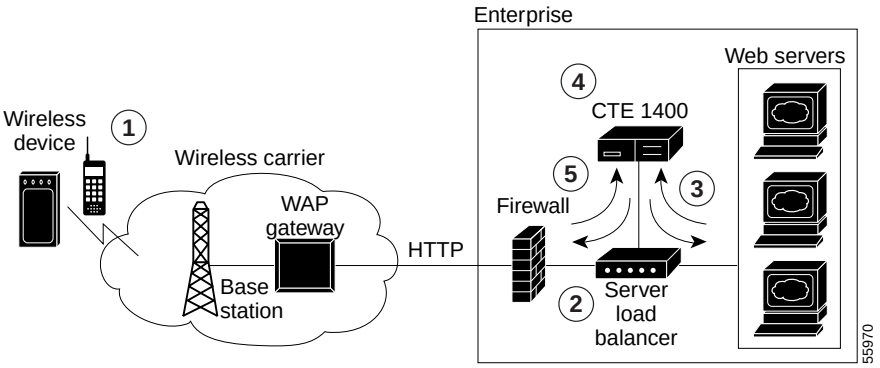
The CTE terminates Secure Sockets Layer (SSL) sessions to provide an endpoint for a secure link. Some PDAs support SSL connections from the device to the CTE. However, WAP phones and the Palm 7 device do not support SSL. WAP phones use Wireless Transport Layer Security (WTLS) and Palm 7 devices use Elliptical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

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 best for sites where most of the network traffic intercepted by the CTE uses content supplied by 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.

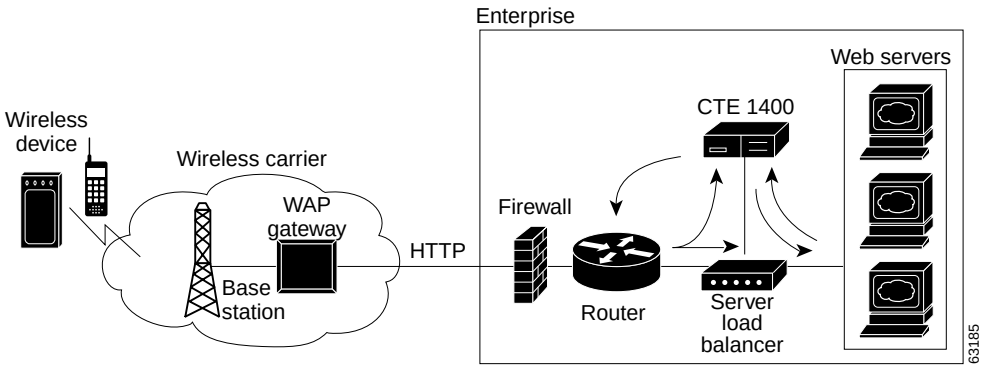
The path the wireless user request takes is as follows:

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 Cisco CTE 1400.
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 best 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.

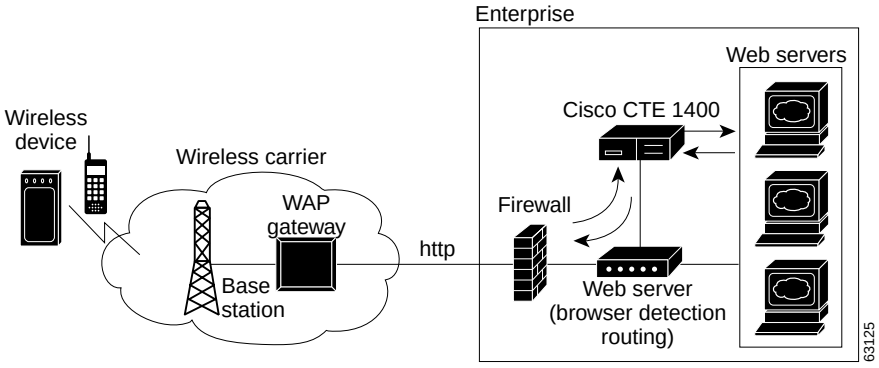
Figure 3 CTE Connected to Router and Server Load Balancer



CTE Connected to Web Server

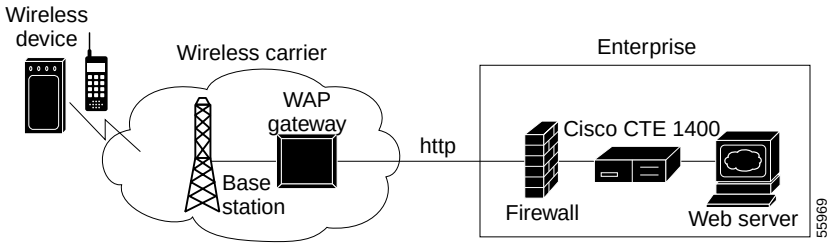
You can connect a CTE to a web server that routes traffic to the CTE or to web servers based on browser detection, as shown in Figure 4.

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 best when you designate specific IP addresses for wireless traffic.

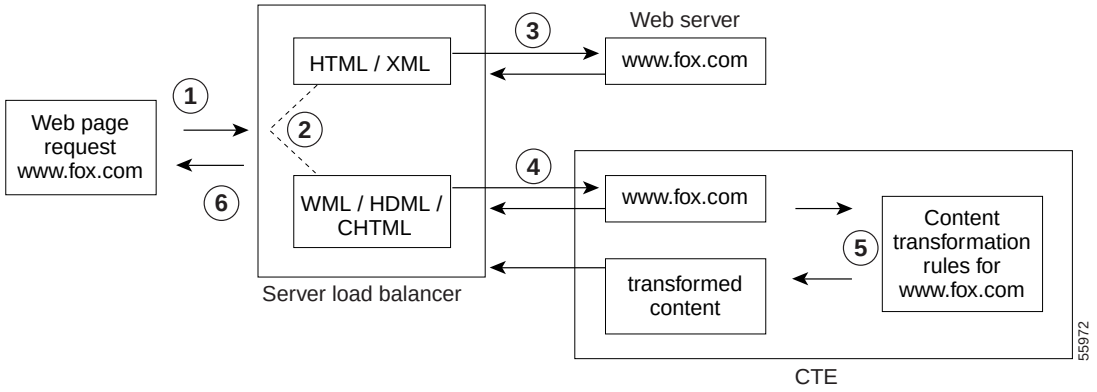
Figure 5 CTE In-line Connection



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.

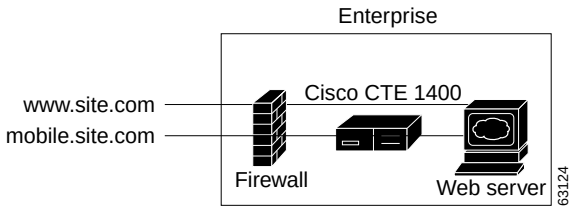
Step 4 The server load balancer directs requests from wireless devices to the CTE. The CTE, acting as a proxy, sends a request to the server load balancer for the HTML/XML content. The server load balancer obtains the content from a web server and sends it to the CTE.

Step 5 The CTE uses the rules created by Design Studio to transform the content and then sends the transformed content to the server load balancer.

Step 6 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



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 6 covers typical network configurations for the CTE. Use Table 2 as a guide to determining the best location for a CTE, based on network topology and website characteristics.

Table 2 CTE Network Location Guidelines

Network Topology and Website Characteristics	Network Location of CTE
A server load balancer sits in front of the web server(s). Most of the network traffic to be intercepted by the CTE(s) 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 the CTE(s) or to web servers based on browser detection.
A server load balancer sits in front of the web server(s). Most of the network traffic to be intercepted by the CTE(s) 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 the CTE(s) 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(s), 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(s).
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 10
- Configuring a CTE Connected Directly to a Web Server, page 11
- Configuring a CTE Connected to a Server Load Balancer, page 13
- Configuring Proxy Settings, 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.

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 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 you want to assign to a Layer 3 content rule.
- CTE server farm names and their virtual IP addresses.

Reopening the CTE Console

The CTE console provides your only access to the Cisco CTE Server Software. Use the CTE console to configure network parameters, create logins for Design Studio 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 you created to the CTE.

The CTE console opens.

Step 2 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 11
- Configuring CTE Parameters, page 12

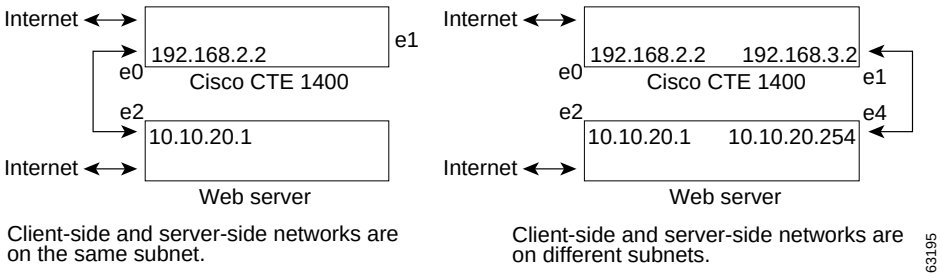
Connecting a CTE to a Web Server

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 to display and configure parameters for the CTE.

To display network parameters, perform this step:

- From the CTE console, type **1** (Display Saved Parameters) and press **Enter**, or type **30** (Display Current Parameters) and press **Enter**.

  Current parameters show any uncommitted changes made in the current session.

To configure network parameters, perform these steps:

Step 1 From the CTE console, type **2** (Set Networking Parameters) and press **Enter**.

Step 2 Answer the prompts as follows:

```
Boot proto [DHCP,static]? static
Enter the Gateway device[0/1]: 1   [0 = e0/NIC 1; 1 = e1/NIC 2]
IP address for eth0[x.x.x.x]? ipaddress
IP address for eth1 [x.x.x.x]? ipaddress    [on separate subnet from e0]
NETMASK [x.x.x.x]? mask
GATEWAY [x.x.x.x]? webserver_port_ipaddress
```

For example, for Figure 8, which shows different subnets, the network parameters are as follows:

```
Boot proto [DHCP,static]? static
Enter the Gateway device[0/1]: 1   [0 = e0/NIC 1; 1 = e1/NIC 2]
IP address for eth0[x.x.x.x]? 192.168.2.2
IP address for eth1 [x.x.x.x]? 192.168.3.2    [on separate subnet from e0]
NETMASK [x.x.x.x]? 255.255.255.0
GATEWAY [x.x.x.x]? 10.10.20.254
```

Note DHCP is not recommended for use with the CTE.

Step 3 Type **5** (Set Default Web-Server/Web-Page), press **Enter**, and enter an IP address for the web server.

Step 4 Type **4** (Set Masquerade Host), press **Enter**, and enter an IP address 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 If you are using DNS, type **3** (Set DNS Parameter), press **Enter**, and enter one or more IP addresses.

Step 6 Type **31** (Review and Commit Changes), press **Enter**, and review the settings.

Step 7 If the settings are correct, type **yes** and press **Enter**.

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:

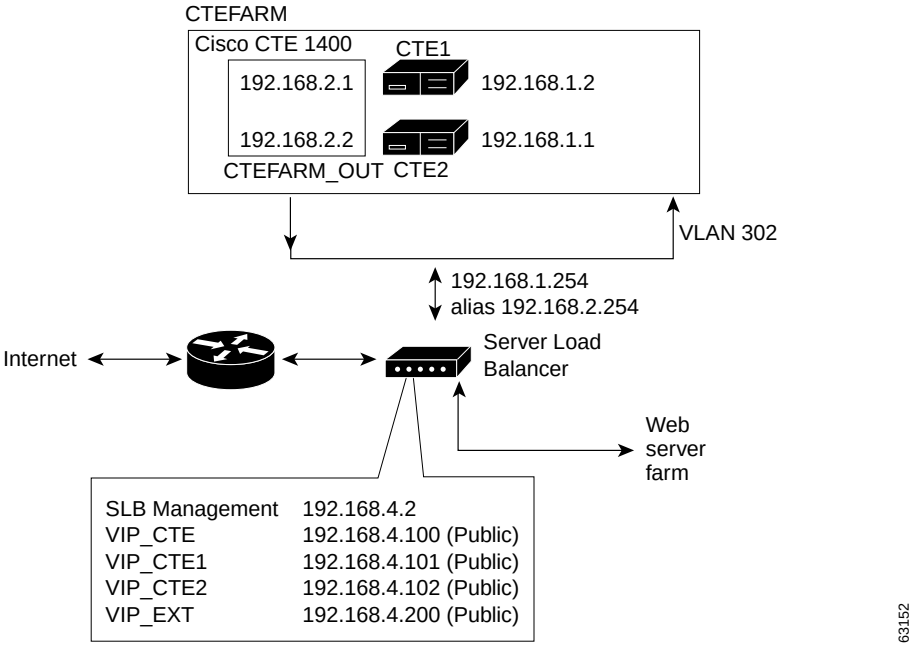
- Incoming web traffic is intercepted by the server load balancer and load-balanced between the CTEs (if more than one CTE is in use). All incoming client IP addresses appear as a single IP address through Network Address Translation (NAT).
- When a CTE receives a request through port 80 for a valid 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 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.

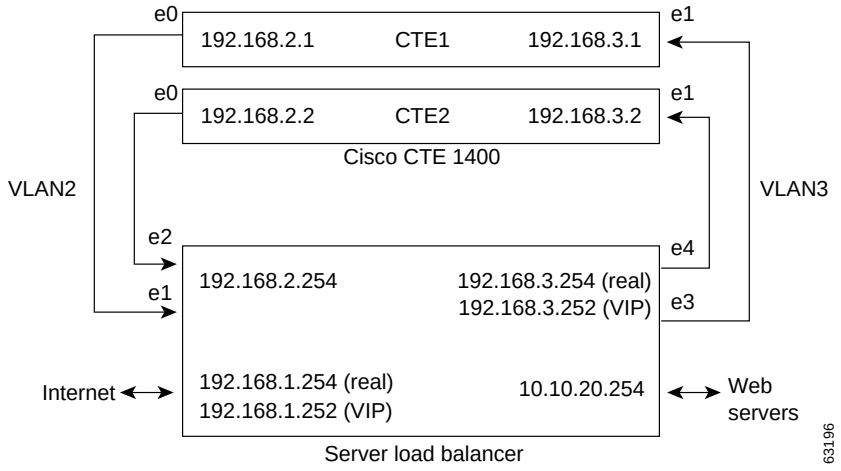
The procedures in this section are specific to the CSS, although CSM setup is similar. Figure 9 shows a CSM setup in which CTE requests go to the server load balancer, rather than the router.

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



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 15
- Configuring CTE Parameters, page 15
- Configuring the Server Load Balancer, page 16

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 to display and configure parameters for the CTE.

To display network parameters, perform this step:

- From the CTE console, type **1** (Display Saved Parameters) and press **Enter**, or type **30** (Display Current Parameters) and press **Enter**.

  Current parameters show any uncommitted changes made in the current session.

To configure network parameters, perform these steps:

Step 1 From the CTE console, type **2** (Set Networking Parameters) and press **Enter**.

Step 2 Answer the prompts as follows:

```
Boot proto [DHCP,static]? static
Enter the Gateway device[0/1]: 1   [should correspond to the NIC that is on the
                                    same subnet as the CTE default gateway]
IP address for eth0[x.x.x.x]? ipaddress
IP address for eth1 [x.x.x.x]? ipaddress    [must be on a different subnet from e0]
NETMASK [x.x.x.x]? mask
GATEWAY [x.x.x.x]? ipaddress_for_slb_port
```

Note Due to a restriction in this release, the subnet mask is the same for e0 and e1.

For Figure 10, the network parameters for CTE1 are as follows:

```
Boot proto [DHCP,static]? static
Enter the Gateway device[0/1]: 1
IP address for eth0[x.x.x.x]? 192.168.2.1
IP address for eth1 [x.x.x.x]? 192.168.3.1
NETMASK [x.x.x.x]? 255.255.255.0
GATEWAY [x.x.x.x]? 192.168.3.254
```

Note DHCP is not recommended for use with the CTE.

Step 3 Type **5** (Set Default Web-Server/Web-Page), press **Enter**, and enter a virtual IP address for the web server or a URL for the CTE start page (such as a portal page).

Step 4 Type **4** (Set Masquerade Host), press **Enter**, and enter an IP address 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 5 If you are using DNS, type **3** (Set DNS Parameter), press **Enter**, and enter one or more IP addresses.

Step 6 Type **31** (Review and Commit Changes), press **Enter**, and review the settings.

Step 7 If the settings are correct, type **yes** and press **Enter**.

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 18.

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 for the CTE2 service is 192.168.2.2.

Step 5 Create an owner so 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.

Configuring Proxy Settings

The following sections describe proxy configuration:

Configuring the Cisco CTE 1400 to Proxy All Web Pages

By default, the CTE proxies only the web pages it has transformed in order to prevent access to protected servers that are on the same subnet as the CTE. You can use the CTE console to override the default behavior so that the CTE proxies all web pages. For more information, see the "Important Security Information" section on page 2.

To proxy all web pages, perform these steps:

Step 1 From the CTE console, type **12** (Enable Unrestricted Proxy Support) and press **Enter**.

Step 2 Enter **yes** to the prompt.

Directing Cisco CTE 1400 Requests through a Proxy Server

You can specify that CTE requests for web pages go through a proxy server or use a direct connection. For example, you can specify a proxy server for nonsecure requests and use a direct connection for secure requests.

To specify a proxy server for HTTP (nonsecure requests), perform these steps:

Step 1 From the CTE console, type **8** (Set Proxy) and press **Enter**.

Step 2 Enter the HTTP proxy IP address and press **Enter**.

To specify a proxy server for HTTPS (secure requests), perform these steps:

Step 1 From the CTE console, type **9** (Set Secure Proxy) and press **Enter**.

Step 2 Enter the HTTPS proxy IP address and press **Enter**.

To disable a proxy server, perform these steps:

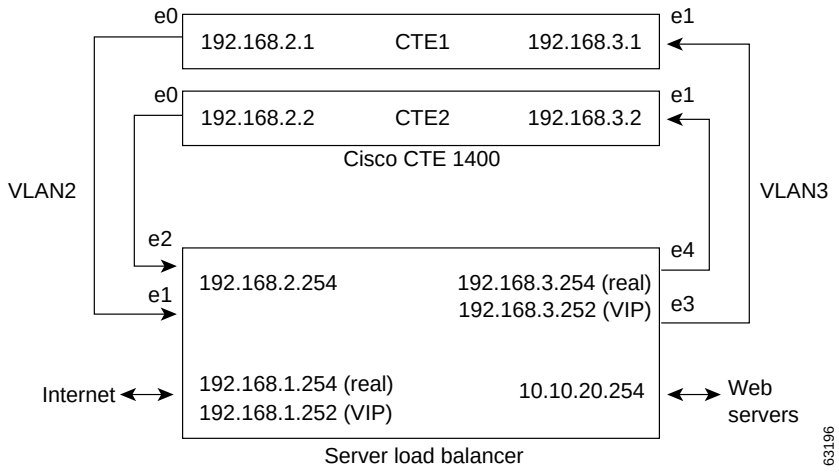
Step 1 From the CTE console, type **8** (Set Proxy) or **9** (Set Secure Proxy) and press **Enter**.

Step 2 Specify **0** as the IP address and press **Enter**.

Configuration Example

This section contains the CTE console and CLI commands needed to configure two CTEs with a Cisco CSS 11000, as shown in Figure 11.

Figure 11 CTE Connected to Server Load Balancer



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

	Task	Command
Step 1	Display the prompts for the networking parameters.	`Enter your choice: 2`
Step 2	Specify static IP addressing; DHCP is not recommended.	`Boot proto [DHCP,static]? static`
Step 3	Specify e1/NIC 2 as the gateway device.	`Enter the Gateway device[0/1]: 1`
Step 4	Specify the IP address for e0.	`IP address for eth0[x.x.x.x]? 192.168.2.1`
Step 5	Specify the IP address for e1.	`IP address for eth1 [x.x.x.x]? 192.168.3.1`
Step 6	Set the mask for the CTE.	`NETMASK [x.x.x.x]? 255.255.255.0`
Step 7	Specify the real server-side IP address of the server load balancer.	`GATEWAY [x.x.x.x]? 192.168.3.254`
Step 8	Display the prompt for the default web server or web page.	`Enter your choice: 5`
Step 9	Specify the IP address of the default web server.	`Virtual IP or In-Line mode host address: 10.10.20.22`
Step 10	Display the prompt for the masquerade host.	`Enter your choice: 4`
Step 11	Specify the IP address for NAT.	`Host to Masquerade as (NaT): 192.168.2.1`
Step 12	Review settings.	`Enter your choice: 31`
Step 13	Save your changes.	`Are you sure? [yes/no] yes`

To configure network parameters for CTE2, perform these steps from the CTE console for CTE2:

	Task	Command
Step 1	Display the prompts for the networking parameters.	`Enter your choice: 2`
Step 2	Specify static IP addressing; DHCP is not recommended.	`Boot proto [DHCP,static]? static`
Step 3	Specify e1/NIC 2 as the gateway device.	`Enter the Gateway device[0/1]: 1`
Step 4	Specify the IP address for e0.	`IP address for eth0[x.x.x.x]? 192.168.2.2`
Step 5	Specify the IP address for e1.	`IP address for eth1 [x.x.x.x]? 192.168.3.3`
Step 6	Set the mask for the CTE.	`NETMASK [x.x.x.x]? 255.255.255.0`
Step 7	Specify the real server-side IP address of the server load balancer.	`GATEWAY [x.x.x.x]? 192.168.3.254`
Step 8	Display the prompt for the default web server or web page.	`Enter your choice: 5`
Step 9	Specify the IP address of the default web server.	`Virtual IP or In-Line mode host address: 10.10.20.22`
Step 10	Display the prompt for the masquerade host.	`Enter your choice: 4`
Step 11	Specify the IP address for NAT.	`Host to Masquerade as (NaT): 192.168.2.2`
Step 12	Review settings.	`Enter your choice: 31`
Step 13	Save your changes.	`Are you sure? [yes/no] yes`

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 cte1** (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 console.

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

Step 1 In the CTE console, type **7** (Set Username and Password) and press **Enter**.

Step 2 Type a username of at least six characters and press **Enter**.

Step 3 Type a password of at least eight characters and press **Enter**.

Step 4 Type **31** (Review and Commit Changes) and press **Enter**.

Step 5 Type **yes** and press **Enter**.

Shutting Down and Restarting the CTE Server Software

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

To shut down the CTE Server Software, perform these steps:

Step 1 In the CTE console, type **32** (Restart/Shutdown) and press **Enter**.

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

To restart the CTE Server Software, perform these steps:

Step 1 In the CTE console, type **32** (Restart/Shutdown) and press **Enter**.

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

Monitoring the Performance of the Cisco CTE 1400

You can monitor the performance of the CTE by using the CTE console to enable and 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. The information provided includes the following:

- How long the CTE has been running
- System load averages for the past 1, 5, and 15 minutes
- Amount of total, used, and free memory
- Number of received connections, inbound/outbound requests, and failed requests
- List of listening and nonlistening sockets
- Number of requests from each type of device

To monitor and view performance information, perform these steps:

Step 1 From the CTE console, type **20** (Enable/Disable System Performance Monitoring) and press **Enter**.

Step 2 Answer **yes** to the prompt to start the monitoring and press **Enter**.

Step 3 When you are ready to view performance information, type **21** (View System Performance Information) and press **Enter**.

To stop the monitoring, perform these steps:

Step 1 From the CTE console, type **20** (Enable/Disable System Performance Monitoring) and press **Enter**.

Step 2 Answer **no** to the prompt to stop the monitoring and press **Enter**.

Uploading a Secure Certificate to the CTE

You can upload a digital certificate to the CTE in order to secure transactions. The certificate must have the following characteristics:

- It must be in Privacy Enhanced Mail (PEM) format and include the 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.

To upload a certificate, perform these steps:

Step 1 From the File menu, choose **Upload Certificate**.

Step 2 In the Open dialog box, navigate to the certificate file and then click **Open**.

Step 3 Use the CTE console to restart the CTE.

Upgrading the CTE Server Software

You upload upgrades to the CTE Server Software from Design Studio.

To upgrade the CTE Server Software, perform these steps:

Step 1 From a PC where Design Studio is already installed, go to the URL http://www.cisco.com/kobayashi/sw-center/sw-contest.shtml and then click the heading “Cisco CTE 1400 Software.”

Step 2 Download the upgrade file for the CTE to your PC.

The download process copies the file CTEserver116 to your PC.

Step 3 Start the already installed version of Design Studio.

Step 4 From the Design Studio File menu, choose **Upload CTE 1400 Upgrade**.

Step 5 In the Open dialog box, navigate to **CTEserver116** and click **Open**.

Design Studio uploads and installs the CTE upgrade file. The CTE drops all active sessions during the installation and resumes operation in one minute or less.

Note When you upgrade a CTE, the Design Studio users who connect to that CTE must also upgrade Design Studio to the corresponding version, as described in *Release Notes for Cisco CTE 1400 and Design Studio*.

Recovering from a CTE Crash

If the CTE device fails, follow the instructions in the *Cisco CTE 1400 Hardware Installation Guide* for diagnosing and recovering from a hardware failure. Once the hardware is operational, reinstall the CTE Server Software from the CD provided with the device.

To reinstall the CTE Server Software, 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 if 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 Cisco CTE 1400.

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 Cisco CTE 1400.

Verify that the following are correctly set up:

- The masquerade IP address specified in the CTE console (option 4) is available outside of your firewall.
- Any changes made in the CTE console have been committed (option 31).
- 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 Cisco CTE 1400, verify the CTE configuration as follows:

- The server load balancer or switch connected to the Cisco CTE 1400 is set up to recognize wireless devices.
- Wireless device traffic is directed through the Cisco CTE 1400.
- The Cisco CTE 1400 is intercepting traffic from wireless devices.

Handheld devices do not authenticate against Microsoft Internet Information Server (IIS).

The Cisco CTE 1400 does not work with Microsoft integrated Windows authentication (formerly called Windows NT Challenge/Response authentication). To work around this limitation, set the affected portion of your web site to Basic Authentication.

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 you must disable secure redirects for the CTE. To do that, choose option **6** in the CTE console (Enable Secure Redirects), enter **no**, and then choose option **31** to commit the change.

Related Documentation

For more information about the Cisco CTE 1400, refer to the following publications:

- *Cisco CTE 1400 and Design Studio Quick Start Guide*
- *Cisco CTE 1400 Hardware Installation Guide*
- *Release Notes for Cisco CTE 1400 and Design Studio*

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 **Leave Feedback** 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.