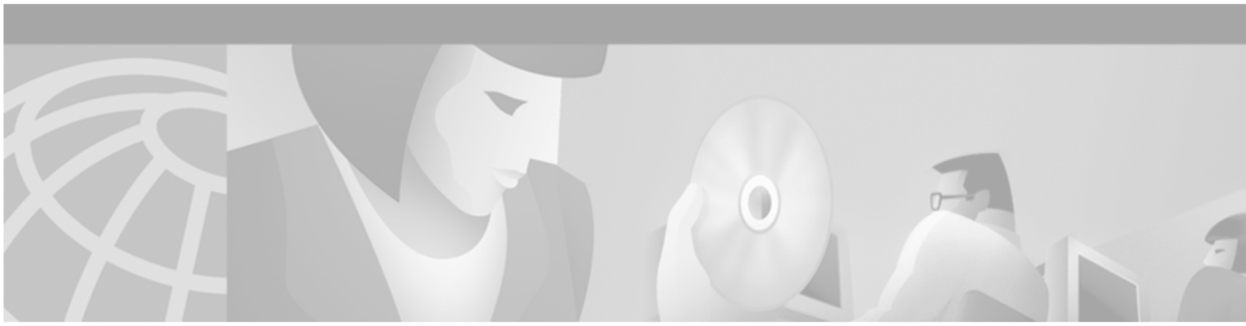


Cisco Content Transformation Engine 1400 Configuration Note

Product Number: CTE-1400

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 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 with your 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 that 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 your firewall. (The default CTE configuration port is port 9001.)

  To assure secure operations, you must deny access to CTE port 9001 from outside 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.

In addition, be aware of the following security considerations:

- IP Phone issues

  The IP Phone protocol is still under development and some elements are not rendered correctly by the CTE. You might experience problems with links, frames, **input** elements, and the display of search result pages.

  Because Cisco CallManager does not support SSL, the connection between Cisco CallManager and the CTE is not secure. We recommend that you locate the connection between Cisco CallManager and the CTE behind a firewall.

- SSL to non-SSL redirects

  When Design Studio is redirected to an SSL site from a non-SSL site (from HTTPS to HTTP), the connection between Design Studio and the CTE is not secure. We recommend that you locate the connection between Design Studio and the CTE behind a 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, firewalls, Virtual Private Network (VPN) solutions, routers, and IEEE 802.11 broadband wireless devices.

The CTE Design Studio is a PC-based application 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, a centralized configuration management tool.

These sections describe the Cisco CTE 1400:

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

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 1000 active concurrent 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.

Table 1 Cisco CTE 1400 Features (continued)

Feature	Description
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 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) • Compact 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
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. • 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.

Table 1 Cisco CTE 1400 Features (continued)

Feature	Description
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 Keep-Alive). An administrator can configure the session timeout interval.
Security[5]	• Fully supports various login authentication mechanisms (such as HTTP 401 Basic and NT LAN Manager (NTLM) 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), 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

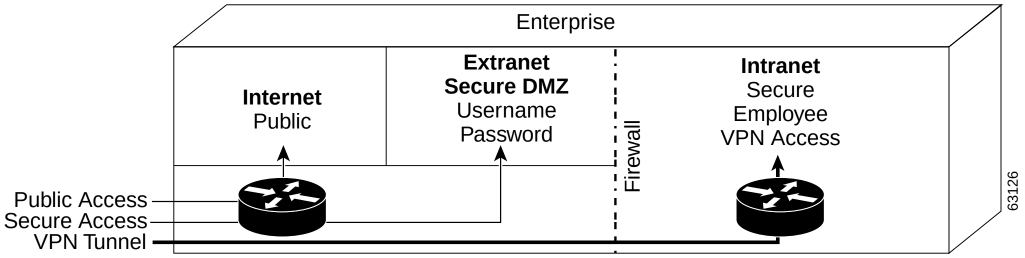
Internet, extranet, and intranet sites require different levels of security, all supported by the Cisco CTE 1400. As shown in Figure 1, those sites have the following characteristics:

- 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

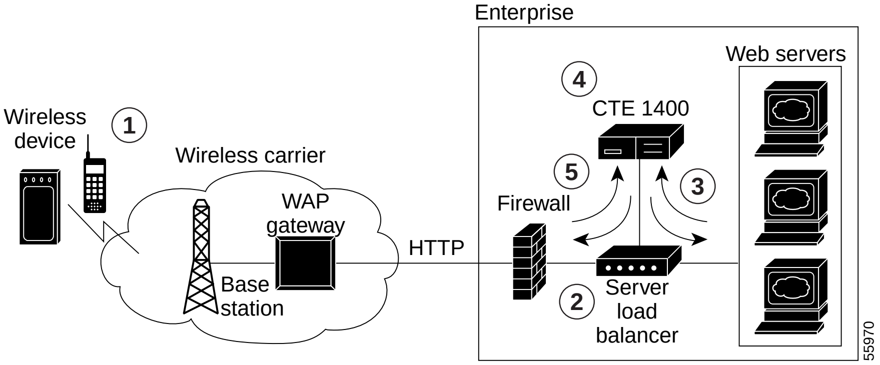
The CTE terminates Secure Sockets Layer (SSL) sessions to provide an endpoint for a secure link. Some PDAs support SSL connections from the device to the CTE. However, WAP phones and the Palm 7 device do not support SSL. WAP phones use Wireless Transport Layer Security (WTLS) and Palm 7 devices use Elliptical 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. We recommend that you use this configuration 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



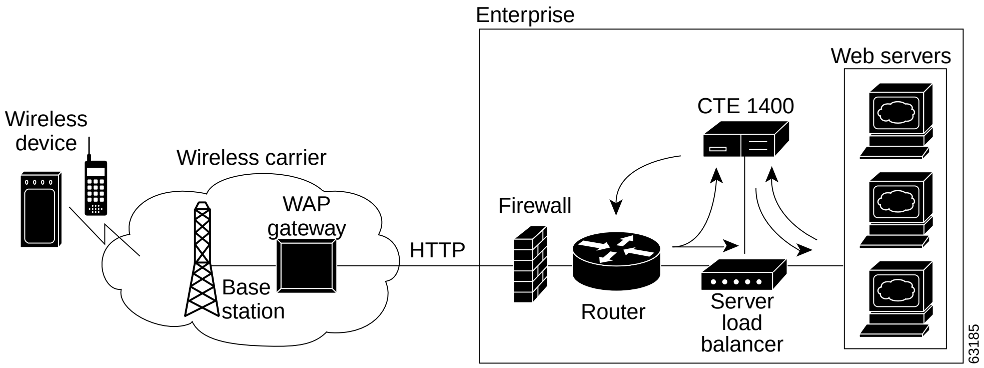
Note The numbers in Figure 2 refer to the following process.

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. We recommend that you use this configuration 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.

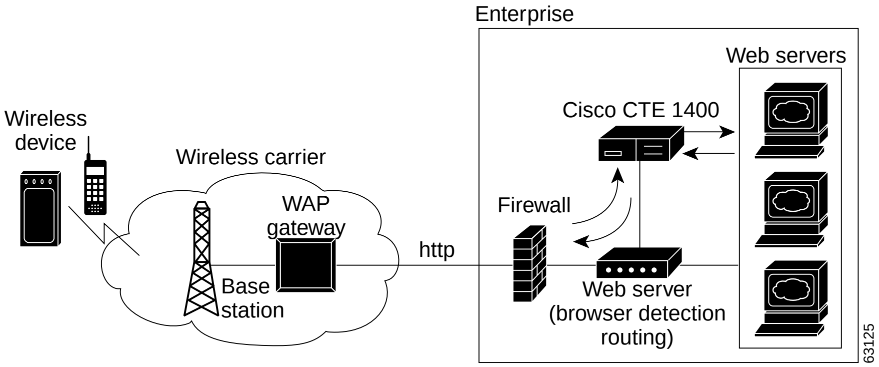
Figure 3 CTE Connected to Router and Server Load Balancer



CTE Connected to Web Server

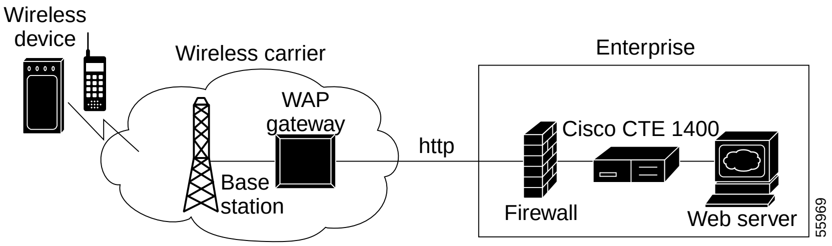
You can connect a CTE to a web server that routes traffic to the CTE or to web servers based on browser detection, as shown in Figure 4.

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. We recommend that you use this configuration when you designate specific IP addresses for wireless traffic.

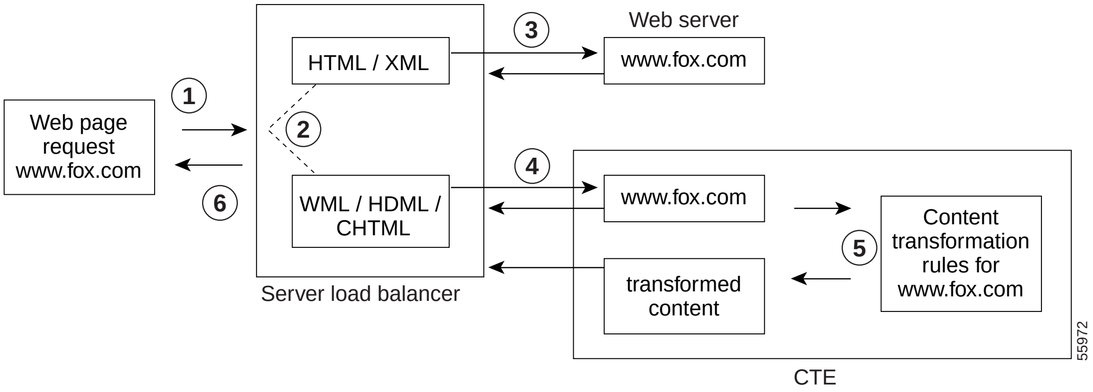
Figure 5 CTE In-line Connection



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.

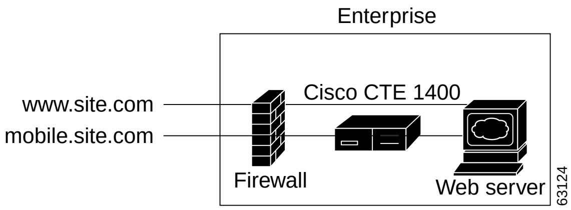
Step 4 The server load balancer directs requests from wireless devices to the CTE.

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 LATIN1. Only one input encoding format can be active at a time. Other input encoding schemes you can choose are RAW, ASCII, UTF8, MACROMAN, ISO2022, SHIFT JIS, ISO-2022-JP (JIS), EUC-JP, GB2312, BIG5, HZ, EUC-KR, and ISO-2022-KR.

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 6 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 the web servers. Most of the network traffic to be intercepted by the CTEs 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 CTEs or to web servers based on browser detection.
A server load balancer sits in front of the web servers. Most of the network traffic to be intercepted by the CTEs 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 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 CTEs, 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 CTEs.

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 15

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 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 Cisco CTE Server Software, 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 you created to the CTE.

Step 2 Log on to the CTE console as **Administrator**. The default password is also **Administrator**.

Step 3 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

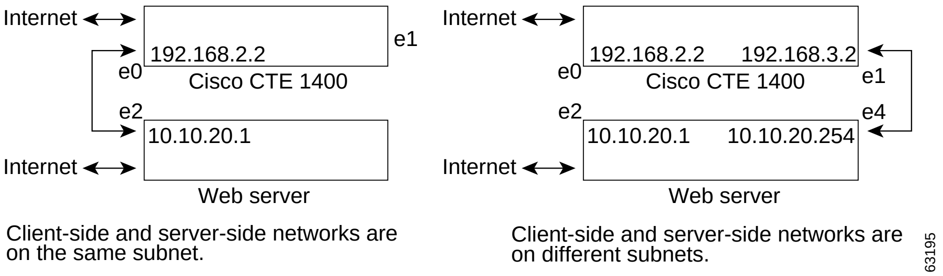
Connecting a CTE to a Web Server

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 that 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 addresses.

Configuring CTE Parameters

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

To display network parameters, perform this step:

- From the CTE console, type **1** (Display Current Configuration) and press **Enter**.

To configure network parameters, perform these steps:

Step 1 From the CTE console, type **3** (Set Networking Parameters for eth0) and press **Enter**.

Step 2 Answer the prompts as follows:

```
IP address for eth0 [x.x.x.x] ([RETURN] to clear): ipaddress
NETMASK for eth0 [x.x.x.x] ([RETURN] to clear): mask
Press ENTER to display CTE Console Menu
```

Step 3 Type **4** (Set Networking Parameters for eth1) and press **Enter**.

Step 4 Answer the prompts as follows:

```
IP address for eth1 [x.x.x.x] ([RETURN] to clear): ipaddress    [on separate subnet
                                                                  from eth0]
NETMASK for eth1 [x.x.x.x] ([RETURN] to clear): mask
Press ENTER to display CTE Console Menu
```

Step 5 Type **5** (Set Default Gateway) and press **Enter**.

Step 6 Answer the prompts as follows:

```
GATEWAY address [x.x.x.x]: gateway ipaddress
GATEWAY device (eth0 or eth1): 0 or 1
```

For Figure 8, which shows different subnets, the network parameters configured so far would be the following:

```
IP address for eth0 [x.x.x.x]: 192.168.2.1
NETMASK for eth0 [x.x.x.x]: 255.255.255.0
IP address for eth1 [x.x.x.x]? 192.168.3.1    [on separate subnet from eth0]
NETMASK for eth1 [x.x.x.x]? 255.255.255.0
GATEWAY address [x.x.x.x]: 10.10.20.254
GATEWAY device: 1
```

Step 7 Type **13** (Review and (optionally) commit console changes), press **Enter**, and review the settings.

Step 8 If the settings are correct, type **yes** when asked if you are sure, and press **Enter**.

Step 9 Type **17** (Restart/Shutdown CTE 1400 Device), and type **R** to restart the CTE so the new changes can take effect.

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

Step 1 Make sure that the following occurs:

- The CTE console is running.
- You have a Design Studio user identity. If you do not, you can create one using the **[12] Manage Users** command on the CTE console.

Step 2 From any browser, enter the following URL:

https://*ip-address***:***configuration-port*

Step 3 Press **OK** if a Security Alert dialog appears.

Step 4 Type your Design Studio username and password, and press **OK**.

Step 5 Under Protocol Settings, define the Masquerade Host by entering an IP address for Network Address Translation (NAT) in the Masquerade Host field.

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 Define the Inline Host by entering an IP address for the web server in the Inline Host field.

Step 7 Define one or more DNS servers by entering their IP addresses in the **Primary Interface** area of the window.

Note The CTE requires a DNS name server. Name lookups must go through a DNS system, rather than INS or LDAT, or they will fail.

Step 8 Press the **Save** button at the bottom of the window to save your changes.

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.

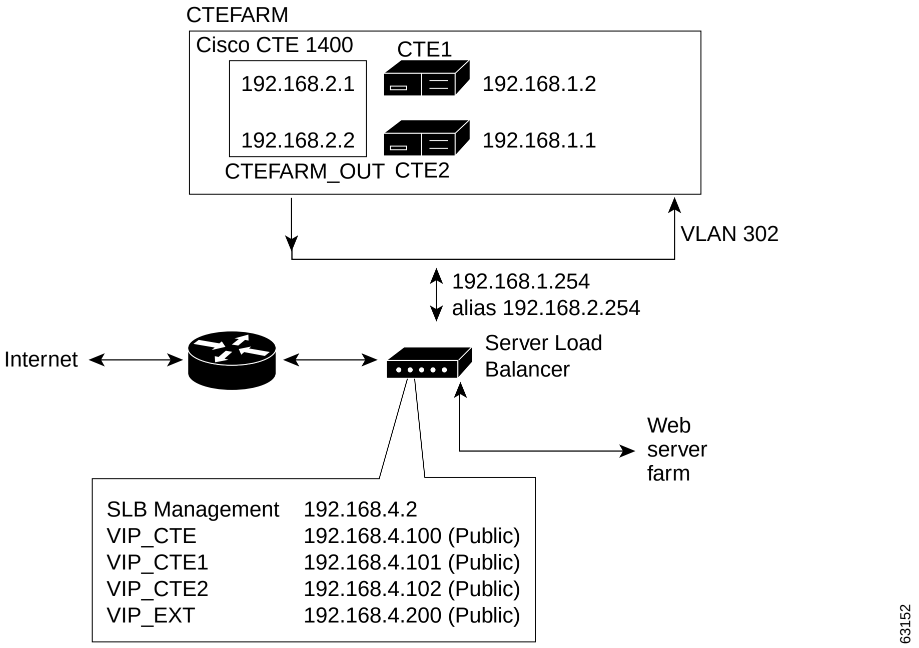
If multiple CTEs are in use, each CTE has a different masquerade host IP address. In addition, the CTE modifies all URLs embedded within a page to include the masquerade host IP address. This use of the masquerade host IP address ensures that the redirected client returns to the CTE it first encountered, providing session stickiness. The association between a particular request and 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 CSM setup is similar. Figure 9 shows a CSM setup in which CTE requests go to the server load balancer, rather than the router.

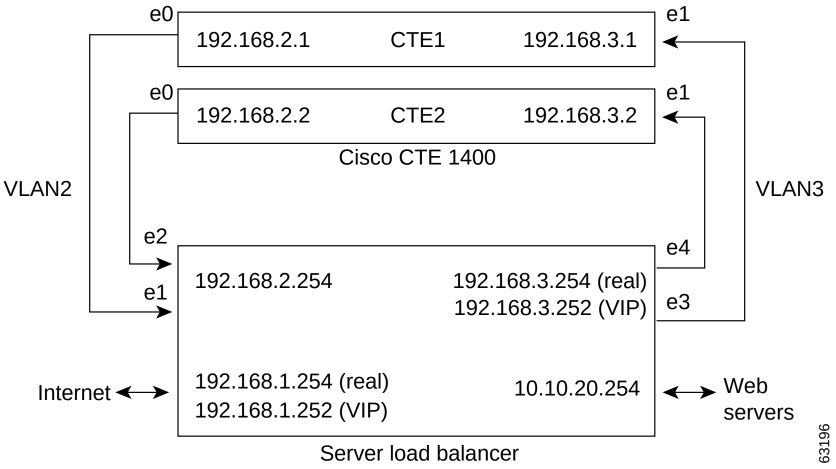
Figure 9 CTE Connected to Catalyst 6000 Family Switch (Requests Not Directed Through Router)



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)

The example configuration is 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 17
- Configuring CTE Parameters, page 17
- Configuring the Server Load Balancer, page 19

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.

To display network parameters, perform this step:

- From the CTE console, type **1** (Display Current Configuration) and press **Enter**.

To configure network parameters, perform these steps:

Step 1 From the CTE console, type **3** (Set Networking Parameters for eth0) and press **Enter**.

Step 2 Answer the prompts as follows:

```
IP address for eth0 [x.x.x.x] ([RETURN] to clear): ipaddress
NETMASK for eth0 [x.x.x.x] ([RETURN] to clear): mask
Press ENTER to display CTE Console Menu
```

Step 3 Type **4** (Set Networking Parameters for eth1) and press **Enter**.

Step 4 Answer the prompts as follows:

```
IP address for eth1 [x.x.x.x] ([RETURN] to clear): ipaddress    [must be on different
                                                                 subnet from eth0]
NETMASK for eth1 [x.x.x.x] ([RETURN] to clear): mask
Press ENTER to display CTE Console Menu
```

Step 5 Type **5** (Set Default Gateway) and press **Enter**.

Step 6 Answer the prompts as follows:

```
GATEWAY address [x.x.x.x]: gateway ipaddress
GATEWAY device (eth0 or eth1): 0 or 1
```

For Figure 8, which shows different subnets, the network parameters configured so far would be the following:

```
IP address for eth0 [x.x.x.x]: 192.168.2.1
NETMASK for eth0 [x.x.x.x]: 255.255.255.0
IP address for eth1 [x.x.x.x]? 192.168.3.1    [on separate subnet from eth0]
NETMASK for eth1 [x.x.x.x]? 255.255.255.0
GATEWAY address [x.x.x.x]: 10.10.20.254
GATEWAY device: 1
```

Step 7 Type **13** (Review and (optionally) commit console changes), press **Enter**, and review the settings.

Step 8 If the settings are correct, type **yes** when asked if you are sure, and press **Enter**.

Step 9 Type **17** (Restart/Shutdown CTE 1400 Device), and type **R** to restart the CTE so the new changes can take effect.

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

Step 1 Make sure that the following occurs:

- The CTE console is running.
- You have a Design Studio user identity. If you do not, you can create one using the **[12] Manage Users** command on the CTE console.

Step 2 From any browser, enter the following URL:

https://*ip-address***:***configuration-port*

Step 3 Press **OK** if a Security Alert dialog appears.

Step 4 Type your Design Studio username and password, and press **OK**.

Step 5 Under Protocol Settings, define the Masquerade Host by entering an IP address for Network Address Translation (NAT) in the Masquerade Host field.

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 Define the Inline Host by entering an IP address for the web server in the Inline Host field.

Step 7 Define one or more DNS servers by entering their IP addresses in the **Primary Interface** area of the window.

Note The CTE requires a DNS name server. Name lookups must go through a DNS system, rather than INS or LDAT, or they will fail.

Step 8 Press the **Save** 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 35.

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 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 20
- CTE 1400 Administration Interface, page 26

Remember that any time you make changes to the CTE configuration, you must save the changes and restart the CTE for those changes to take effect.

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

Commands	Description

[1] Display Current Configuration	Displays the current saved configuration, including the IP address and subnet mask for the Ethernet 1 and 2 ports, the gateway device and IP address, the IP addresses for DNS servers 1, 2, and 3, and the SNMP status.
	Type **1** to display the current configuration. The console returns the following information:
	`eth0 static address is: –`
	Displays the IP address of the eth0 port if defined.
	`eth0 netmask is: –`
	Displays the subnet mask of the eth0 port if defined.
	`eth0 boot protocol is: static`
	Displays the boot protocol of the eth0 port if defined.
	`eth1 static address is: –`
	Displays the IP address of the eth1 port if defined.
	`eth1 netmask is: –`
	Displays the subnet mask of the eth1 port if defined.
	`eth1 boot protocol is: static`
	Displays the boot protocol of the eth1 port if defined.
	`default gateway device is: 0`
	Displays the specified gateway device.
	`default gateway is: x.x.x.x`
	Displays the IP address of the eth0 gateway device.
	`DNS[1] is: x.x.x.x`
	Displays the IP address of DNS server 1.
	`DNS[2] is: x.x.x.x`
	Displays the IP address of DNS server 2.
	`DNS[3] is: x.x.x.x`
	Displays the IP address of DNS server 3.
	`Domain Name is: –`
	Displays the DNS domain if defined.
	`SNMP is: DISABLED`
	Displays whether SNMP is disabled or enabled.

[2] Display Pending Configuration	Displays any pending changes you have made to the configuration, but not yet saved. This information is displayed in the same format as the Display Current Configuration option. If there are no pending changes, a message appears telling you so.

[3] Set Networking Parameters for eth0	Allows you to set or change the IP address and subnet mask for the Ethernet 0 (eth0) port.
	Type **3**, press **Enter**, and enter the requested information at the following prompts:
	`IP address for eth0 [x.x.x.x] ([RETURN] to clear):`
	`NETMASK for eth0 [x.x.x.x] ([RETURN] to clear):`

Table 4 CTE Console Commands (continued)

Commands	Description

[4] Set Networking Parameters for eth1	Allows you to set or change the IP address and subnet mask for the Ethernet 1 (eth1) port.
	Type **4**, press **Enter**, and enter the requested information at the following prompts:
	`IP address for eth1 [x.x.x.x] ([RETURN] to clear):`
	The IP address must be on a separate subnet from eth0.
	`NETMASK for eth1 [x.x.x.x] ([RETURN] to clear):`

[5] Set Default Gateway	Allows you to specify the default gateway address and device.
	Type **5**, press **Enter**, and enter the requested information at the following prompts:
	`GATEWAY Device (eth0 or eth1)`
	`([RETURN] to select eth0):`
	Type **eth0** or **eth1** to specify the Ethernet 1 or Ethernet 2 port as the default gateway device.
	`DEFAULT GATEWAY [x.x.x.x] ([RETURN] to clear):`
	Type the IP address of the gateway device you want to be the default, or press **Enter** to leave the value blank.

[6] Set Routes	Allows you to add a static route from the CTE to the specified host or network via the specified network interface device. You will want to add a static route whenever you want to use a route that differs from the default gateway. Static routes are set up on the CTE port that is not being used by the default gateway.
	Type **6**, press **Enter**, and enter the requested information at the following prompts:
	`GATEWAY Device (eth0 or eth1) []`
	`([RETURN] to select eth0):`
	Type **eth0** or **eth1** to specify the gateway device.
	`Network address [x.x.x.x] (default to 127.0.0.0):`
	Type the IP address of the network interface device.
	`NETMASK [x.x.x.x] (default 255.255.255.0):`
	Type the subnet mask of the network interface device.
	`GATEWAY [x.x.x.x] (default 127.0.0.1):`
	Type the IP address of the gateway device.

[7] Clear Routes	Allows you to clear all specified routes. Type **7**, and press **Enter**, and you will see the following prompt: `Are you sure? (yes/no):` Type **yes** to clear all routes, or **no** to retain them.

Table 4 CTE Console Commands (continued)

Commands	Description

[8] Set DNS Parameters	Allows you to define up to three DNS servers and an associated domain name.
	Type **8**, press **Enter**, and enter the requested information at the following prompts:
	`DNS server[0] [x.x.x.x]:`
	Type the IP address of the first DNS server, or press **Enter** to leave the value blank.
	`DNS server[1] [x.x.x.x]:`
	Type the IP address of the second DNS server, or press **Enter** to leave the value blank.
	`DNS server[2] [x.x.x.x]:`
	Type the IP address of the third DNS server, or press **Enter** to leave the value blank.
	`Enter the Domain Name:`
	Type the domain name, or press **Enter** to leave the value blank.

[9] Configure SNMP	Allows you to define the location, contact person, community (read only), and port for Simple Network Management Protocol (SNMP). SNMP expedites the exchange of management information between network devices, allowing network administrators to manage network performance and solve any network problems.
	Type **9**, press **Enter**, and enter the requested information at the following prompts:
	`Location:`
	Type or view location information, such as the rack, building, or network.
	`Contact:`
	Type or view name of contact person.
	`Community (read only):`
	View password or string used to read statistics from the CTE.
	`Port:`
	Type or view SNMP port number. If not specified, the default port number is 161.

[10] Enable/Disable SNMP	Allows you to turn SNMP on or off. Type **10**, press **Enter**, and you will see the following prompt: `Enable SNMP? (yes/no):` Type **yes** or **no** to enable or disable the SNMP function.

Table 4 CTE Console Commands (continued)

Commands	Description

[11] Configure HTTP Parameters	Allows you to define HTTP parameters, including HTTP Listener IP address, subnet mask, and ports.
	Type **11** and press **Enter**. Press **Enter** again, and the following list of options appears:
	`[1] Set HTTP Listener IP Address(`
	`[2] Set HTTP Listener Subnet Mask`
	`[3] Set HTTP Listener Ports`
	`[4] Commit Changes / Return`
	Type **1** and press **Enter** to define the IP address of the HTTP Listener. The HTTP Listener can be the CTE server, or it may be a different IP address. The CTE will listen to one or more ports depending on how you define the HTTP Listener:
	• If no HTTP Listener is defined, or if you define the HTTP Listener IP address as 0.0.0.0, 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.
	• 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.
	Type **2** and press **Enter** to define the subnet mask of the HTTP Listener.
	Type **3** and press **Enter** to define the HTTP, HTTPS, and CONFIG ports.
	Press **Enter** to return to the HTTP Configuration Menu.
	Press **4** to save your changes and return to the Console menu.

[12] Manage Users	Allows you to add and delete Design Studio users. Type **12** and press **Enter**, and three options appear: [**0**] 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. [**1**] List Users lists current Design Studio users. [**2**] Delete User lets you delete users. Enter the complete username when prompted and press **Enter**. The name is deleted from the list.

Table 4 CTE Console Commands (continued)

Commands	Description
[13] Review and (optionally) commit console changes	Allows you to look at the pending configuration and to save your changes if you wish. Type **13** and press **Enter** to see the pending configuration. Type **yes** or **no** at the following prompt: `Are you sure? [yes/no]`
[14] 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 the route was successfully set. Type **14**, 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.
[15] Change Password for console authentication	Allows you to change the administrator password. Type **15**, and you will be prompted to enter the current password, the new password, and the new password again for confirmation. The password must be at least six characters long.
[16] Log out from console	Allows you to exit the console.

[17] Restart/Shutdown CTE 1400 Device	Allows you to restart or shut down the CTE.
	Type **17**, press **Enter**, and you will see the following prompts:
	`Enter R for Restart or S for Shutdown`
	`        [R] Restart Device`
	`        [S] Shutdown Device`
	`        Any other key will cancel the action`
	Configuration changes do not take effect until the CTE is restarted. Therefore, it is recommended that you restart the CTE after saving your changes to use the new configuration.
	To restart the CTE, type **R**.
	To shut down the CTE, type **S**.
	Press any other key to exit this function without restarting or shutting down the device.

CTE 1400 Administration Interface

The CTE 1400 Administration Interface lets you monitor and maintain the activity on your CTE from any browser on the Internet. Through this interface, you can set or display the following information:

- Protocol Settings, such as masquerade host, inline host, outbound proxy and port, outbound secure proxy and port, and session timeout.
- Primary Interface, such as the IP address, the IP subnet mask, DNS servers and domain, and the HTTP, HTTPS, and ADMIN ports.
- Content and Management Settings, such as the maximum buffer size and input encoding scheme. You can also enable or disable secure redirects, logging, system monitoring statistics, JavaScript support, HTTP and URL keep-alive messages, and specify the input encoding scheme.

You can also view logs of server and SNMP messages, as well as monitor system activities and device and load statistics.

Logging On to the Administration Interface

To access the CTE Administration Interface, perform these steps:

Step 1 Make sure that the following occurs:

- The CTE console is running.
- You have a Design Studio user identity. If you do not, you can create one using the **[12] Manage Users** command on the CTE console.

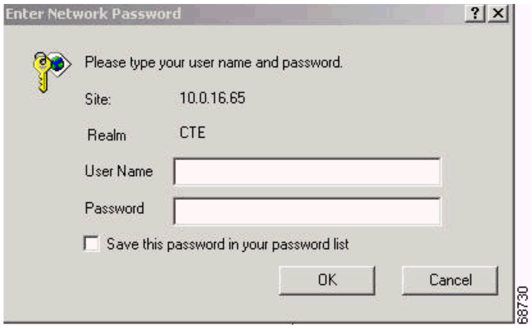
Step 2 From any browser, enter the following URL:

https://*ip-address***:***configuration-port*

Step 3 Press **OK** at the Security Alert dialog.

The CTE 1400 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

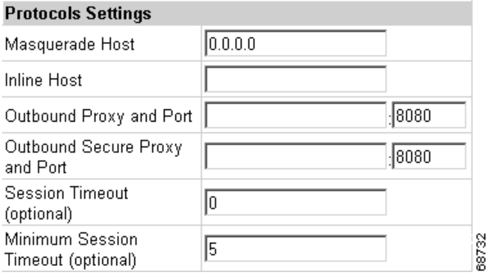
Step 4 Log in using your Design Studio user name and password., and press **OK**.

The CTE 1400 Administration Interface screen is described in the following sections.

Specifying Protocol Settings

The first segment of the Administration Interface screen, Protocol Settings, is shown in Figure 12.

Figure 12 Protocol Settings



Protocols Settings	
Masquerade Host	0.0.0.0
Inline Host	
Outbound Proxy and Port	: 8080
Outbound Secure Proxy and Port	: 8080
Session Timeout (optional)	0
Minimum Session Timeout (optional)	5

From the Protocol Settings segment of the screen, you can view and set the values shown in Table 5.

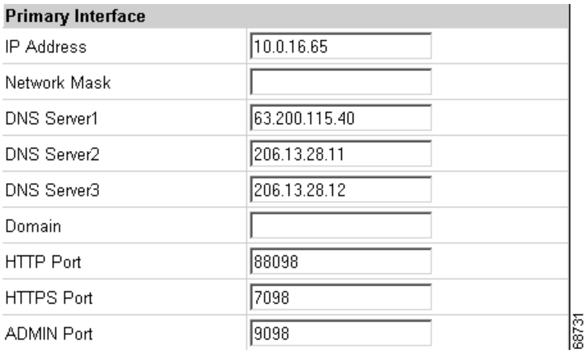
Table 5 Protocol Settings

Setting	Description
Masquerade Host	Specifies the current IP address for Network Address Translation (NAT), which makes all requests appear to originate from the same client. The current setting is displayed when the screen appears.
Inline Host	Specifies the IP address of the web server.
Outbound Proxy and Port	Specifies the IP address and port of an outbound proxy server. This sets a proxy server for HTTP (nonsecure requests).
Outbound Secure Proxy and Port	Specifies the IP address and port of an outbound secure proxy server. This sets a proxy server for HTTPS (secure requests).
Session Timeout (optional)	Specifies in seconds an interval after which an inactive user session will be removed from the system. You can configure the value for this interval. To turn this function off, do not enter a value.
Minimum Session Timeout (optional)	Specifies in seconds an interval during which a user session is guaranteed to remain in the system. When set to zero, user sessions can be removed from the system at any time. The default interval is zero. To turn this function off, do not enter a value.

Setting the Primary Interface

The second segment of the Administration Interface screen, Primary Interface, is shown in Figure 13.

Figure 13 Primary Interface



Primary Interface	
IP Address	10.0.16.65
Network Mask	
DNS Server1	63.200.115.40
DNS Server2	206.13.28.11
DNS Server3	206.13.28.12
Domain	
HTTP Port	88098
HTTPS Port	7098
ADMIN Port	9098

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 this segment of the screen, you can view or set values for these items as shown in Table 6.

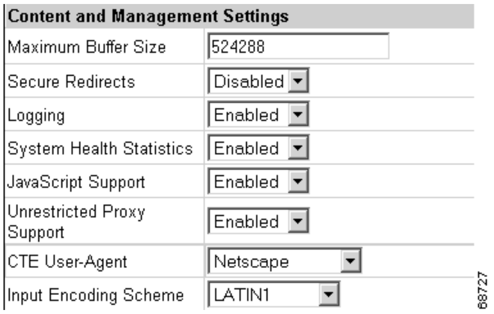
Table 6 Primary Interface Settings

Setting	Description
IP Address	Specifies the IP address of the CTE.
Network Mask	Specifies the subnet mask.
DNS Server1	Specifies the IP address of the first DNS server.
DNS Server2	Specifies the IP address of the second DNS server.
DNS Server3	Specifies the IP address of the third DNS server.
Domain	Specifies the DNS domain name.
HTTP Port	Specifies the HTTP port number.
HTTPS Port	Specifies the HTTPS port number.
ADMIN Port	Specifies the ADMIN port number.

Specifying Content and Management Settings

The Content and Management Settings segment of the Administration Interface screen is shown in Figure 14.

Figure 14 Content and Management



Content and Management Settings	
Maximum Buffer Size	524288
Secure Redirects	Disabled
Logging	Enabled
System Health Statistics	Enabled
JavaScript Support	Enabled
Unrestricted Proxy Support	Enabled
CTE User-Agent	Netscape
Input Encoding Scheme	LATIN1

From this segment of the screen, you can view or set values for maximum buffer size and the input encoding scheme. You can also enable or disable certain monitoring and other functions, as shown in Table 7.

Table 7 Content and Management Settings

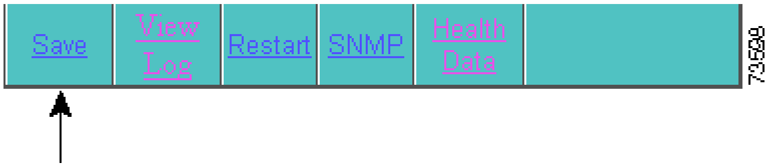
Setting	Description
Maximum Buffer Size	Displays the maximum buffer size. By default, this setting is already set and displayed, but you can change it from this menu.
Secure Redirects	Enables or disables the secure redirect function. When this function is enabled, the CTE will only accept requests coming in on a secure connection. If the CTE receives a request on an insecure connection, it will ask the requester to use a secure connection. By default, this function is disabled.
Logging	Enables or disables the logging of server messages. When this function is enabled, the CTE stores server messages, which you can view by pressing the **View Log** button at the bottom of the Administration Interface screen. Enable logging when you are troubleshooting, but do not leave it enabled all the time or the log will become too full and decrease system performance severely.
System Health Statistics	Enables or disables the monitoring of system conditions. When this function is enabled, the CTE stores information about the system, such as how long the CTE has been running, system loads, and memory usage. You can view this information by pressing the **Health Data** button at the bottom of the Administration Interface screen.
JavaScript Support	Enables or disables JavaScript support. 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 7 Content and Management Settings (continued)

Setting	Description
Unrestricted Proxy Support	Enables or disables unrestricted proxy support. When this function is enabled, the CTE proxies all web pages. When it is disabled, 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.
CTE User-Agent	Specifies the CTE user-agent as either Netscape or Internet Explorer.
Input Encoding Scheme	Defines the format into which information coming into the CTE is written. By default, this setting is LATIN1. Other input encoding schemes you can choose are RAW, ASCII, UTF8, MACROMAN, ISO2022, SHIFT-JIS, ISO-2022-JP (JIS), EUCJP, GB2312, BIG5, HZ, EUC-KR, and ISO-2022-KR.

Saving Your Changes

To save any changes you have made to the Administration Interface screen, press the **Save** button at the bottom of the screen.

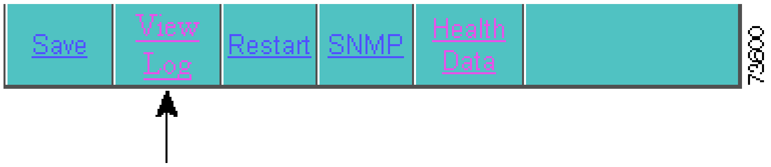


Viewing the Log

To view the log of CTE server messages, perform these steps:

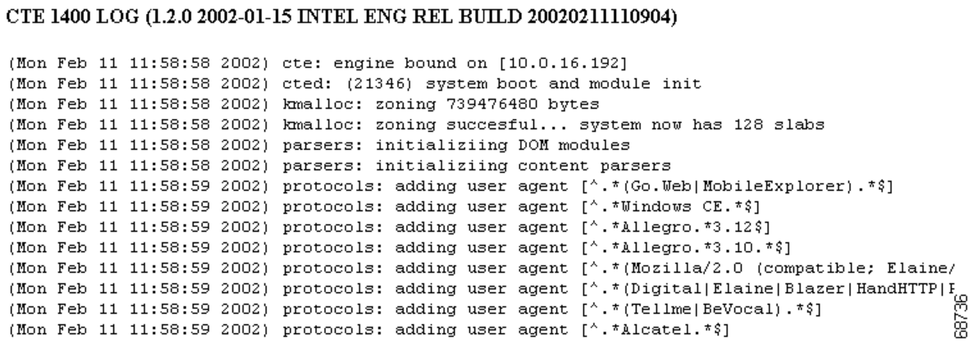
Step 1 Make sure **Logging** is enabled.

Step 2 Press **View Log**.



The message log appears. A portion of this log is shown in Figure 15.

Figure 15 CTE Server Message Log

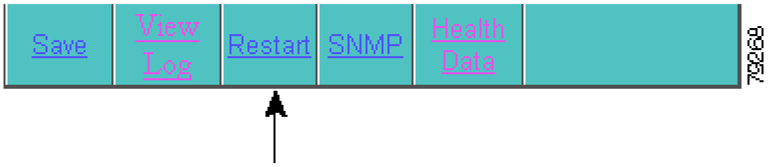


CTE 1400 LOG (1.2.0 2002-01-15 INTEL ENG REL BUILD 20020211110904)

```
(Mon Feb 11 11:58:58 2002) cte: engine bound on [10.0.16.192]
(Mon Feb 11 11:58:58 2002) cted: (21346) system boot and module init
(Mon Feb 11 11:58:58 2002) kmalloc: zoning 739476480 bytes
(Mon Feb 11 11:58:58 2002) kmalloc: zoning succesful... system now has 128 slabs
(Mon Feb 11 11:58:58 2002) parsers: initializiing DOM modules
(Mon Feb 11 11:58:58 2002) parsers: initializiing content parsers
(Mon Feb 11 11:58:59 2002) protocols: adding user agent [^.*(Go.Web|MobileExplorer).*$]
(Mon Feb 11 11:58:59 2002) protocols: adding user agent [^.*Windows CE.*$]
(Mon Feb 11 11:58:59 2002) protocols: adding user agent [^.*Allegro.*3.12$]
(Mon Feb 11 11:58:59 2002) protocols: adding user agent [^.*Allegro.*3.10.*$]
(Mon Feb 11 11:58:59 2002) protocols: adding user agent [^.*(Mozilla/2.0 (compatible; Elaine/
(Mon Feb 11 11:58:59 2002) protocols: adding user agent [^.*(Digital|Elaine|Blazer|HandHTTP|F
(Mon Feb 11 11:58:59 2002) protocols: adding user agent [^.*(Tellme|BeVocal).*$]
(Mon Feb 11 11:58:59 2002) protocols: adding user agent [^.*Alcatel.*$]
```

Restarting the CTE

To restart the CTE, press **Restart**.



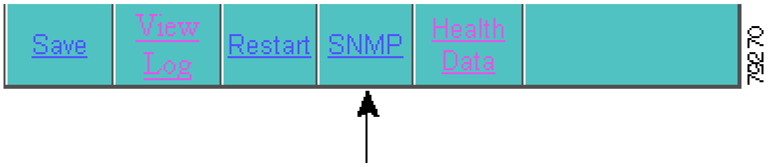
Whenever you make changes to the CTE configuration, perform these steps:

Step 1 Press the **Save** button to save your changes.

Step 2 Press the **Restart** button to restart the CTE so the changes can take effect.

Viewing the SNMP Log

To view the SNMP message log, press **SNMP**.

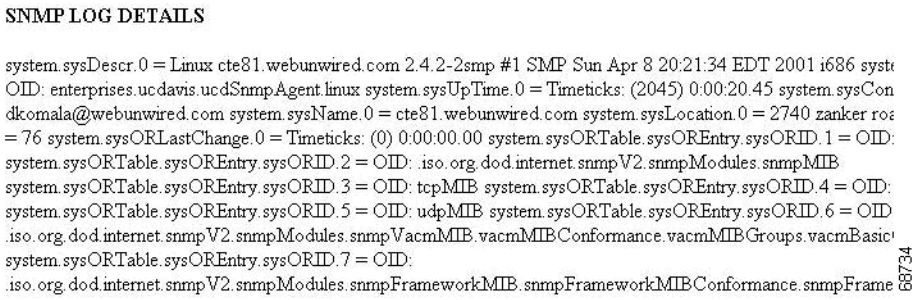


Before you attempt to view the SNMP messages, make sure that the SNMP function is enabled from the CTE Console menu.

If SNMP is disabled and you press the **SNMP** button, you will see a message telling you that the SNMP feature is currently disabled.

If SNMP is enabled and you press the **SNMP** button, the SNMP Message Log appears. A portion of the log is shown in Figure 16.

Figure 16 CTE SNMP Message Log



SNMP LOG DETAILS

```
system.sysDescr.0 = Linux cte81.webunwired.com 2.4.2-2smp #1 SMP Sun Apr 8 20:21:34 EDT 2001 i686 syst
OID: enterprises.ucdavis.ucdSnmpAgent.linux system.sysUpTime.0 = Timeticks: (2045) 0:00:20.45 system.sysCon
dkomala@webunwired.com system.sysName.0 = cte81.webunwired.com system.sysLocation.0 = 2740 zanker roa
= 76 system.sysORLastChange.0 = Timeticks: (0) 0:00:00.00 system.sysORTable.sysOREntry.sysORID.1 = OID:
system.sysORTable.sysOREntry.sysORID.2 = OID: .iso.org.dod.internet.snmpV2.snmpModules.snmpMIB
system.sysORTable.sysOREntry.sysORID.3 = OID: tcpMIB system.sysORTable.sysOREntry.sysORID.4 = OID:
system.sysORTable.sysOREntry.sysORID.5 = OID: udpMIB system.sysORTable.sysOREntry.sysORID.6 = OID
.iso.org.dod.internet.snmpV2.snmpModules.snmpVacmMIB.vacmMIBConformance.vacmMIBGroups.vacmBasic
system.sysORTable.sysOREntry.sysORID.7 = OID:
.iso.org.dod.internet.snmpV2.snmpModules.snmpFrameworkMIB.snmpFrameworkMIBConformance.snmpFrame
```

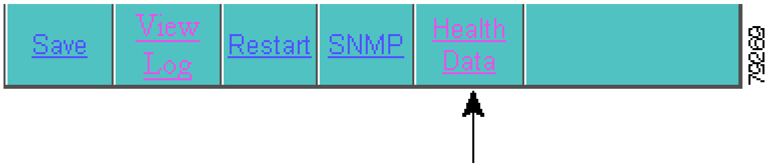
Viewing System Health

You can monitor the performance of the CTE from the Administration Interface screen. You can 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.

To access these statistics, perform these steps:

Step 1 Under Content and Management Settings, enable **System Health Statistics**.

Step 2 At the bottom of the Administration Interface screen, press **Health Data**.



The information provided includes the following:

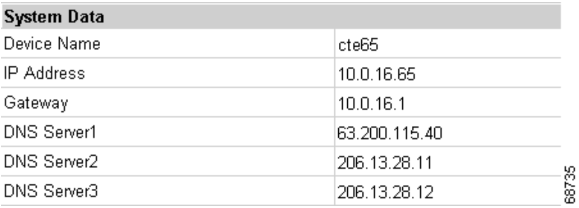
- CTE server information, such as the device name and the IP address
- The device driver statistics
- How long the CTE has been running
- The system load averages for the past 1, 5, and 15 minutes
- The amount of total, used, and free memory
- The number of received connections, inbound/outbound requests, and failed requests
- The number of requests from each type of device

The information displayed on the Health Statistics screen is organized in three categories:

- System Data
- Device Driver Statistics
- Load Statistics

The System Data segment of CTE Health Statistics gives you information about the system, as shown in Figure 17.

Figure 17 System Data



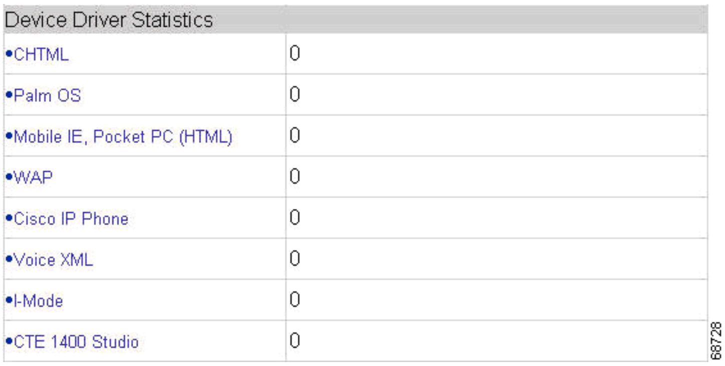
System Data	
Device Name	cte65
IP Address	10.0.16.65
Gateway	10.0.16.1
DNS Server1	63.200.115.40
DNS Server2	206.13.28.11
DNS Server3	206.13.28.12

The fields in this portion of the screen allow you to modify the following:

- Device Name—Specifies the name of the CTE server.
- IP Address—Specifies the IP address of the CTE server.
- Gateway—Specifies the web server port IP address if the CTE is connected to a web server, or the IP address for the server load balancer port if the CTE is connected to a server load balancer.
- DNS Server1, 2, and 3—Specifies the IP addresses of the three DNS servers.

The Device Driver Statistics segment of CTE Health Statistics gives you information about the system, as shown in Figure 18.

Figure 18 Device Driver Statistics

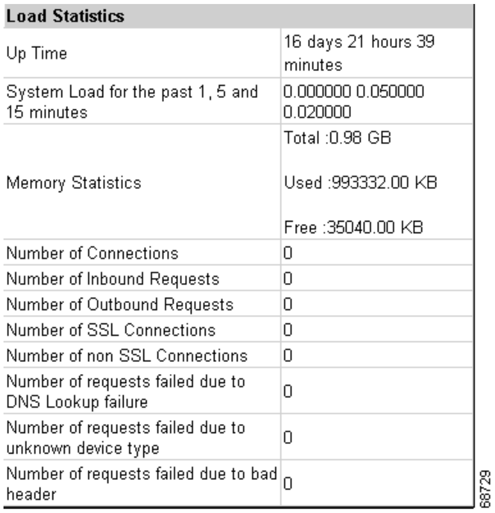


Device Driver Statistics	
•CHTML	0
•Palm OS	0
•Mobile IE, Pocket PC (HTML)	0
•WAP	0
•Cisco IP Phone	0
•Voice XML	0
•I-Mode	0
•CTE 1400 Studio	0

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

The Load Statistics segment of CTE Health Statistics gives you information about load levels, as shown in Figure 19.

Figure 19 Load Statistics



Load Statistics	
Up Time	16 days 21 hours 39 minutes
System Load for the past 1, 5 and 15 minutes	0.000000 0.050000 0.020000
Memory Statistics	Total :0.98 GB Used :993332.00 KB Free :35040.00 KB
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
Number of requests failed due to DNS Lookup failure	0
Number of requests failed due to unknown device type	0
Number of requests failed due to bad header	0

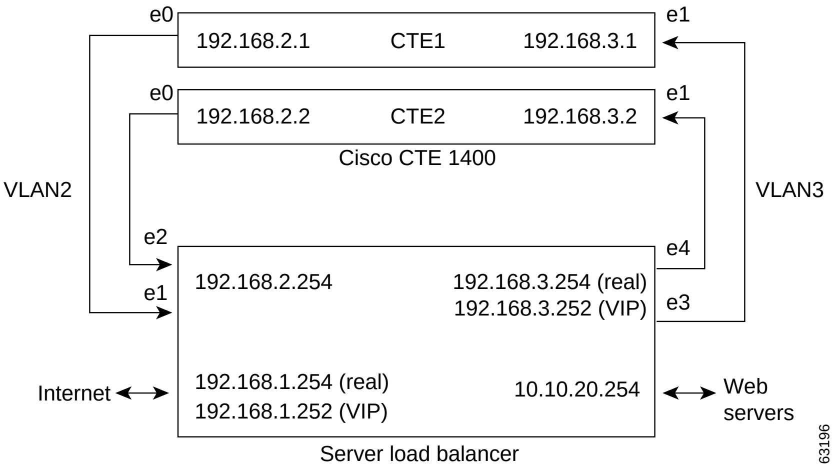
The fields in this portion of the screen display the following information:

- Up Time—Displays how long the CTE has been running in the current session, in days, hours, and minutes.
- System Load—Displays the system load, measured for the past 1, 5, and 15 minutes.
- Memory Statistics—Displays the total memory capacity, the amount of memory used, and 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 Socket Layer connections.
- Number of non-SSL Connections—Displays the number of non-Secure Socket Layer connections.
- Number of requests failed due to DNS lookup failure—Displays the number of requests that failed because of DSN lookup failure.
- Number of requests failed due to unknown device type—Displays the number of requests that failed because the device type was unknown.
- Number of requests failed due to bad header—Displays the number of requests that failed because of bad header addresses.

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 20.

Figure 20 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**] Display Current Configuration
Step 2	Specify the IP address for eth0.	Console	[**3**] Set Networking Parameters for eth0 IP address for eth0 [x.x.x.x] ([RETURN] to clear) **192.168.2.1** NETMASK for eth1 [x.x.x.x] ([RETURN] to clear) **255.255.255.0**
Step 3	Specify the IP address for eth1.	Console	[**4**] Set Networking Parameters for eth1 IP address for eth1 [x.x.x.x] ([RETURN] to clear) **192.168.3.1** NETMASK for eth1 [x.x.x.x] ([RETURN] to clear) **255.255.255.0**
Step 4	Specify eth1/NIC 2 as the gateway device.	Console	[**5**] Set Default Gateway Gateway address [x.x.x.x]:**192.168.2.1** Gateway device [0/1] **1**
Step 5	Review your changes.	Console	[**13**] Review and (optionally) commit console changes
Step 6	Save your changes.	Console	Are you sure? [yes/no] **yes**
Step 7	Restart CTE.	Console	[**17**] Restart/Shutdown CTE 1400 Device Type **R** to restart the device.
Step 8	Open the CTE Administration Interface.	Web browser	Enter the URL: *https://ip-address:configuration-port/* Press **OK** at the security alert dialog. Enter your username and password.

	Task	Application	Command/Field

Step 9	Set the subnet mask for the CTE.	Administration Interface	`Primary Interface: Network Mask field`
			`255.255.255.0`

Step 10	Specify the IP address of the default web server.	Administration Interface	`Protocol Settings: Inline Host field`
			`10.10.20.22`

Step 11	Specify the IP address for NAT.	Administration Interface	`Protocol Settings: Masquerade Host`
			`192.168.2.1`

Step 12	Save any changes made in the Administration Interface.	Administration Interface	`Press the` **`Save`** `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`**

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`**

	Task	Command
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 **12** (Manage Users) and press **Enter**.

Step 2 Type **0** (Add User) and press **Enter**.

Step 3 Type a username of at least six characters and press **Enter**.

Step 4 Type a password of at least eight characters and press **Enter**.

Step 5 Type **13** (Review and (optionally) commit console changes) and press **Enter**.

Shutting Down and Restarting the CTE Server Software

Always use the CTE console to shut down the CTE Server Software.

Caution 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 **17** (Restart/Shutdown CTE 1400 Device) 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 **17** (Restart/Shutdown CTE 1400 Device) and press **Enter**.

Step 2 Type **R** 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**.

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

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

Step 3 Do not exit Design Studio.

Step 4 Open Internet Explorer, and access a page through the CTE. For example, enter a URL similar to the following:

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

where:

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

Step 5 Accept the https security alert.

Step 6 Double-click the Lock symbol in the bottom right corner of the browser.

Step 7 Switch to the Certificate Path window pane at the top of the screen.

Step 8 Double-click the first path level to bring up the Certificate information for the first level and go to the Details screen.

Step 9 Click the **Copy to File** button at the bottom. A Certificate Export Wizard appears.

Step 10 Click **Next**.

Step 11 Make sure the format selected is: "DER encoding binary X.509(.CER)"

Step 12 Click **Next**.

Step 13 Enter a filename. For example, **G:\tmp\root.cer**.

Step 14 Review the information and note the complete filename. Click **Finish**.

Step 15 Click **OK** to close the Certificate information window for the first level.

Step 16 Repeat steps 6-14 for all levels except the last level, which is the signed certificate that has been created for the CTE.

Step 17 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
```

Step 18 Use the CTE console to restart the CTE.

Recovering from a CTE Crash

If the CTE device fails, follow the instructions in the *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 CTE 1400.

Verify that the following are correctly set up:

- The masquerade IP address specified in the CTE 1400 Administration Interface is available outside of your firewall.
- Any changes made in the CTE console have been committed (option 13).
- 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.

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, go to the CTE 1400 Administration Interface, and under Content and Management Settings, disable Secure Redirects, and press the **Save** button to commit the change.

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 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 38.

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

The CTE does not handle the multipart class of content types.

Some application servers send content with a content-type of multipart and delimit sections of the content with boundaries. The CTE does not handle the delimited content and may end up sending incorrectly transcoded content to the end device. Advanced features such as JavaScript emulation will also fail in this case.

I was unable to select certain user events on a page.

The CTE supports button clicks, form submissions, and select box changes. Pages that depend on certain JavaScript events may not work as expected.

I was asked for my password when I was already logged in.

This behavior may occur because the CTE does not support automatic NT LAN Manager (NTLM) renegotiation. To resume your session, simply reenter your username and password.

I was unable to open a user session.

This behavior may occur because Minimum Session Timeout is set to zero. You can adjust or unset Minimum Session Timeout under Protocol Settings in the CTE Administration Interface. For more information, see the "Specifying Protocol Settings" section on page 27.

XML stylesheets with uppercase HTML tags may not apply correctly.

In XML projects, if stylesheets use uppercase HTML tags, your stylesheet may not apply as expected because XML is case sensitive, and HTML is not case sensitive. We recommend that you avoid using uppercase HTML tags on XML stylesheets.

There is a known issue with URL paths containing &amp;amp.

For content containing anchors such as <a href="http://www.cisco.com/&amp;amp">, the CTE transcodes the anchors to be <a href="http://www.cisco.com/&amp>. End devices may further interpret this and, when following the link, may incorrectly request http://www.cisco.com/&, rather than http://www.cisco.com/&amp.

There is a known issue with cross-frame JavaScript references or document write calls.

Because the CTE does not support cross-frame JavaScript references or document.write calls, pages that depend on these functions may not work as expected.

My user session stopped unexpectedly.

If an active user session is dropped, then refresh (reload) the page and continue entering data.

Related Documentation

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

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

For information about using Design Studio, see the *Cisco CTE 1400 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 **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.