Cisco Reader Comment Card

General Information

1 Years of networking experience: ______ Years of experience with Cisco products: ______

2 I have these network types: □ LAN □ Backbone □ WAN
□ Other: ______

3 I have these Cisco products: □ Switches □ Routers
□ Other (specify models): ______

4 I perform these types of tasks: □ H/W installation and/or maintenance □ S/W configuration
□ Network management □ Other: ______

5 I use these types of documentation: □ H/W installation □ H/W configuration □ S/W configuration
□ Command reference □ Quick reference □ Release notes □ Online help
□ Other: ______

6 I access this information through: ____% Cisco.com (CCO) ____% CD-ROM
____% Printed docs ____% Other: ______

7 I prefer this access method: ______

8 I use the following three product features the most:

______

______

______

Document Information

Document Title: Cisco Application and Content Networking Software E-CDN Administrator's Guide

Part Number: 78-13953-01 S/W Release (if applicable): 4.1

On a scale of 1–5 (5 being the best), please let us know how we rate in the following areas:

______ The document is written at my technical level of understanding.

______ The information is accurate.

______ The document is complete.

______ The information I wanted was easy to find.

______ The information is well organized.

______ The information I found was useful to my job.

Please comment on our lowest scores:

______

______

______

______

Mailing Information

Company Name ______ Date ______

Contact Name ______ Job Title ______

Mailing Address ______

______

City ______ State/Province ______ ZIP/Postal Code ______

Country ______ Phone (   ) ______ Extension ______

Fax (   ) ______ E-mail ______

Can we contact you further concerning our documentation? □ Yes □ No

You can also send us your comments by e-mail to **bug-doc@cisco.com**, or by fax to **408-527-8089**.

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 4631 SAN JOSE CA

POSTAGE WILL BE PAID BY ADDRESSEE

ATTN DOCUMENT RESOURCE CONNECTION
CISCO SYSTEMS INC
170 WEST TASMAN DRIVE
SAN JOSE CA 95134-9883

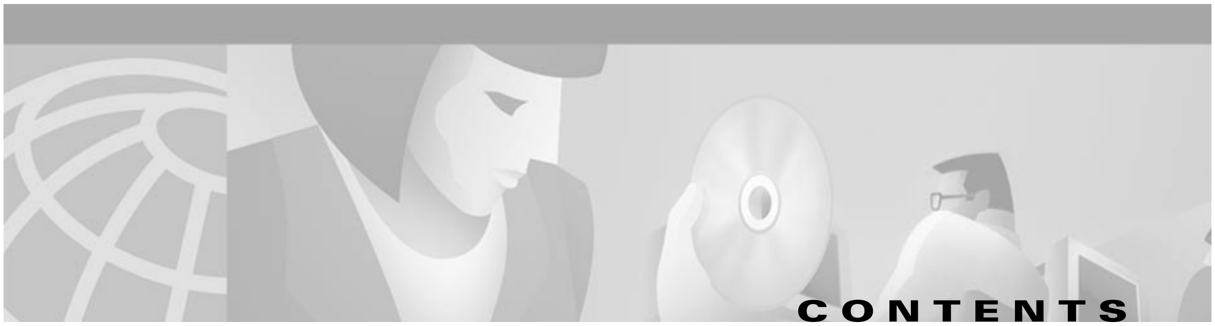
Cisco Application and Content Networking Software E-CDN Administrator's Guide

Version 4.1

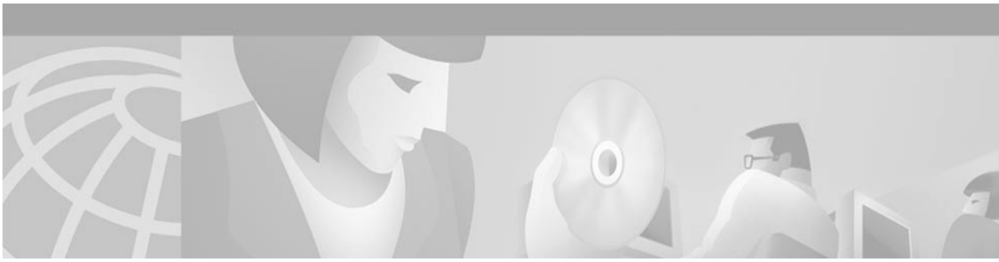
Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number: DOC=7813953
Text Part Number: 78-13953-01

Cisco Application and Content Networking Software E-CDN Administrator's Guide



CONTENTS



Preface

This preface describes who should read the *Cisco Application and Content Networking Software E-CDN Administrator's Guide*, how it is organized, and its document conventions.

This preface contains the following sections:

- Document Objectives, page x
- Audience, page x
- Organization, page xi
- Conventions, page xii
- Related Documentation, page xiii
- Obtaining Documentation, page xiv
- Obtaining Technical Assistance, page xv

Document Objectives

This administration guide provides detailed information about how to use the Cisco Application Content Networking Software (ACNS) Enterprise Content Delivery Network (E-CDN) application for network administrators and media managers. The person responsible for managing the E-CDN application Content Distribution Manager, Content Routers, and Content Engines should be experienced with the following topics:

- PC operating systems and conventions
- LAN environments
- TCP/IP
- Media formats

This guide provides step-by-step instructions for using the E-CDN application software. It assumes that the Content Distribution Managers, Content Routers, and Content Engines are physically present and have been installed and activated, as outlined in the *Cisco Content Delivery Networking Products Getting Started Guide.*

Audience

This guide is intended for network and media administrators who are going to configure and use the E-CDN application. Administrators should be familiar with the following topics:

- Configuration
- Internet browsers
- Media players

Organization

This document is organized in the following manner:

Chapter	Title	Description
Chapter 1	Introducing the Cisco Application and Content Networking Software E-CDN Application	Contains an overview of the ACNS E-CDN application.
Chapter 2	Configuring Content Delivery Network Devices	Describes how to use the Content Distribution Manager to configure and maintain devices on your CDN.
Chapter 3	Working with the Content Delivery Network	Describes how to use the Content Distribution Manager interface to establish, populate, and maintain content channels.
Chapter 4	Administering the System Software	Introduces basic system maintenance procedures such as rebooting devices, reconfiguring devices, moving devices between administrative domains, and backup and restore operations. It also contains application log file information.
Appendix A	Error Messages	Documents CDM error messages and workarounds for common problems.

Conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands and keywords are in **boldface**.
italic font	Arguments for which you supply values are in ***italics***.
[ ]	Elements in square brackets are optional.
{**x** | **y** | **z**}	Alternative keywords are grouped in braces and separated by vertical bars.
[**x** | **y** | **z**]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	An unquoted set of characters. Do not use quotation marks around the string, or the string will include the quotation marks.
`screen` font	Terminal sessions and information the system displays are in `screen` font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.
`italic screen` font	Arguments for which you supply values are in *`italic screen`* font.
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords, are in angle brackets.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

⚠ **Caution** Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Related Documentation

For additional information about the E-CDN application, refer to the following documentation. These documents contain installation (Installation Wizard), configuration, and command reference information regarding the E-CDN application software.

- *Cisco Content Delivery Networking Products Getting Started Guide*
- *Cisco Application and Content Networking Software Command Reference*
- *Cisco ACNS System Maintenance and Troubleshooting Guide*
- *Cisco Application and Content Networking Software Caching Configuration Guide*
- *Release Notes for Cisco Application and Content Networking Software Release 4.1*
- Cisco E-CDN application online help system

For information about hardware platforms related to the E-CDN application, refer to the following documents:

- *Cisco Content Engine 500 Series Hardware Installation Guide*
- *Cisco Content Distribution Manager 4630 Hardware Installation Guide*
- *Cisco Content Router 4430 Hardware Installation Guide*
- *Cisco Content Networking Hardware Installation Guide for the Seven Rack-Unit Chassis*
- *Regulatory Compliance and Safety Information for the Cisco Content Networking Product Series*

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.

CHAPTER 1

Introducing the Cisco Application and Content Networking Software E-CDN Application

This chapter provides a basic conceptual and functional overview of the E-CDN application, including the Content Distribution Manager, Content Routers, and Content Engines that make up the Content Delivery Network (CDN), as well as the architecture (SODA) that enables the E-CDN application to manage content efficiently. This chapter contains the following sections:

Cisco Application and Content Networking Software Overview

Cisco Application and Content Networking Software (ACNS) is a software platform that unifies the Cisco E-CDN application features and the Cisco Cache software features into a single software platform. ACNS software is supported on Content Engines, Content Distribution Managers, and Content Routers. (See the “Platform and Operating System Requirements” section on page 1-8.)

For more information about the Cisco Cache software, refer to the *Cisco Application and Content Networking Software Caching Configuration Guide.*

E-CDN Application Overview

The E-CDN application offers accelerated content delivery, hosting, and other content-based services. It addresses the need to distribute and receive high-bandwidth, media-rich content across the Internet or an intranet without performance losses or content delivery delays.

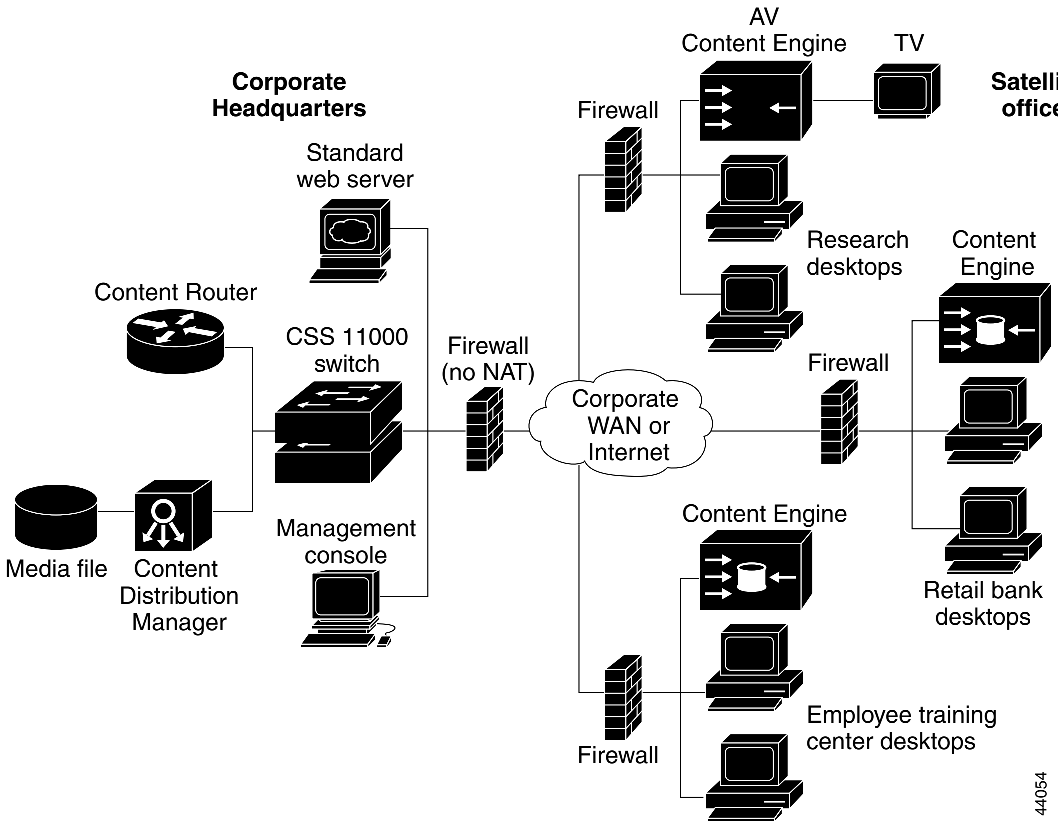
When the ACNS E-CDN application is enabled, Content Engines, Content Routers, Content Services Switches, and Content Distribution Managers can be deployed to create a complete Content Delivery Network system. This system includes content routing, content switching (using the Content Services Switch (CSS) switch), content distribution and management, and content services, as well as content delivery. Figure 1-1 shows a typical E-CDN application topology.

The E-CDN application allows organizations to maximize the impact of web communications by making possible the rapid delivery of high-quality video, rich audio, large graphics, presentations, and documents over corporate LANs, WANs, and other broadband networks.

This guide provides instructions on the use and administration of the E-CDN application, including the Content Distribution Manager, which includes a web-based user interface that is the main conduit to the network for users and administrators. The Content Distribution Manager includes features for configuring new devices and users on the E-CDN application, creating and populating content channels, allocating bandwidth, viewing media over the CDN, and more.

Using the E-CDN application (see Figure 1-1), Internet devices take advantage of Self-Organizing Distributed Architecture (SODA) to efficiently manage high-bandwidth content. SODA enables your organization to leverage existing bandwidth to deliver high-quality media to the desktops of target audiences within your organization.

Figure 1-1 Cisco Enterprise Content Delivery Network



Self-Organizing Distributed Architecture Overview

Self-Organizing Distributed Architecture (SODA) is a proprietary technology that uses sophisticated algorithms to efficiently manage high-bandwidth media over office networks or even over the Internet. The foundation of the E-CDN application software, SODA eliminates network bottlenecks that often accompany large multimedia streaming products.

Content Engines deliver media to desktop users without the typical delays and latency associated with high-bandwidth media streaming through a data network. All the network administrator or desktop user needs to review media is a standard web browser and media player, such as Internet Explorer and Windows Media Player.

To take advantage of SODA technology, a Content Distribution Manager and at least one Content Engine must be installed on your network. The E-CDN application is scalable to multiple sites through the addition of Content Engines and Content Routers to the network.

Content Distribution Manager Overview

The Content Distribution Manager connects to your corporate data network and replicates media to the connected Content Engines through Content Routers located across your LAN. The Content Distribution Manager:

- Controls devices
- Manages media
- Controls redirection of media requests
- Controls media replication to Content Engines

Through the interface you can:

- Configure network settings for the Content Distribution Manager, Content Engines, and Content Routers
- Specify bandwidth parameters for replicating media to the Content Engines and streaming media from the Content Engines
- Import media files to the Content Distribution Manager
- Set replication guidelines

Access the Content Distribution Manager interface from your browser by entering the Content Distribution Manager URL or IP address.

Content Engine Overview

The Content Engine is a device that supports many concurrent streams of Moving Picture Experts Group (MPEG) video or other rich media types. As a remote device attached to your company LAN, the Content Engine identifies itself to the Content Distribution Manager and is subscribed to one or more content channels using the Content Distribution Manager subscriber feature. Once subscribed, Content Engines begin receiving media files for each channel from the Content Distribution Manager. Media files are stored locally on the Content Engine and streamed to end user desktops on demand.

When end users request a media file from the Content Distribution Manager, the Content Distribution Manager sends a redirect to the client's browser redirecting the client to a Content Engine that is local to the user. The client's browser then requests the media from the Content Engine which was selected by the Content Distribution Manager. Using SODA technology, Content Engines are able to calculate the fastest and most efficient route for replication of media and to optimize the allocation of replication bandwidth.

Content Router Overview

Content Routers assist the Content Distribution Manager and serve as backups if the Content Distribution Manager suddenly goes offline. This means that Content Routers allow request redirection to continue, but administrative capabilities are lost. Like Content Distribution Managers, Content Routers store routing hierarchies for CDN devices and can route playback requests from end users to Content Engines, and send the "keepalive" messages that prevent Content Engines from going offline if the Content Distribution Manager is unavailable.

Unlike Content Distribution Managers, there can be multiple Content Routers dispersed throughout the CDN. Also unlike Content Distribution Managers, Content Routers do not create or manage channel content (Content Routers can be subscribed to only the manual upgrade channel when it exists), nor do they store or perform bulk replication of data.

Coverage Zones

Decisions about which devices on your E-CDN application serve a particular request for content are made by the ACNS 4.1 software using a powerful organizing model. In the simplest scenario, requests from workstations on the CDN are routed to the nearest Content Engine on their network. However, CDN administrators can override the CDN default settings and influence content routing through the deployment of "preferred coverage zones" and "regular coverage zones" for Content Engines and the Content Distribution Manager.

Preferred coverage zones are ranges of IP addresses assigned to Content Engines or the Content Distribution Manager. When a request for content originates from an address within the preferred coverage zone of a device, that device (which could be a Content Engine or the Content Distribution Manager) is selected to serve that request.

All requests originating from outside the preferred coverage zones for your CDN devices (that is, requests from a "regular" zone) are processed by the nearest device. The "nearness" of a device is derived from the local network segment each device is on, as determined by its IP address and network mask.

When content requests originate from addresses that are covered by more than one preferred coverage zone or regular coverage zone, the Content Distribution Manager chooses from among the qualified Content Engines in serving the request.

E-CDN Application-Supported Media

The E-CDN application supports any standard media format for import and distribution. Among the supported file types are:

- Advanced Streaming Format (ASF)
- Advanced Stream Redirector (ASX)
- Apple QuickTime
- Graphics Interchange Format (GIF)
- HTML
- Joint Photographic Experts Group (JPEG)
- Moving Picture Experts Group (MPEG-1)

- MPEG-2
- RealMedia
- Shockwave
- Synchronized Multimedia Integration Language (SMIL)
- Windows Media Audio (WMA)
- Windows Media Audio Redirector (WAX)
- Windows Media Audio-Video (WMV)
- Windows Media Redirector (WMX)
- Windows Media Video Redirector (WVX)

Media Files Distribution

Media is imported to the Content Distribution Manager in an efficient manner and is downloaded to Content Engines according to bandwidth constraints you set. Using a web browser, users can view these media files on their PCs.

From a Content Distribution Manager, you can import and replicate, or distribute, your media files to Content Engines. The network uses standard Internet TCP/IP protocols for all communication.

All transfers are fault-tolerant. This means that if a file transfer is interrupted, the replication process picks up where it left off, rather than resending the entire channel.

E-CDN Application System Requirements

Users and CDN administrators interact with the E-CDN application using a web-based graphical user interface to the Content Distribution Manager that provides easy access to most CDN functions. The following minimum hardware and software requirements apply to each machine that will be used as a workstation to access the Content Distribution Manager.

Network Requirements

Ethernet connection

Platform and Operating System Requirements

- Windows 95/98 or Windows 2000 Pentium-class system, 133 MHz, 32 MB of RAM
- Windows NT Pentium-class system, 200 MHz, 64 MB of RAM
- Apple Macintosh G3-class, 32 MB of RAM

Browser Requirements

Microsoft Internet Explorer 5.0/5.5 or Netscape Communicator Version 4.7

Media Player Requirements

- Microsoft Windows Media Player 6.x or later
- RealNetworks RealPlayer Version 6.x or 7.0
- Apple QuickTime Version 4.0

Cisco IOS Software Requirement

Cisco IOS Software Release 12.2(4)T is required for support of Resource Reservation Protocol (RSVP), Quality of Service (QoS), and multicast.

CHAPTER 2

Configuring Content Delivery Network Devices

This chapter provides information on configuring your CDN devices, including the Content Distribution Manager, Content Routers, and Content Engines, as well as creating user accounts and setting parameters for media replication and playback.

Note Make sure that you have unpacked your Content Distribution Manager, Content Router, and Content Engine hardware, as well as activated your Content Distribution Manager. Refer to the *Cisco Content Delivery Networking Products Getting Started Guide* for more information on completing these preliminary steps before continuing with this chapter.

This chapter contains the following sections:

Verifying Content Distribution Manager Configuration

Before attempting to log on to your Content Distribution Manager, you must have first activated the Content Distribution Manager by following the procedure outlined in the *Cisco Content Delivery Networking Products Getting Started Guide*.

To log on to your Content Distribution Manager, verify configuration settings, and, if necessary, modify configuration settings, perform the following steps:

Step 1 Open the Content Distribution Manager user interface from your web browser by entering the URL or IP address for the Content Distribution Manager. For example, from your browser, enter:

```
http://name_of_Content_Distribution_Manager
```

or

```
http://IP_address_of_Content_Distribution_Manager
```

If a screen appears requesting your username and password, the Content Distribution Manager was successfully activated and is up and running on your network.

Note If using a DNS name for the Content Distribution Manager then DNS server configuration is needed on the CLI and in the Content Manager GUI.

Step 2 Enter the default administrator username and password as follows, and then click **OK**.

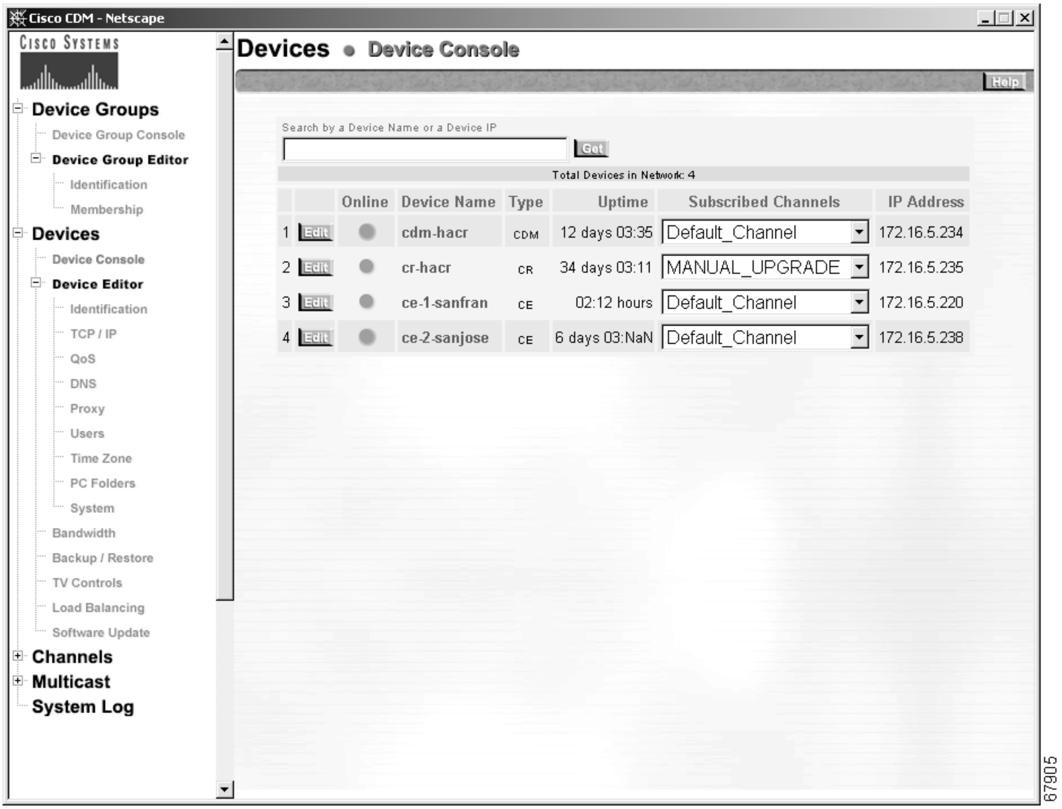
```
Username: admin
Password: default
```

The Cisco Content Distribution Manager screen appears.

Step 3 Choose **Devices > Device Console** and verify that the Content Distribution Manager is listed as an online device.

A green circle appears in the Online column. Any other active CDN devices should also be listed here. (See Figure 2-1.)

Figure 2-1 Devices Device Console Screen



Total Devices in Network: 4

		Online	Device Name	Type	Uptime	Subscribed Channels	IP Address
1	Edit	●	cdm-hacr	CDM	12 days 03:35	Default_Channel	172.16.5.234
2	Edit	●	cr-hacr	CR	34 days 03:11	MANUAL_UPGRADE	172.16.5.235
3	Edit	●	ce-1-sanfran	CE	02:12 hours	Default_Channel	172.16.5.220
4	Edit	●	ce-2-sanjose	CE	6 days 03:NaN	Default_Channel	172.16.5.238

Step 4 You can now proceed with the configuration of your other CDN devices such as Content Engines and Content Routers. See the next section, "Setting Up Content Delivery Network Devices."

Setting Up Content Delivery Network Devices

Once you have verified that your Content Distribution Manager is up and running, you can set up or configure your Content Engines or Content Routers. This step is necessary in order for you to begin distributing media files to users on the CDN.

After devices have been configured for the first time using the Installation Wizard or the CLI commands, the Content Distribution Manager Device Editor can be used to modify configuration settings.

To configure your E-CDN application devices (Content Distribution Manager, Content Routers, and Content Engines), follow the sequence of steps for configuring CDN devices in the *Cisco Content Delivery Networking Products Getting Started Guide.*

Once initial configuration is complete, use the information that follows in this chapter to edit the configuration of your E-CDN application devices using the Content Distribution Manager Device Editor.

Editing Network and E-CDN Application Settings

You use the Devices menu to manage your E-CDN application devices in your network. From the Devices menu you can configure the Content Distribution Manager, Content Routers, and Content Engines and edit device properties.

Note Only users with administrator privileges have access to the Devices menu.

The E-CDN application device properties that can be edited include the device configuration properties described in Table 2-1.

Table 2-1 Device Configuration Properties

Device Property	Description
Identification	Name and description.
TCP/IP	Indicates whether to use DHCP or manually configure static IP addresses for your E-CDN application devices.
QoS	Indicates whether the selected Content Engine will employ Quality of Service (QoS) guarantees when delivering media to a requesting CDN user. Content Routers do not use QoS.
DNS	Indicates whether to use a Domain Name System (DNS) server.
Proxy	Indicates whether to use a proxy server.

Table 2-1 Device Configuration Properties (continued)

Device Property	Description
Users	Changes the system administration password, and adds or modifies E-CDN application user accounts.
Time Zone	Sets the geographical region and time zone for each device.
PC Folders	Configures your device to import media files from Windows for your network.
System	Updates the E-CDN application or reboots a device.

Editing the Device Name and Description

Although changing the name of a device and adding a description for it are optional, we recommend that you change the default name of each device to something more meaningful to you and that you add some descriptive information, such as location, for each device. See Figure 2-2 and Table 2-2 for more information on the Identification screen and its options.

The default name of a device is the device's system ID, which is in the form:

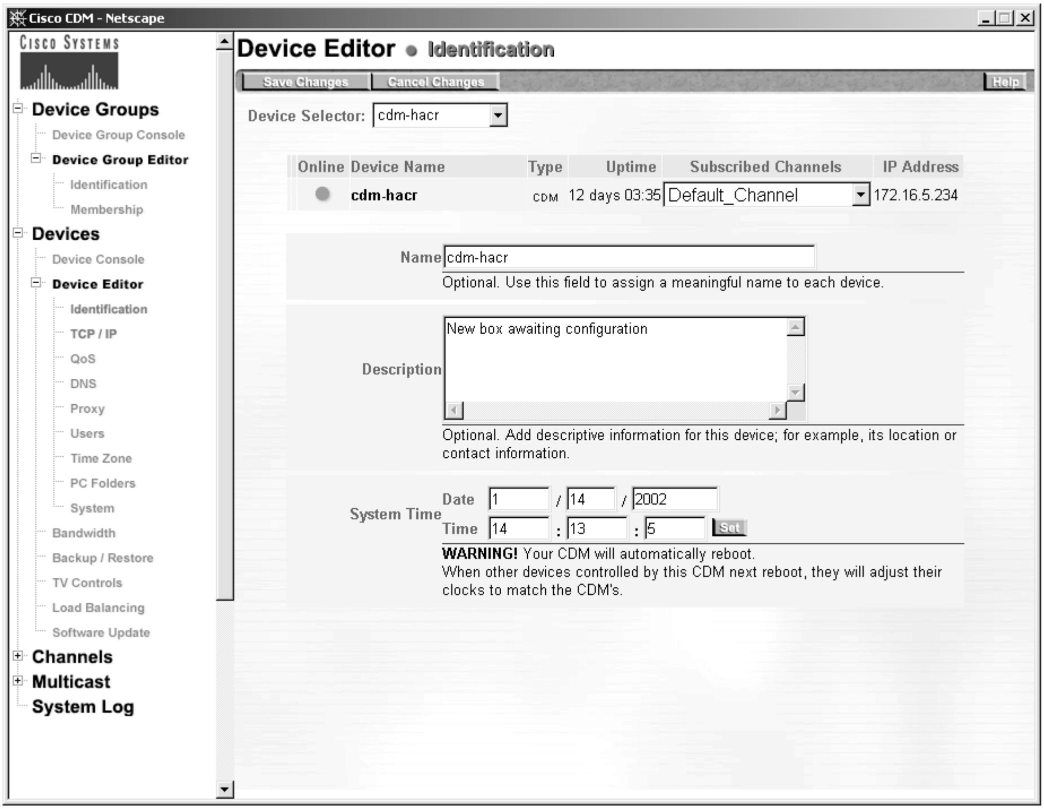
MAC_address.box.*provider*.sn

Note The name cannot contain any spaces.

To enter an identifying name and description for a device, perform the following steps:

Step 1 Choose **Devices > Device Editor > Identification**. (See Figure 2-2.) The Device Editor Identification screen appears.

Figure 2-2 Device Editor Identification Screen



Device Editor ● Identification

Device Selector: cdm-hacr

Online	Device Name	Type	Uptime	Subscribed Channels	IP Address
●	cdm-hacr	CDM	12 days 03:35	Default_Channel	172.16.5.234

Name: cdm-hacr
Optional. Use this field to assign a meaningful name to each device.

Description: New box awaiting configuration
Optional. Add descriptive information for this device; for example, its location or contact information.

System Time
Date 1 / 14 / 2002
Time 14 : 13 : 5

WARNING! Your CDM will automatically reboot.
When other devices controlled by this CDM next reboot, they will adjust their clocks to match the CDM's.

Step 2 Choose the device that you want to edit from the Device Selector drop-down list. Some general information about the selected device is displayed. The default name is listed in the Name field.

Step 3 Enter a new name and description, as needed.

Step 4 Click **Save Changes**.

Clicking **Cancel Changes** returns all values to their previous settings when you last clicked **Save Changes**.

Table 2-2 Device Identification Properties

Device Identification	Description
Online	Indicates whether a device is online or not. A solid green circle shows that the device is online. A red circle shows that the device is not online. A yellow triangle indicates the device has not been approved by the Content Distribution Manager. See the "Setting Up Content Delivery Network Devices" section on page 2-3.
Device Name	Displays the name of the selected device.
Type	Identifies the device as a Content Distribution Manager, Content Router, or Content Engine.
Uptime	Specifies how long the device has been running since it was last rebooted.
Subscribed Channels	Identifies channels, or content groups, to which the device is subscribed. See the "Creating Channels" section on page 3-2 and the "Subscribing a Content Engine to a Channel" section on page 3-10 for more information.
IP Address	Displays the Internet Protocol (IP) address assigned to the device.

Setting the System Time

All devices on the CDN set their time based on two settings:

- System time—This setting defines the date in MM/DD/YYYY format and time in HH:MM:SS format using a 24-hour clock for the Content Distribution Manager, Content Routers, and all associated Content Engines.

  Note If the system time for the Content Distribution Manager is changed, then the devices may automatically reboot if they detect a clock skew.

- Time zone—This setting is configured for each device separately, allowing devices that are geographically dispersed to coordinate with one another and to apply the appropriate local time settings, based on the system time, when you change bandwidth settings or activate playlists.

To set the system time for your CDN, perform the following steps:

Step 1 Choose **Devices > Device Editor > Identification**. The Device Editor Identification screen appears.

Step 2 From the Device Selector drop-down list, choose the Content Distribution Manager.

Step 3 Next to the System Time heading, place your cursor in the first Date field and enter the date in MM/DD/YYYY format. Press the **Tab** key to move between fields when entering the date.

Step 4 Move your cursor to the first Time field and enter the time in HH:MM:SS format. Press the **Tab** key to move between fields when entering the time.

Step 5 Click **Set**. You are prompted to confirm your decision to reset your system time.

Note Setting or changing the system time causes the Content Distribution Manager to reboot immediately. You must manually reboot your Content Engines and Content Routers for them to begin using the new system time settings.

Step 6 Click **OK** to confirm your decision. Clicking **Cancel** returns the system time values to their previous settings.

Setting the Time Zone for a Device

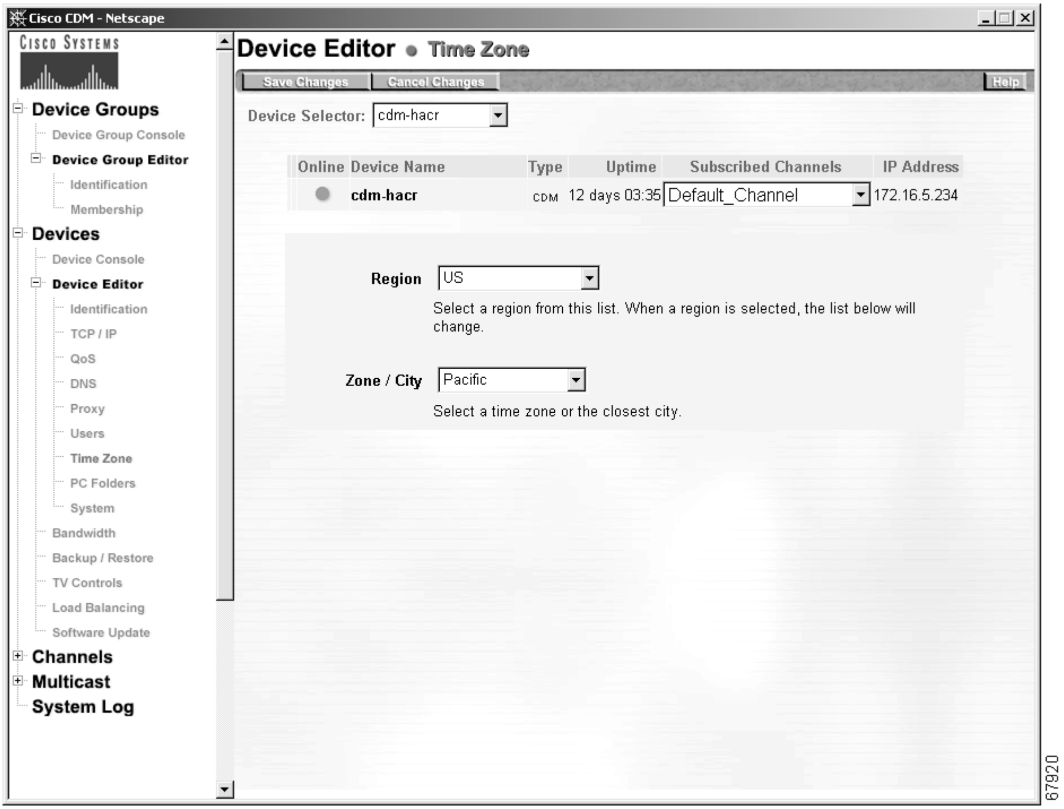
Use this option to set the region and time zone for each of your CDN devices. Specifying a time zone is important when coordinating activity on geographically dispersed CDN devices.

To set the time zone for a device:

Step 1 Choose **Devices > Device Editor > Time Zone**. The Device Editor Time Zone screen appears (See Figure 2-3.)

Step 2 Make sure that the correct device is displayed in the Device Selector drop-down list. If it is not, choose the correct device from the drop-down list. Some general information about the selected device is displayed.

Figure 2-3 Device Editor Time Zone Screen



Device Selector: cdm-hacr

Online	Device Name	Type	Uptime	Subscribed Channels	IP Address
●	cdm-hacr	CDM	12 days 03:35	Default_Channel	172.16.5.234

Region: US

Select a region from this list. When a region is selected, the list below will change.

Zone / City: Pacific

Select a time zone or the closest city.

Step 3 Choose a region in the Region list. When you have chosen a region, the zone/city settings change correspondingly.

Step 4 Choose a time zone or city from the Zone/City list.

Step 5 Click **Save Changes**.

Clicking **Cancel Changes** returns all values to their previous settings when you last clicked **Save Changes**.

Editing TCP/IP Settings

If you are using DHCP, TCP/IP properties are set automatically by the DHCP server. If you are not using DHCP, you must specify TCP/IP properties manually.

To specify a DHCP server or to enter IP address information, perform the following steps:

Step 1 Choose **Devices > Device Editor > TCP/IP**. The Device Editor TCP/IP screen appears. (See Figure 2-4.)

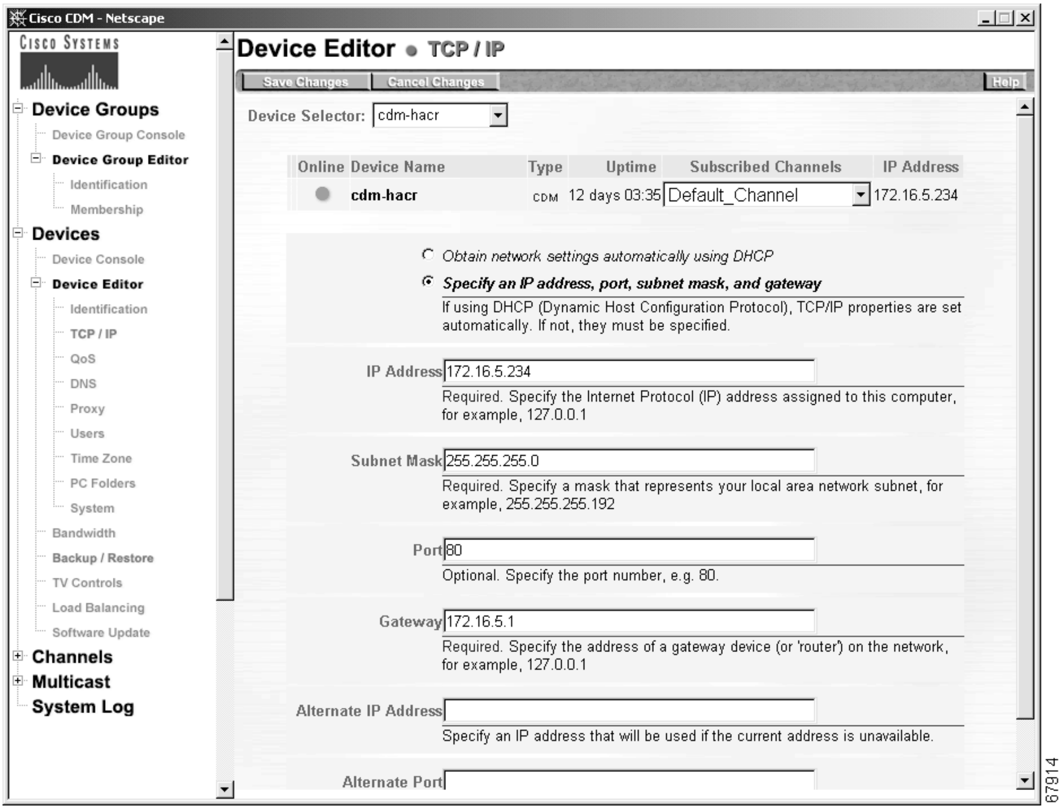
Step 2 Choose the correct device from the Device Selector drop-down list.

General information about the selected device is displayed.

- If the network that your device is running on uses DHCP, go to Step 3.
- If the network that your device is running on does not use DHCP, go to Step 4.

Step 3 Click **Obtain network settings automatically using DHCP** and go to Step 5.

Figure 2-4 Device Editor TCP/IP Screen



Device Editor ● TCP / IP

Device Selector: cdm-hacr

Online	Device Name	Type	Uptime	Subscribed Channels	IP Address
●	cdm-hacr	CDM	12 days 03:35	Default_Channel	172.16.5.234

○ Obtain network settings automatically using DHCP

● Specify an IP address, port, subnet mask, and gateway

If using DHCP (Dynamic Host Configuration Protocol), TCP/IP properties are set automatically. If not, they must be specified.

IP Address: 172.16.5.234
Required. Specify the Internet Protocol (IP) address assigned to this computer, for example, 127.0.0.1

Subnet Mask: 255.255.255.0
Required. Specify a mask that represents your local area network subnet, for example, 255.255.255.192

Port: 80
Optional. Specify the port number, e.g. 80.

Gateway: 172.16.5.1
Required. Specify the address of a gateway device (or 'router') on the network, for example, 127.0.0.1

Alternate IP Address:
Specify an IP address that will be used if the current address is unavailable.

Alternate Port:

Step 4 Click **Specify an IP address, subnet mask, port, and gateway** to set an IP address, subnet mask, port, and gateway.

Enter the information as required for the network.

- IP Address—Specifies the IP address assigned to the computer (required).
- Subnet Mask—Specifies a mask that represents your local-area network subnet (required).
- Port—Specifies a port number (optional). The default port is 80.Select another port number if you want to use port 80 for something else.
- Gateway—Specifies the address of a gateway device (or router) on the network (required).

Step 5 Click **Save Changes**.

Clicking **Cancel Changes** returns all values to their previous settings when you last clicked **Save Changes**.

Step 6 Choose **Devices > Device Editor > System**. The Device System Editor screen appears. Click **System Reboot** to ensure that the new settings will take effect.

Note You *must* reboot the Content Distribution Manager from the Device Editor System screen after saving the TCP/IP settings, or the settings will not take effect.

Changing the Content Distribution Manager IP Address

Changing the IP address of your Content Distribution Manager can have ramifications throughout your entire CDN. When changing the address of your Content Distribution Manager, remember to:

- Make sure that you configure the Content Distribution Manager *before* it is moved, rather then attempting to change the Content Distribution Manager IP settings after the move has taken place.
- Point your Content Engines and Content Routers to the new Content Distribution Manager IP address and verify that all Content Engines and Content Routers are able to reach the Content Distribution Manager at its new address.

To reset your Content Distribution Manager IP address and point your Content Engines and Content Routers to the new location of your Content Distribution Manage, perform the following steps:

Step 1 Choose **Devices > Device Editor > TCP/IP**. The Device Editor TCP/IP screen appears.

Step 2 Choose the correct device from the Device Selector drop-down list.

Step 3 Click the **Specify an IP address, port, subnet mask, and gateway** option. The current IP address of the Content Distribution Manager appears in the IP Address field.

Step 4 Without changing any of the information presented, place the cursor in the Alternate IP Address field and enter the IP address to which the Content Distribution Manager will be moving in valid “dotted quad” format. For example:

```
192.168.200.0
```

Step 5 Click **Save Changes** to save the address.

Step 6 Wait approximately 1 hour before moving the Content Distribution Manager to the address you entered in the Alternate IP Address field.

Step 7 When an hour has passed, you can change the Content Distribution Manager actual IP address using the Content Distribution Manager Device Editor or the E-CDN Installation Wizard, or by reconfiguring your DHCP server. Enter the new IP address of the Content Distribution Manager in the IP Address field on the TCP/IP screen. This address should match the address in the Alternate IP Address field.

See the “Editing TCP/IP Settings” section on page 2-11 for more instructions on changing the IP address of E-CDN application devices.

Step 8 Click **Save Changes**.

Step 9 Click **System**.

The System screen appears.

Step 10 Make sure that the Content Distribution Manager is selected in the Device Selector drop-down list. If it is not, expand the drop-down list and choose your Content Distribution Manager from the devices listed.

Step 11 Click **System Reboot** to reboot your Content Distribution Manager and reconnect it to your network using the new IP address.

Step 12 Wait for your Content Engines and Content Routers to reconfigure themselves to point to the new address of the Content Distribution Manager.

Note Approximately 45 minutes after your Content Distribution Manager comes back online at its new address, your Content Engines and Content Routers will begin going offline because they can no longer detect the Content Distribution Manager at its prior address. They will then automatically use the alternate IP address to connect to the Content Distribution Manager's new IP address.

Step 13 Click **Device Console**. Monitor your Content Engines and Content Routers and verify that each device is able to locate the Content Distribution Manager and come back online.

If one or more Content Engines or Content Routers are not able to resolve the Content Distribution Manager's new address, use the Installation Wizard to manually point them to the location of the Content Distribution Manager. See the "Installation Wizard-Based Reconfiguration" section on page 4-7 for information.

Editing Quality of Service Settings

Quality of Service (QoS) is a strategy that helps to guarantee uninterrupted high-bandwidth video and multimedia content delivery over your E-CDN application. Content Engines use QoS when sending media to requesting clients, and use one of two transmission protocols:

- Resource Reservation Protocol (RSVP)—When Content Engines use RSVP, streams of packets passing through gateway hosts are expedited based on policies and bandwidth reservation requests made in advance by the requesting client and cleared from the client all the way back to the Content Engine. Using RSVP, hosts can request per-flow resources in advance of broadcast or playback. RSVP is ideally suited for smaller CDNs, in which the total number of data flows remains small.
- Differentiated Services (DiffServ)—When Content Engines use DiffServ, the behaviors of individual packets are controlled from point to point between the Content Engine and the requesting client (these are referred to as per-hop

behaviors). These travel instructions are stored in the IP header for each network packet. DiffServ is well suited to large CDNs in which the number of data flows is large, and in which flexibility and scalability are paramount.

Using the Content Distribution Manager Device Editor, you can enable the QoS feature and then configure Content Engines to use both RSVP and DiffServ when sending data to E-CDN application clients.

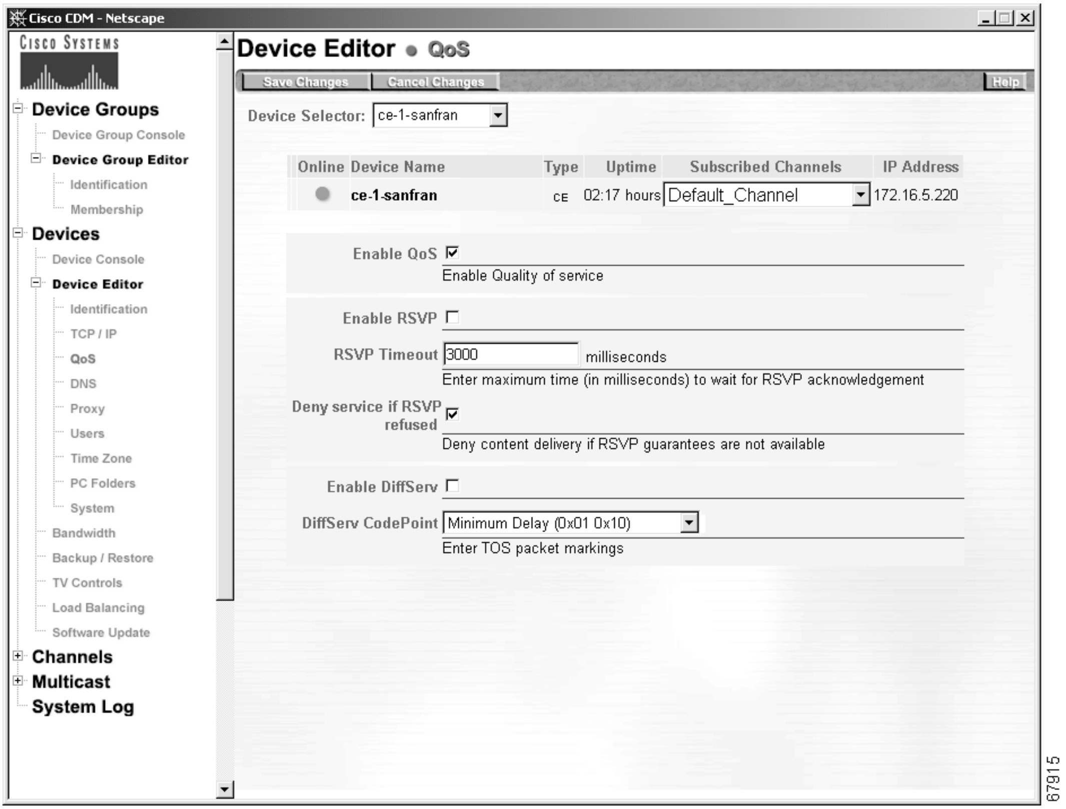
Note Content Routers do not use QoS. The QoS option is disabled when the selected device is a Content Router.

To enable the QoS feature, perform the following steps:

Step 1 Choose **Devices > Device Editor > QoS**. The Device Editor QoS screen appears. (See Figure 2-5.)

Step 2 Choose the Content Engine for which you are enabling QoS from the Device Selector drop-down list.

Figure 2-5 Device Editor QoS Screen



Device Editor ● QoS

Device Selector: ce-1-sanfran

Online	Device Name	Type	Uptime	Subscribed Channels	IP Address
●	ce-1-sanfran	CE	02:17 hours	Default_Channel	172.16.5.220

Enable QoS ☑
Enable Quality of service

Enable RSVP □

RSVP Timeout 3000 milliseconds
Enter maximum time (in milliseconds) to wait for RSVP acknowledgement

Deny service if RSVP refused ☑
Deny content delivery if RSVP guarantees are not available

Enable DiffServ □

DiffServ CodePoint Minimum Delay (0x01 0x10)
Enter TOS packet markings

Step 3 Check the **Enable QoS** check box. Options for enabling RSVP and DiffServ appear.

See the following sections for information on configuring RSVP and DiffServ for your E-CDN application.

Enabling RSVP

When enabling RSVP, you can specify the following:

- RSVP Timeout—Time period during which the RSVP server on your network must respond to the Content Engine reservation request. If the RSVP server fails to respond within the specified timeframe, the request is canceled.
- Enable RSVP Service Policy—Option that allows RSVP requests to be created on your RSVP server even when the server cannot guarantee bandwidth along the entire delivery path.

To enable a Content Engine to use RSVP as part of QoS when sending media to requesting clients, perform the following steps:

Step 1 Check the **Enable RSVP** check box.

Step 2 In the RSVP Timeout field, enter the timeout value in milliseconds. This is the length of time that the requesting Content Engine will wait for acknowledgment of the RSVP request from intermediary devices before canceling the request. For example, a timeout value of one-half second would be:

```
500
```

Step 3 If you wish RSVP requests to be sent regardless of whether bandwidth guarantees have been received from all intermediary devices along the delivery route, check the **Enable RSVP Service Policy** check box.

Step 4 Click **Save Changes** to save your RSVP configuration settings for the selected Content Engine.

If you need to configure your Content Engine to use the DiffServ protocol in addition to RSVP, see the next section, "Enabling DiffServ."

Enabling DiffServ

When enabling the DiffServ protocol, you are required to specify a Differentiated Services Code Point (DSCP), which controls the per-hop behavior of packets transferred from the Content Engine to the requesting client. The code point setting determines the instructions that network packets follow at each point (or hop) along their path to the requesting client. The DSCP options are:

- Minimum delay (0x01 0x02)
- Maximum throughput (code point 0x01 0x08)
- Maximum reliability (0x01 0x04)
- Minimum cost (0x01 0x02)

To enable a Content Engine to use DiffServ as part of QoS when sending media to requesting clients, perform the following steps:

Step 1 Check the **Enable DiffServ** check box.

Step 2 Click the **DiffServ CodePoint** drop-down arrow.

Step 3 Choose from among the DSCP settings on the list. DSCP settings determine the per-hop instructions assigned to each network packet on the path between the Content Engine and the requesting client.

Step 4 Click **Save Changes** to save your DiffServ configuration settings for the selected Content Engine.

If you need to configure your Content Engine to use the RSVP protocol in addition to DiffServ but have not yet done so, see the "Enabling RSVP" section on page 2-18.

Editing DNS Server Settings

A DNS server is used to provide user-friendly names for computers in a network, including the Content Distribution Manager, Content Routers, and Content Engines that make up your E-CDN application. If a DNS server is not used, the numerical value of the IP address is used to identify and access machines on your network.

To enter DNS server settings, perform the following steps:

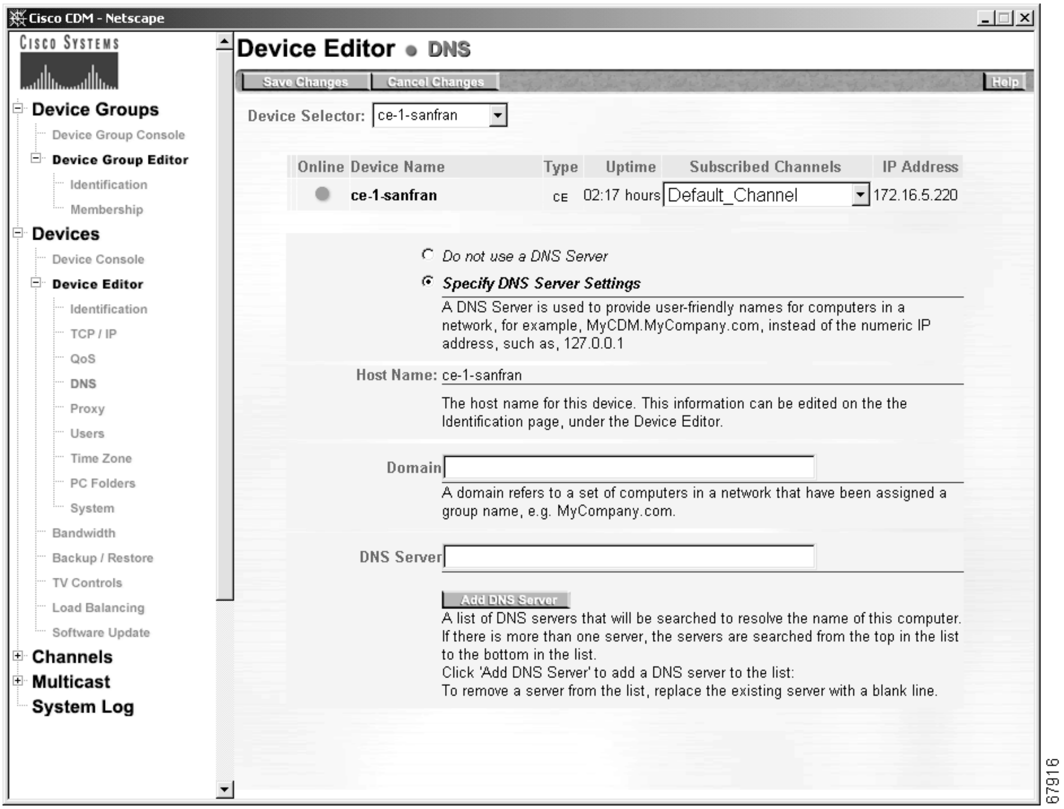
Step 1 Choose **Devices > Device Editor > DNS**. The Device Editor DNS screen appears. (See Figure 2-6.)

Step 2 Make sure that the correct device is displayed from the Device Selector drop-down list. If it is not, choose it from the drop-down list.

General information about the selected device is displayed.

- If you do not use a DNS server, click **Do not use a DNS Server** and go to Step 4.
- If you use a DNS server, click **Specify DNS Server Settings** and go to Step 3.

Figure 2-6 Device Editor DNS Screen



Device Selector: ce-1-sanfran

Online	Device Name	Type	Uptime	Subscribed Channels	IP Address
●	ce-1-sanfran	CE	02:17 hours	Default_Channel	172.16.5.220

○ Do not use a DNS Server

● Specify DNS Server Settings

A DNS Server is used to provide user-friendly names for computers in a network, for example, MyCDM.MyCompany.com, instead of the numeric IP address, such as, 127.0.0.1

Host Name: ce-1-sanfran

The host name for this device. This information can be edited on the the Identification page, under the Device Editor.

Domain

A domain refers to a set of computers in a network that have been assigned a group name, e.g. MyCompany.com.

DNS Server

A list of DNS servers that will be searched to resolve the name of this computer.
If there is more than one server, the servers are searched from the top in the list to the bottom in the list.
Click 'Add DNS Server' to add a DNS server to the list:
To remove a server from the list, replace the existing server with a blank line.

Step 3 Enter the following information to identify your DNS server:

- Host Name—DNS name of the E-CDN application device on your LAN (assigned by your network administrator).
- Domain—Name assigned to the group of computers on your network to which the device belongs, for example, acme.com.
- DNS Server—Network address of your Domain Name System server.

  If your network is using more than one DNS server, click **Add Server** to add another DNS server to the list, and repeat this step.

Step 4 Click **Save Changes**.

Editing Proxy Server Settings

A web server or HTTP proxy server might be required by your site administrator to access the Internet. The following definitions should help you configure your proxy server for use with the E-CDN application. See Table 2-3 for information and default proxy server settings.

After saving changes to your proxy server settings, you must reboot all affected E-CDN application devices, including your Content Distribution Manager and any affected Content Routers and Content Engines, before resuming use of the E-CDN application. Rebooting affected devices ensures that changes to your proxy server settings are communicated to all devices in your CDN.

Table 2-3 Proxy Server Configuration Settings

Device Setting	Description
HTTP Address and Port	(Required) IP address and port number of the proxy server used to access the Internet using HTTP protocol. The default HTTP port is 80.
Secure Address and Port	(Required) IP address and port number of the proxy server used to access the Internet using secure HTTP protocol. The default secure address port number is 443.
Exceptions	(Optional) Addresses for which the proxy server is not used so that data transmission occurs directly over the LAN or Internet. **Note** The format for the Exceptions address is *IP_address/subnet_mask*, for example: 10.0.0.0/8.

To enter proxy server settings, perform the following steps:

Step 1 Choose **Devices > Device Editor > Proxy**. The Device Editor Proxy Server screen appears. (See Figure 2-7.)

Step 2 Choose the correct device from the Device Selector drop-down list. General information about the selected device is displayed.

- If you do not use a proxy server, click **Do not use a proxy server** and proceed to Step 4.
- If you do use a proxy server or secure proxy server, click **Specify proxy server settings** and proceed to Step 3.

Step 3 Enter the proxy server configuration settings.

See Table 2-3 for a description of each setting.

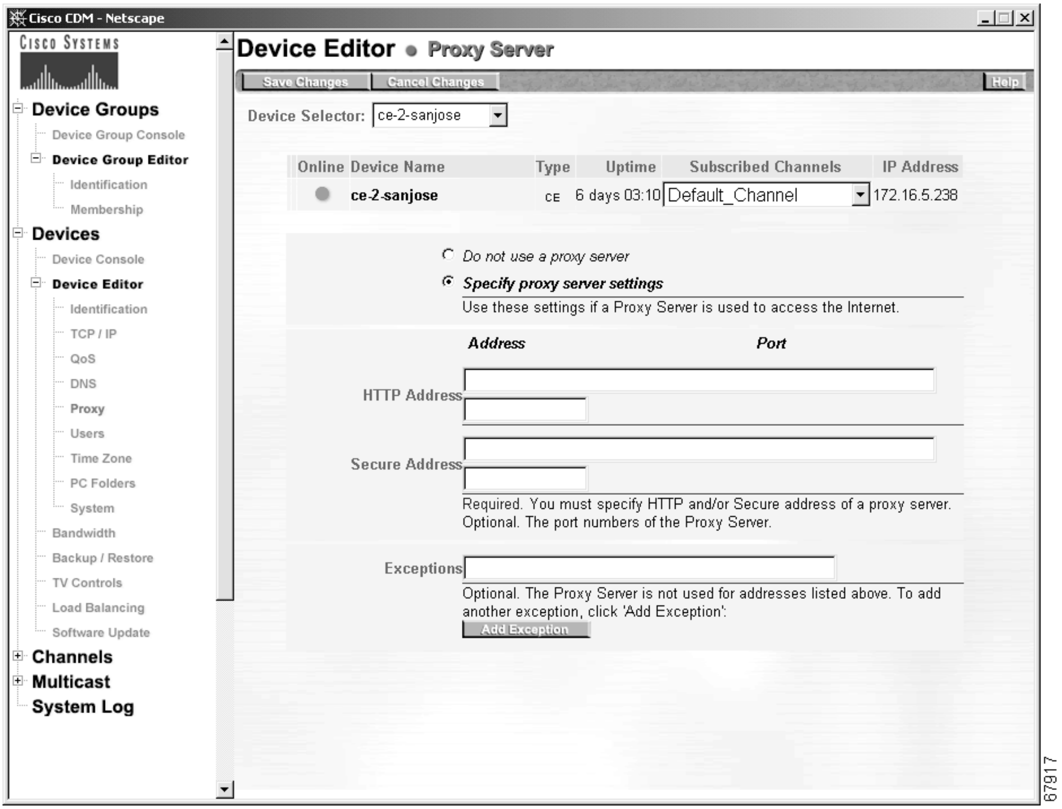
If you are using a secure proxy server, the address and port for the server will appear in the fields labeled Secure Address.

If you want to exempt certain IP addresses from using the proxy server, add them at this time. Enter the first exception IP address in the Exceptions field provided.

If there are multiple exception addresses, click **Add Exception** to add another field for entering an exception address, and then enter the proxy exception address.

Repeat this step for each exception address.

Figure 2-7 Device Editor Proxy Server Screen



Device Editor ● Proxy Server

Device Selector: ce-2-sanjose

Online	Device Name	Type	Uptime	Subscribed Channels	IP Address
●	ce-2-sanjose	CE	6 days 03:10	Default_Channel	172.16.5.238

○ *Do not use a proxy server*

● ***Specify proxy server settings***

Use these settings if a Proxy Server is used to access the Internet.

	Address	Port
HTTP Address		
Secure Address		

Required. You must specify HTTP and/or Secure address of a proxy server.
Optional. The port numbers of the Proxy Server.

Exceptions

Optional. The Proxy Server is not used for addresses listed above. To add another exception, click 'Add Exception':

Step 4 Click **Save Changes**.

Step 5 Repeat Step 1 through Step 4 for each device that requires changes to its proxy server settings. You will have to reboot each device you have changed, beginning with any affected Content Engines and Content Routers, and concluding with the Content Distribution Manager.

Step 6 From the Device Editor, choose **System**. The Device Editor System screen appears.

Step 7 Choose a Content Engine from the Device Selector drop-down list.

The Device Editor System screen displays the Content Engine system information.

Step 8 Click **System Reboot**.

Step 9 Repeat Step 6 through Step 8 for each affected Content Engine and Content Router, as well as the Content Distribution Manager.

You are ready to resume use of the E-CDN application with new proxy settings when your Content Distribution Manager finishes rebooting.

Interaction Between the HTTP Proxy Cache and the E-CDN Application

If the E-CDN application is enabled in ACNS 4.1 software, with the E-CDN application HTTP server listening on default port 80 for HTTP requests and port 443 for Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) requests, interaction may occur between the proxy and the E-CDN application.

The interaction does not occur if the E-CDN application listens on ports other than the default port 80 for HTTP and port 443 for HTTPS. Interactions between the proxy and the E-CDN application are:

- Rules Template—If the Rules Template is enabled, many rules also apply to E-CDN application HTTP requests and communication. These rules are **block**, **redirect**, **rewrite**, and **use-server**. Other rules apply to HTTP-specific parameters and do not apply here.
- HTTP authentication—HTTP authentication using Remote Authentication User Dial-In Service (RADIUS), Lightweight Directory Access Protocol (LDAP), or NT Lan Manager (NTLM) does not apply to the E-CDN application.
- URL filtering—If this option is enabled, it also applies to E-CDN application HTTP requests and communication, both Websense and built-in goodlist and badlist filtering.

- Proxy transaction log—If the proxy transaction log is enabled, all E-CDN application requests are also logged to the proxy transaction log. This includes both end user requests for E-CDN application content as well as communication between the Content Distribution Manager and the Content Engine. Therefore, if the transaction log is exported, the extra E-CDN application requests are also visible. For HTTPS requests, the log entry does not contain all of the normal information that a normal entry contains, but it does contain the client IP address and request time.
- DNS name—If you are using a DNS name for browsing to the Content Distribution Manager, then you need to have a DNS name server configured on the CLI.

Assigning Coverage Zones to CDN Devices

The Content Distribution Manager and all Content Engines, by default, serve a coverage zone—a range of IP addresses that is assigned to a device. You can define the coverage zones of a device to maximize the efficiency with which content requests are served.

About Coverage Zones

Decisions about which devices running the E-CDN application serve a particular request for content are made by the CDN software using an intelligent model designed to maximize the success of each content request.

In the simplest scenario, requests from workstations on the CDN are routed to the nearest Content Engine on the network by the Content Distribution Manager or Content Router. However, E-CDN application administrators can override the default settings and influence content routing through the deployment of "preferred coverage zones" and "regular coverage zones" for Content Engines and even the Content Distribution Manager.

Preferred coverage zones are ranges of IP addresses assigned to Content Engines or the Content Distribution Manager. When a request for content originates from an address within the preferred coverage zone of a Content Engine or the Content Distribution Manager, that device is directed to serve the request.

All requests originating from outside the preferred coverage zone for a device are processed by the nearest device. "Nearness" is determined by the local network segment of each device, defined by its IP address and network mask.

When content requests originate from addresses that are covered by more than one preferred coverage zone or regular coverage zone, the Content Distribution Manager chooses a Content Engine from among the qualified Content Engines to serve the request.

Creating Coverage Zones

Coverage zones are ranges of IP addresses on the E-CDN application that are associated with content-serving devices. You can specify two types of coverage zones:

- Preferred coverage zones

  Preferred coverage zones are groupings of IP addresses served by a single Content Engine or group of Content Engines. Requests originating from within the range of preferred addresses are served by one of a small group of designated Content Engines, ideally devices that are in close physical proximity, ensuring optimal performance. By default, all Content Engines serve a preferred coverage zone that is defined by their local network segment (determined by the IP address and the netmask configured for the device).

- Regular coverage zones

  Regular coverage zones are broader groupings of IP addresses served generally by a Content Distribution Manager and a pool of Content Engines on the CDN.

Coverage zones that override the network defaults can be defined separately for each Content Engine and for the Content Distribution Manager. When devices are not assigned a particular coverage zone, they use default “preferred” and “regular” coverage zones.

To assign a preferred coverage zone or regular coverage zone to a Content Engine, perform the following steps:

Step 1 Choose **Devices > Device Editor > System**. The Device Editor System screen appears.

Step 2 Choose the correct Content Engine from the Device Selector drop-down list. General information about the selected device is displayed.

Step 3 In the section labeled Device Coverage Zones, choose the **Specify coverage zone settings** option. Fields for configuring your coverage zones appear.

Step 4 If you are configuring a preferred coverage zone for the Content Engines, place the cursor in the Preferred field and enter the address range and netmask in the proper format.

The format for the coverage zone address is *IP_address/netmask*, for example:

```
192.168.0.0/24
```

You can also specify a series of specific addresses and netmasks in this field separated by semicolons, for example:

```
192.168.200.222/32; 192.168.200.223/32; 192.168.200.224/32
```

Step 5 Repeat Step 4 for the regular coverage zone by moving your cursor to the Regular field and entering the address range in the proper format.

As with the preferred coverage zone address field, you can also enter a range of addresses in the Regular field.

Step 6 In the Network Hierarchy section, check the **Build the network hierarchy automatically** check box if you want to build a hierarchy of devices in the network. The hierarchy is used for content replication. Disabling the protocol makes this device a direct child of the Content Distribution Manager.

Step 7 Click **Save Changes** to assign the preferred and regular coverage zones you specified to the selected device.

Note If storage is added to or removed from devices (Content Distribution Managers and Content Engines only), click the **Update Storage Capacity** button to determine if the added or removed storage has changed and is recognized by the E-CDN software.

Specifying Bandwidth

You use the Content Distribution Manager Bandwidth feature to set the maximum bandwidth to be used by each device for replicating media to the Content Engines and for streaming media to user desktops. Bandwidth controls limit the bandwidth consumed by your Content Distribution Manager and Content Engines. Bandwidth can be limited in megabits per second for both replication and playback.

- Playback bandwidth sets the maximum bandwidth to stream media from a Content Distribution Manager or Content Engine to user desktops for playback, typically based on the LAN bandwidth between the device and the desktops.
- Replication bandwidth sets the maximum bandwidth needed to move media files that are imported to a channel between E-CDN devices.

Intelligent bandwidth management provides the ability to limit the maximum bandwidth allowed for replication between E-CDN application devices to particular days of the week and hours of the day.

Setting Playback Bandwidth

Content Engines and the Content Distribution Manager use a specific playback bandwidth when streaming media to user desktops. Although this bandwidth value can be changed, it is not possible to schedule changes to the playback bandwidth as it is with replication bandwidth.

The user has to specify the maximum bandwidth that each device can use to play back content to the user desktop. Each Content Engine has three playback servers: the WMT server, the HTTP server, and the RealServer. The user has to consider the content type and decide how to distribute maximum bandwidth among these three servers. For example, if the user has only the WMT content type, then the user should allocate 100 percent of the playback bandwidth to the WMT server and 0 percent to the HTTP server and the RealServer.

The Total playback field on the Devices Bandwidth screen is used to enter the maximum playback bandwidth. (See Figure 2-8.) Under this field are three more fields: WMT, HTTP, and Real. In these fields, the user can specify what percentage of the playback bandwidth is to be used for the WMT server, HTTP server, and RealServer, respectively.

On the left side of each field is a green or red circle that indicates whether that server is enabled or not on the device. For example, if the WMT field has a red circle, then the WMT server is not enabled on the device. If the Real field has a green circle, then the RealServer is enabled on the device. HTTP is always green because it cannot be disabled.

If a server is disabled, then its distributed bandwidth is 0. If a server is not disabled, then its associated field displays the current bandwidth distributed to that server as a percentage of total bandwidth. You can modify this field to change the bandwidth distribution.

If you do not update bandwidth settings, then default bandwidth settings are used. Default settings are:

- WMT—34 percent
- HTTP—33 percent
- Real—33 percent

Note Content Routers do not deliver media directly to users and thus do not require playback bandwidth settings. As a result, the bandwidth feature will be disabled for Content Routers.

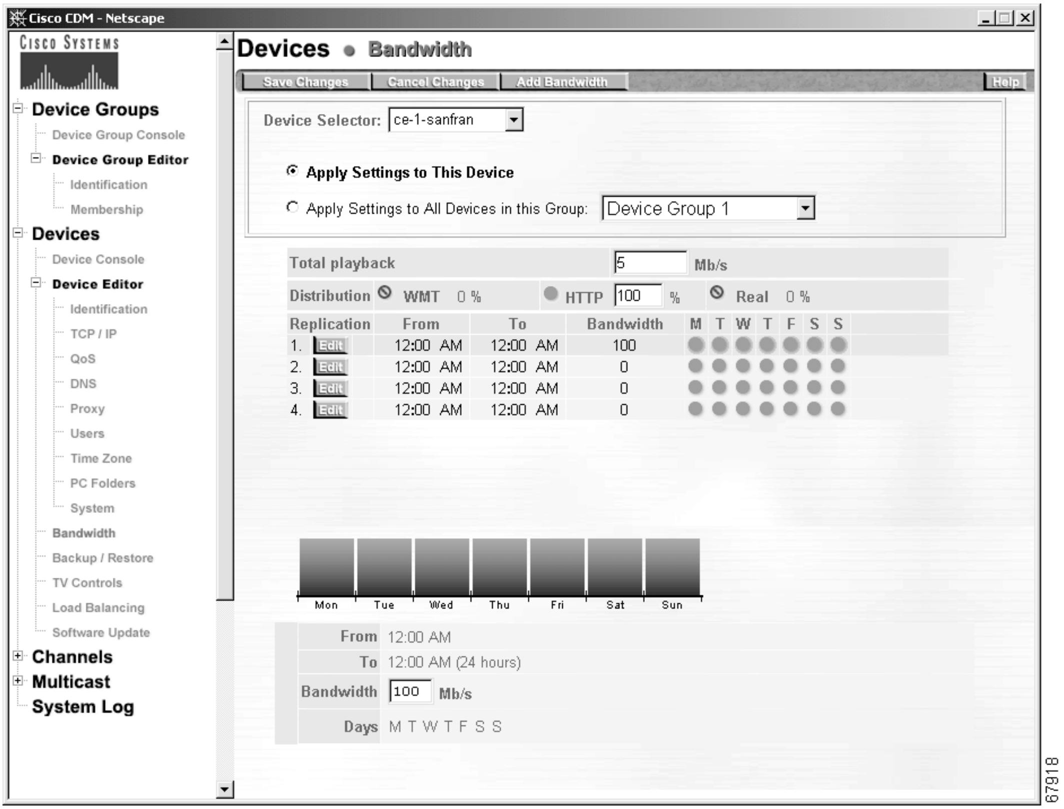
To set the playback bandwidth for a Content Engine or the Content Distribution Manager, perform the following steps:

Step 1 Choose **Devices > Bandwidth**. The Devices Bandwidth screen appears. (See Figure 2-8.)

Step 2 Make sure that the correct device is displayed in the Device Selector drop-down list.

Caution Use care when making bandwidth setting changes to an entire device group. Any unique bandwidth settings for an individual device within a group will be overridden by the group settings. You will need to reset unique settings for an individual device after completing settings for the group.

Figure 2-8 Devices Bandwidth Screen



Devices • Bandwidth

Device Selector: ce-1-sanfran

● Apply Settings to This Device

○ Apply Settings to All Devices in this Group: Device Group 1

Total playback 5 Mb/s

Distribution WMT 0 % HTTP 100 % Real 0 %

Replication		From	To	Bandwidth	M	T	W	T	F	S	S
1.	Edit	12:00 AM	12:00 AM	100	●	●	●	●	●	●	●
2.	Edit	12:00 AM	12:00 AM	0	●	●	●	●	●	●	●
3.	Edit	12:00 AM	12:00 AM	0	●	●	●	●	●	●	●
4.	Edit	12:00 AM	12:00 AM	0	●	●	●	●	●	●	●

From 12:00 AM

To 12:00 AM (24 hours)

Bandwidth 100 Mb/s

Days M T W T F S S

Step 3 In the Total playback field, enter a bandwidth value in megabits per second.

Step 4 In the Distribution field, enter a bandwidth distribution value (in percentage from 0 to 100) in the field next to the enabled server type. The total of the three values for WMT, HTTP, and Real should be 100 percent.

Note A server must be enabled (green circle) before you can set or change its bandwidth distribution.

Step 5 Perform one of the following actions:

- To apply bandwidth settings to the selected device, click the **Apply Settings to This Device** radio button.
- To apply the bandwidth settings to all devices within a specific device group, click the **Apply Settings to All Devices in this Group** radio button.

  Choose the desired device group from the drop-down list.

Step 6 Click **Save Changes** to store the new playback bandwidth setting for the selected device or device group.

Clicking **Cancel Changes** returns all values to their previous settings when you last clicked **Save Changes**.

Setting Replication Bandwidth

All E-CDN application devices ship with a default replication bandwidth. This bandwidth setting is enabled from 12:00 a.m. to 11:59 p.m. (24 hours) for each day of the week. Although the default replication bandwidth can be changed, its operating schedule cannot. Instead, you use the bandwidth feature to create additional replication settings to take effect at certain times during the week.

To add a replication bandwidth setting for moving media files over the network:

Step 1 Choose **Devices > Bandwidth**. The Devices Bandwidth screen appears. (See Figure 2-8.)

You can apply bandwidth settings to an individual device or to a device group.

Step 2 Perform one of the following actions:

- Apply bandwidth settings to the individual device displayed in the Device Selector field, click the **Apply Settings to This Device** radio button.
- Apply the bandwidth settings to all devices within a specific device group, click the **Apply Settings to All Devices in this Group** radio button.

Step 3 Choose the desired device group from the drop-down list.

Step 4 Click **Add Bandwidth**. A new screen appears.

A new bandwidth setting is added to the bottom of the bandwidth list, and options appear for configuring the new bandwidth setting.

Step 5 In the Bandwidth field, enter the replication bandwidth value for this setting in megabits per second.

Step 6 Above the Bandwidth field, set the time at which the device will begin to replicate media using this bandwidth by entering a time in the From field and clicking the **AM** radio button or the **PM** radio button.

Note Replication times are in local time for each device.

Alternatively, click the **24 hour** radio button or **9-5** radio button to set the interval from 12:00 a.m. to 11:59 p.m. (24 hours), or 9:00 a.m. to 5:00 p.m.

Step 7 Set the time at which the device will cease replicating media at this bandwidth by entering a time in the To field and clicking **AM** radio button or the **PM** radio button.

Note New time-of-day settings take precedence over previous settings if the intervals overlap.

Step 8 In the area beneath the Bandwidth field, check the appropriate **Days** check boxes to set which days of the week the device will use the replication bandwidth you are configuring.

You can click **All** to choose every day or click **None** to clear your selections.

Step 9 Click **Save Changes**. Clicking **Cancel Changes** returns all values to their previous settings when you last clicked **Save Changes**.

The screen refreshes, updating the replication bandwidth schedule for the device or device group.

The device replicates media at the bandwidth you set during the hours and on the days you specified. Remember that the device operates according to its local time zone. See the “Setting the Time Zone for a Device” section on page 2-9 for information on establishing time zones for your E-CDN application.

Removing Replication Bandwidth

To remove a replication bandwidth setting, perform the following steps:

Step 1 Choose **Devices > Bandwidth**. The Devices Bandwidth screen appears. (See Figure 2-8.)

Step 2 Choose the correct device from the Device Selector drop-down list.

Step 3 Perform one of the following actions:

- Click the **Apply Settings to This Device** radio button.
- Choose a device group and click the **Apply Settings to All Devices in This Group** radio button.

Step 4 Click **Edit** next to the interval setting that you want to remove.

Step 5 Click **Remove Bandwidth** at the top of the screen.

Editing Replication Bandwidth

To edit a replication bandwidth setting, perform the following steps:

Step 1 Choose **Devices > Bandwidth**. The Devices Bandwidth screen appears. (See Figure 2-8.)

Step 2 Perform one of the following actions:

- Choose the correct device from the Device Selector drop-down list and click the **Apply Settings to This Device** radio button.
- Choose a device group and click the **Apply Settings to All Devices in This Group** radio button.

Step 3 Click **Edit** next to the interval setting that you would like to change.

Step 4 Modify the playback and replication bandwidths, time intervals, or days of the week.

Step 5 Click **Save Changes**.

Enabling Load Balancing

You can use load balancing to enable optimal distribution of user requests for content over the Content Distribution Manager and Content Routers.

Note Load balancing can only be used if you have Content Routers on your network.

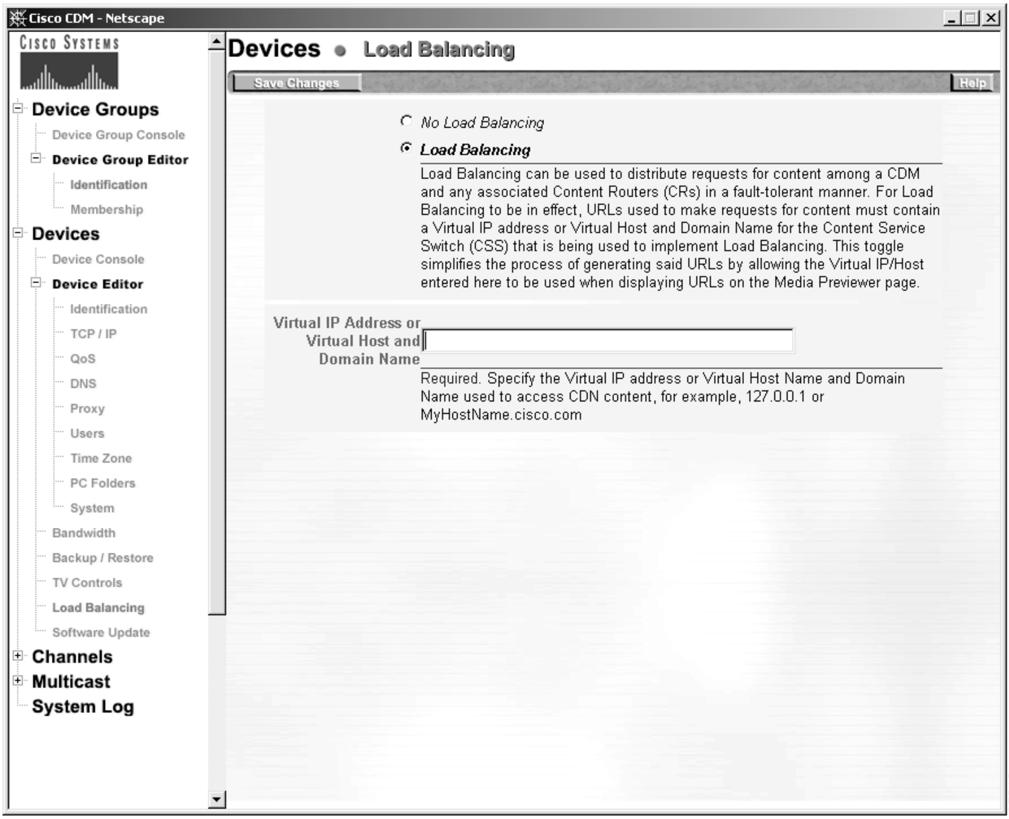
To enable load balancing, perform the following steps:

Step 1 Choose **Devices > Load Balancing**. The Devices Load Balancing screen appears. (See Figure 2-9.)

- If there are no Content Routers on your network, the **No Load Balancing** radio button is selected by default.
- If there are Content Routers on your network, then you need to click the **Load Balancing** radio button.

Step 2 You must first configure and add the Content Service Switch (CSS) 11000 that implements the load balancing.

Figure 2-9 Devices Load Balancing Screen



Devices ● Load Balancing

○ *No Load Balancing*

● ***Load Balancing***

Load Balancing can be used to distribute requests for content among a CDM and any associated Content Routers (CRs) in a fault-tolerant manner. For Load Balancing to be in effect, URLs used to make requests for content must contain a Virtual IP address or Virtual Host and Domain Name for the Content Service Switch (CSS) that is being used to implement Load Balancing. This toggle simplifies the process of generating said URLs by allowing the Virtual IP/Host entered here to be used when displaying URLs on the Media Previewer page.

Virtual IP Address or Virtual Host and Domain Name

Required. Specify the Virtual IP address or Virtual Host Name and Domain Name used to access CDN content, for example, 127.0.0.1 or MyHostName.cisco.com

Note For a sample CSS configuration, see Example 2-1. For more information about configuring a CSS 11000 switch, refer to the following Cisco Content Services Switch documentation on Cisco.com:
http://www.cisco.com/univercd/cc/td/doc/product/webscale/css/index.htm

Step 3 Enter a virtual IP address or a virtual host and domain name. This should be the same as the one specified in the "vip address" section in the CSS configuration. For load balancing to take effect, the URLs that request content must contain this virtual IP address, host name, and domain name so that the CSS 11000 switch is used to implement load balancing.

Step 4 Click **Save Changes**.

Sample CSS 11000 Switch Configuration for Load Balancing

Example 2-1 is a very basic CSS 11000 configuration for a virtual IP address that load balances between the Content Distribution Manager and Content Routers based on the least number of connections. The keepalive heartbeat is an HTTP request to /cgi/CSS-keepalive.

Example 2-1 CSS 11000 Switch Configuration Sample for Load Balancing

```
configure
ip route 0.0.0.0 0.0.0.0 10.0.2.1 1
circuit VLAN1
  ip address 10.0.2.254 255.255.255.0
service CDM
  ip address 10.0.2.55
  keepalive type http
  keepalive uri "/cgi/CSS-keepalive"
  active
service CR1
  ip address 10.0.2.56
  keepalive type http
  keepalive uri "/cgi/CSS-keepalive"
  active
owner foo.com
  content L3_LeastConnections
    vip address 10.0.2.50
    add service CDM
    add service CR1
    balance leastconn
    active
```

Setting the Time Used by CDN Devices

All devices on your CDN use time settings based on two factors:

- System time—This setting defines the date in MM/DD/YYYY format and time in HH:MM:SS format using a 24-hour clock for the Content Distribution Manager and all associated Content Engines and Content Routers.
- Time zone—This setting is configured for each device separately, allowing devices that are geographically dispersed to coordinate with one another and to apply the appropriate local time settings, based on the system time, when you change bandwidth settings or activate playlists. See the "Setting the Time Zone for a Device" section on page 2-9 for more information on setting the time zone for each of your CDN devices.

Configuring PC Folders

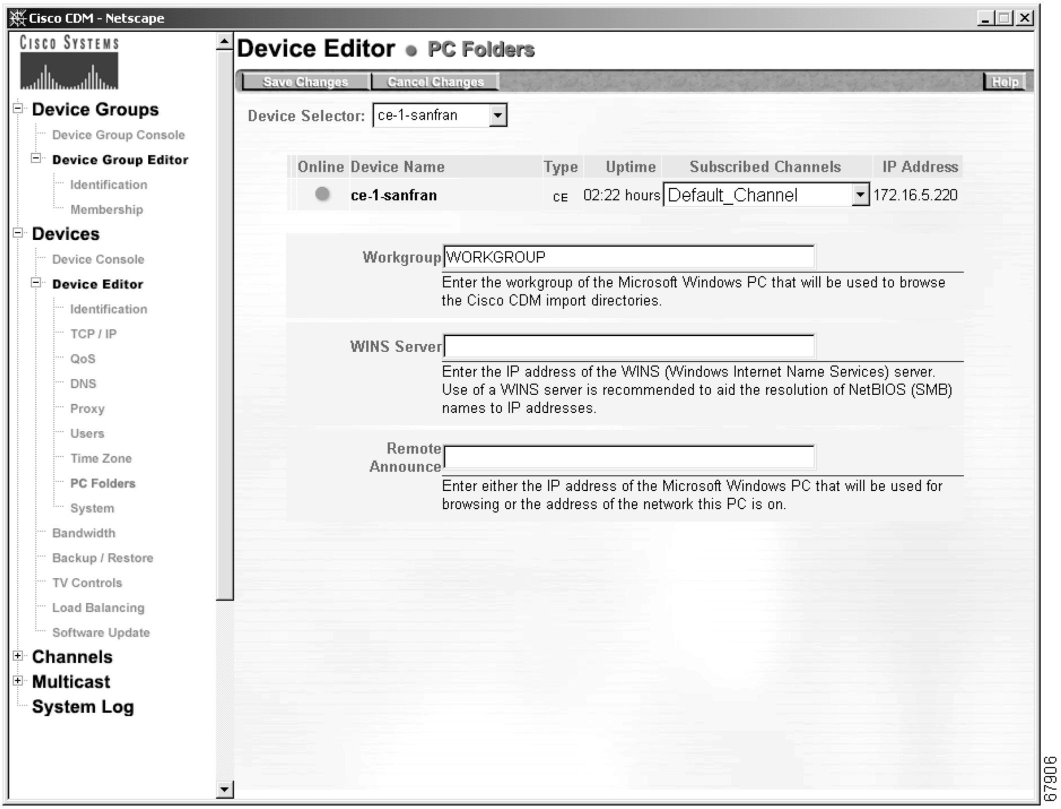
Use the PC folders option to configure your Content Distribution Manager so that it appears in your Network Neighborhood or My Network Places. This enables CDN administrators to browse the contents of the Content Distribution Manager channel-level import directories using Windows Explorer, as well as drag and drop files for import to particular channels.

Note Your office network must be running the Windows 95/98, Windows NT, or Windows 2000 operating system in order to use the PC folders option to import media files.

To configure PC folders, perform the following steps:

Step 1 Choose **Devices > Device Editor > PC Folders**. The Device Editor PC Folders screen appears. (See Figure 2-10.)

Figure 2-10 Device Editor PC Folders Screen



Device Selector: ce-1-sanfran

Online	Device Name	Type	Uptime	Subscribed Channels	IP Address
●	ce-1-sanfran	CE	02:22 hours	Default_Channel	172.16.5.220

Workgroup: WORKGROUP
Enter the workgroup of the Microsoft Windows PC that will be used to browse the Cisco CDM import directories.

WINS Server:
Enter the IP address of the WINS (Windows Internet Name Services) server. Use of a WINS server is recommended to aid the resolution of NetBIOS (SMB) names to IP addresses.

Remote Announce:
Enter either the IP address of the Microsoft Windows PC that will be used for browsing or the address of the network this PC is on.

Step 2 Choose the correct device from the Device Selector drop-down list. General information about the selected device is displayed.

Step 3 In the Workgroup field, enter the workgroup of the Microsoft Windows PCs that will be used to browse the Content Distribution Manager media import directories.

Step 4 In the WINS Server field, enter the IP address of the Windows Internet Naming Service (WINS) server.

Step 5 In the Remote Announce field, enter either the IP address of the PC that will be used for web browsing or the address of the network that the PC is on.

Step 6 Click **Save Changes**.

Adding, Removing, and Modifying Users

Users can be assigned either administrator-level or user-level privileges.

- Administrator-level privileges—Access to modify device attributes, add users, change user passwords, create channels, change channel sizes, subscribe channels to Content Engines, and view or preview all channels
- User-level privileges—Access to assigned channels to add and remove content, mark content for replication, and view or preview content

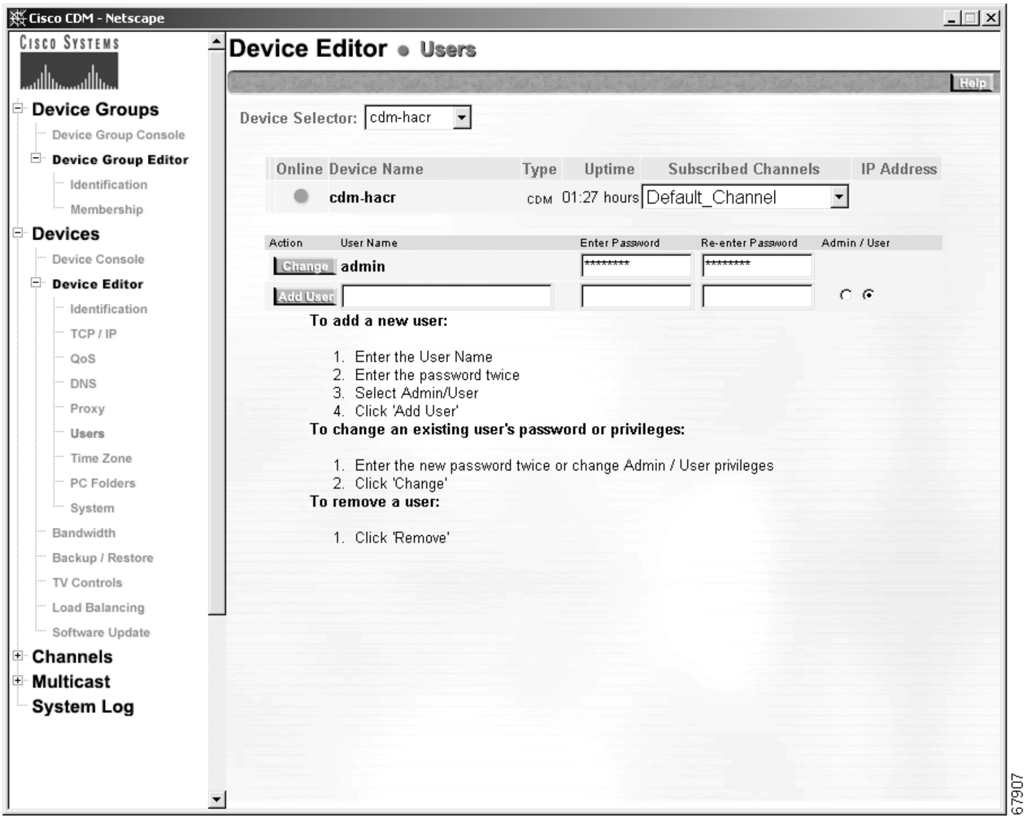
Adding a New User

Users are added through the Content Distribution Manager Users screen. To add a user, perform the following steps:

Step 1 Choose **Devices > Device Editor > Users**. The Device Editor Users screen appears. (See Figure 2-11.)

Step 2 Choose the Content Distribution Manager from the Device Selector drop-down list. Options for editing user accounts appear. Accounts are listed alphabetically.

Figure 2-11 Device Editor Users Screen



Device Editor • Users

Device Selector: cdm-hacr

Online	Device Name	Type	Uptime	Subscribed Channels	IP Address
●	cdm-hacr	CDM	01:27 hours	Default_Channel	

Action	User Name	Enter Password	Re-enter Password	Admin / User
Change	admin	*********	*********	
Add User				○ ●

To add a new user:

1. Enter the User Name
2. Enter the password twice
3. Select Admin/User
4. Click 'Add User'

To change an existing user's password or privileges:

1. Enter the new password twice or change Admin / User privileges
2. Click 'Change'

To remove a user:

1. Click 'Remove'

Step 3 Enter the new username in the field next to the Add User button.

Step 4 Enter a new password for the user in the Enter Password field.

Step 5 Enter the new password a second time in the Re-enter Password field.

Step 6 Click the **Admin** or **User** radio button to designate the access level of the account, and then click **Add User**. The new user is added to the user list.

Note The Content Distribution Manager users feature only allows users to access FTP and HTTP when the E-CDN application is running. This feature does not allow users to access a Telnet connection. Use the appropriate CLI command to access Telnet. For more information about CLI commands, refer to the *Cisco Application and Content Networking Software Command Reference.*

Removing a User

User accounts are removed using the Content Distribution Manager users feature.

Note It is not possible to remove the admin account, nor is it possible to remove the current user's account.

To remove a user, perform the following steps:

Step 1 Choose **Devices > Device Editor > Users**. The Device Editor Users screen appears. (See Figure 2-11.)

Step 2 Choose the Content Distribution Manager from the Device Selector drop-down list. Options for editing user accounts appear. Accounts are listed alphabetically.

Step 3 Locate the name of the user you wish to remove.

Step 4 Click **Remove** next to the username that you want to remove.

If you attempt to remove the current account (the account you used to log on), you are prompted to log on again using another administrator account before you are allowed to delete the account you were using.

Editing User Privileges

User privileges can be modified using the Content Distribution Manager Users feature. To change user privileges, perform the following steps:

Step 1 Choose **Devices > Device Editor > Users**. The Device Editor Users screen appears. (See Figure 2-11.)

Step 2 Choose the Content Distribution Manager from the Device Selector field. Options for editing user accounts appear. Accounts are listed alphabetically.

Step 3 Locate the account you wish to edit.

Step 4 Click the **Admin** or **User** radio button to change the designation of the account.

Step 5 Click **Change**.

Changing a User Password

You change the password of a user or administrator through the Content Distribution Manager users feature. Passwords can only be changed from the Content Distribution Manager user interface.

To change a user password, perform the following steps:

Step 1 Choose **Devices > Device Editor > Users**. The Device Editor Users screen appears. (See Figure 2-11.)

Step 2 Choose the Content Distribution Manager from the Device Selector drop-down list. Options for editing user accounts appear. Accounts are listed alphabetically.

Step 3 Locate the user or administrator account for which you wish to change passwords.

Step 4 Enter the new password in the Enter Password field.

Step 5 Enter the new password again in the Re-enter Password field.

Step 6 Click **Change**.

If the screen refreshes without error, you have successfully changed the password. If you encounter an error, see Appendix A, “Error Messages.”

Changing the Default Administrator Password

The E-CDN application system ships with a default administrator account already configured. This account, which uses the admin username, gives administrators full access to the Content Distribution Manager graphical user interface.

To access or edit the administrator account, perform the following steps:

Step 1 Choose **Devices > Device Editor > Users**. The Device Editor Users screen appears. (See Figure 2-11.)

Step 2 Choose the Content Distribution Manager from the Device Selector drop-down list. Options for editing user accounts appear. Accounts are listed alphabetically.

Step 3 Locate the admin account.

Step 4 Enter the new password in the Enter Password field.

Step 5 Enter the new password again in the Re-enter Password field.

Step 6 Click **Change**.

The Enter Network Password screen appears.

Step 7 Enter the *new* administrator password a third time in the Password field provided and click **OK**.

If the screen refreshes successfully, you have changed the password. If you encounter an error, see Appendix A, “Error Messages.”

Resetting the Default Administrator Password

Ordinarily, E-CDN application administrators change the default administrator account password (**admin**) in the same manner as any other account password. Refer to the *Cisco Content Delivery Networking Products Getting Started Guide* for details on changing passwords for accounts.

However, if you lose track of the password for the admin account and accidentally lock yourself out of the Content Distribution Manager administrative user interface, you must manually reset the password for the admin account before regaining access to the Content Distribution Manager and the Users feature.

Resetting the admin account password restores the factory-configured password to the account. After resetting this password and rebooting the Content Distribution Manager, administrators can again log on using the admin account and configure the password for the account, as well as for other user and administrative accounts.

Note In order to reset the password for the default administrator account, **admin**, you must have physical access to the Content Distribution Manager and have sufficient permissions to be able to log on to that device.

To reset your default administrator password, perform the following steps:

Step 1 Ask any users currently using the Content Distribution Manager to exit the system. In order to reset the default administrator password, you must reboot the Content Distribution Manager twice.

Step 2 Terminate any active Linux sessions by entering **exit** at the prompt.

Step 3 Reboot the Content Distribution Manager by powering the device off, and then on again.

Step 4 Wait for the following prompt:

```
LILO Boot:
```

Step 5 Log on to the Content Distribution Manager.

- If your CDN devices are using Cisco hardware, enter the following command to log on to the Content Distribution Manager as a single user, and then press **Enter**:

```
LILO Boot# linux single
```

- If your CDN devices are installed on hardware that was not manufactured by Cisco Systems, enter the following command to log on to the Content Distribution Manager as a single user, instead of the command listed above. Press **Enter** to initiate the logon.

```
LILO Boot# linux single console=tty0
```

Step 6 Enter the following path for the reset password script, resetpass, as follows at the bash# prompt:

```
bash# source /sonoma/sys/bin/resetpass
```

The script is executed, resetting the password for the admin account and rebooting the Content Distribution Manager. Once the Content Distribution Manager has completed its reboot, you can log on using the default administrator account by entering the username, **admin**, and the factory-configured password.

Managing Device Groups

The device groups feature lets E-CDN system administrators group individual devices by category in order to efficiently apply bandwidth settings across many devices at one time. Applying bandwidth settings to each device can be repetitive and tedious. Enabling the user to apply settings to multiple devices at one time reduces configuration and administration overhead.

You can apply bandwidth settings to the existing Default Device group (to which all devices initially belong by default) or you can create, name, and describe a new device group. After you decide whether to use the existing Default Device group or create a new device group, choose **Devices > Bandwidth** on the Content Distribution Manager to apply the bandwidth settings.

You can perform the following device group tasks:

- Create a device group.
- Name and describe a device group.
- Add and remove members from a device group.
- Remove a device group.

Creating a Device Group

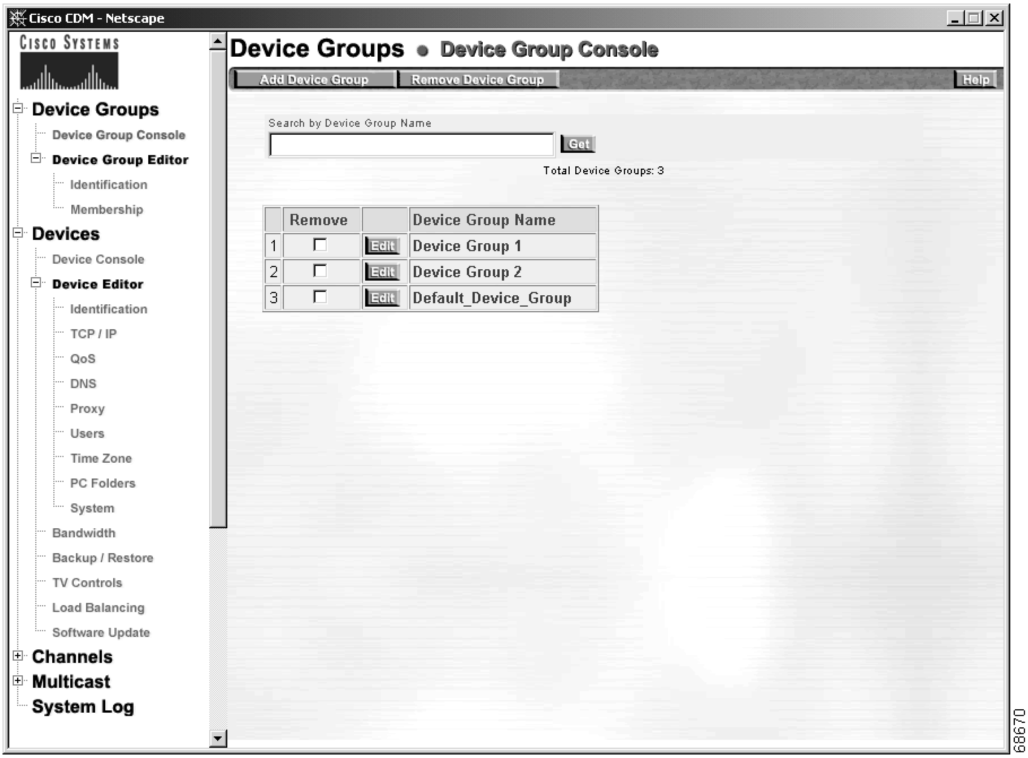
To add or create a new device group, perform the following steps:

Step 1 Choose **Device Groups > Device Group Console**. The Device Groups Device Group Console screen appears. (See Figure 2-12.)

Step 2 Click **Add Device Group** to add a new device group.

Step 3 To search for an existing device group, enter that device group name in the Search by Device Group Name field and click **Get**.

Figure 2-12 Device Groups Device Group Console Screen



Device Groups ● Device Group Console

Search by Device Group Name

Total Device Groups: 3

	Remove		Device Group Name
1	□	Edit	Device Group 1
2	□	Edit	Device Group 2
3	□	Edit	Default_Device_Group

Step 4 To edit a device group, click **Edit** next to the group that you want to edit. The Device Group Editor Identification screen appears. (See Figure 2-13.)

Step 5 To remove a device group, check the **Remove** check box next to the group that you want to remove and click **Remove Device Group**.

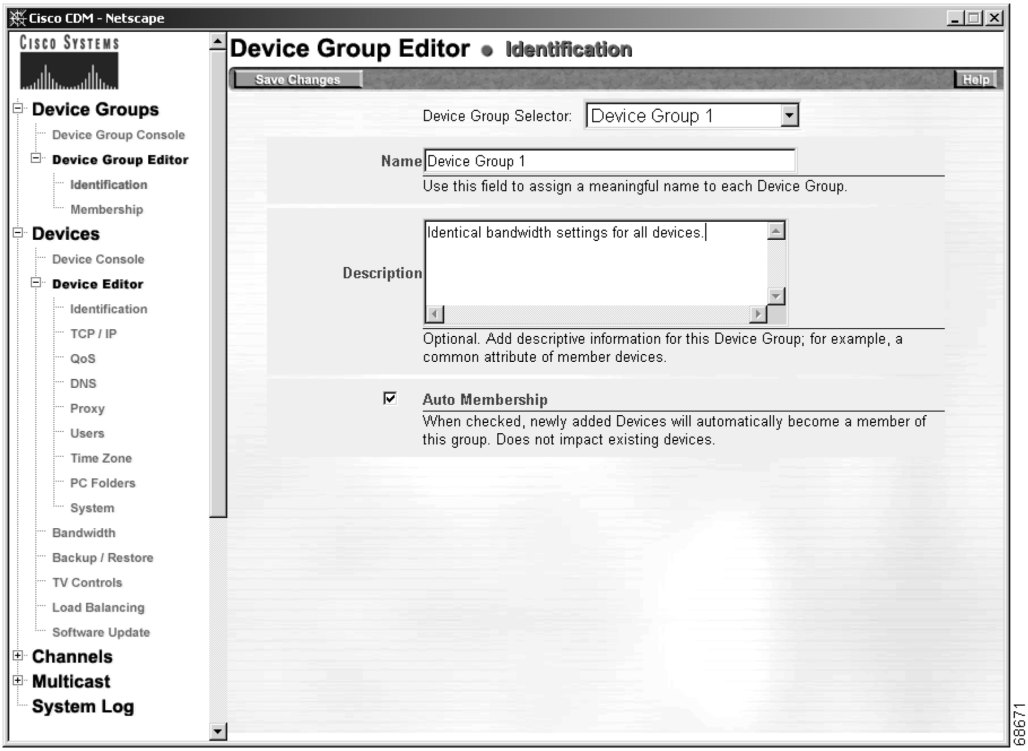
Note By default, all devices are members of the Default Device Group. Auto Membership (on the Identification screen) is enabled by default.

Naming and Describing a Device Group

To name and describe a device group, perform the following steps:

Step 1 Choose **Device Groups > Device Group Editor > Identification**. The Device Group Editor Identification screen appears. (See Figure 2-13.)

Figure 2-13 Device Group Editor Identification Screen



Device Group Editor ● Identification

Device Group Selector: Device Group 1

Name: Device Group 1
Use this field to assign a meaningful name to each Device Group.

Description: Identical bandwidth settings for all devices.
Optional. Add descriptive information for this Device Group; for example, a common attribute of member devices.

☑ Auto Membership
When checked, newly added Devices will automatically become a member of this group. Does not impact existing devices.

Step 2 Choose the device group whose name and description you want to edit from the Device Group Selector drop-down list.

Step 3 Enter a new name for this group in the Name field. Note that a device group name must be unique and cannot have the same name as an individual device.

Step 4 Enter a description of the group in the Description field.

Step 5 If desired, uncheck the **Auto Membership** check box if you do not want newly added devices to automatically become members of this group.

Step 6 Click **Save Changes** to save any changes.

Adding Members to a Device Group

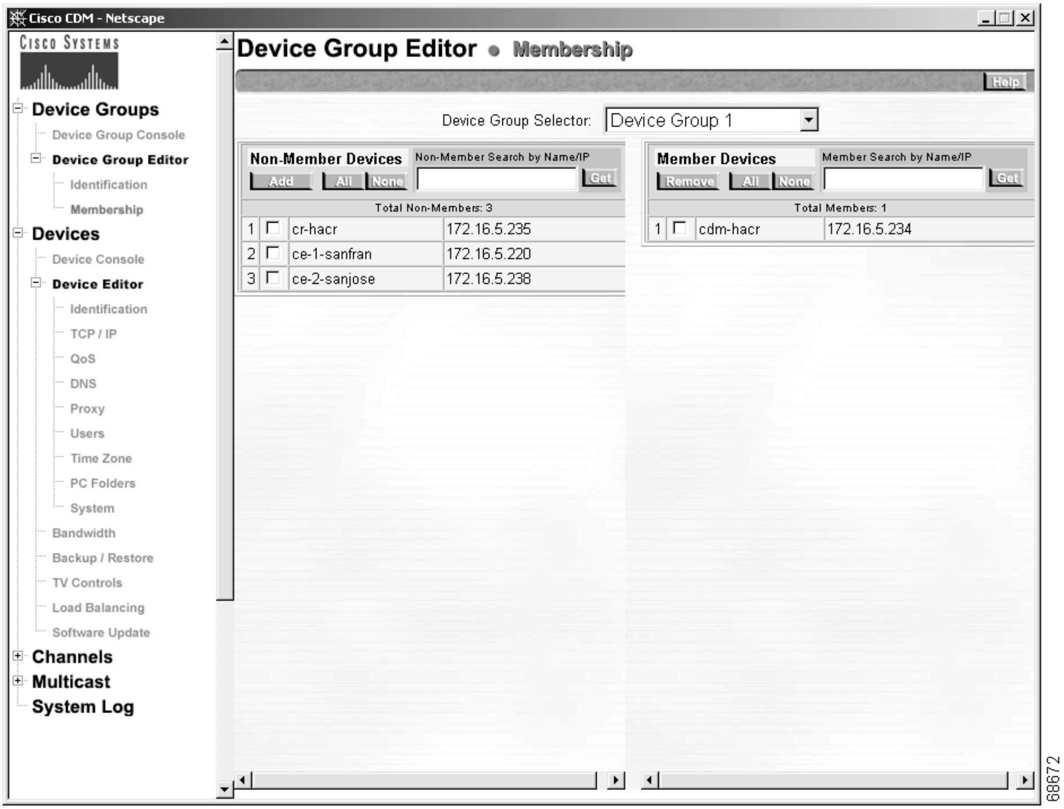
To add a device to the membership list of a group, perform the following steps:

Step 1 Choose **Device Groups > Device Group Editor > Membership**. The Device Group Editor Membership screen appears. (See Figure 2-14.) The left side of this screen lists all the nonmember devices, and the right side lists all devices that are members of this group.

Step 2 From the Device Group Selector drop-down list, choose the device group to which you want to add members.

Step 3 To find a device that does not appear on the Non-Member Devices list, enter the device in the Non-Member Search by Name/IP field and click **Get**. The device name is added to this list. You can then add it to the Member Devices list. Perform the same operation when looking for a device that is already a member. Enter its name in the Member Search by Name/IP field and click **Get**.

Figure 2-14 Device Group Editor Membership Screen



Device Group Selector: Device Group 1

Total Non-Members: 3

1	□	cr-hacr	172.16.5.235
2	□	ce-1-sanfran	172.16.5.220
3	□	ce-2-sanjose	172.16.5.238

Total Members: 1

1	□	cdm-hacr	172.16.5.234

Step 4 To add a nonmember device to the Member Devices list, check the check box next to the desired nonmember device and click **Add**. The device now appears in the Member Devices list.

Step 5 To remove any device from Member Devices list, check the check box next to the device that you want to remove and click **Remove**.

CHAPTER 3

Working with the Content Delivery Network

Through the Content Distribution Manager user interface, you have complete control over media distribution on your Enterprise CDN. This chapter provides information on the basic procedures that apply to working with the E-CDN application, including how to import media, how to preview and edit media, how to replicate and manage media, and how to play video directly to a TV monitor.

This chapter contains the following sections:

Creating Channels

Channels allow content to be organized into logical content groups. Once created, channels are subscribed to by Content Engines, which receive, store, and distribute the media imported to the channels.

Channels are created and reside on the Content Distribution Manager. It is not possible to create channels on Content Engines or Content Routers.

Adding a Channel

To add a channel, perform the following steps:

Step 1 Choose **Channels > Channel Console**. The Channels Channel Console screen appears.

Step 2 Click **Add Channel**.

A new channel with the default name "Channel#" is added to the Channel Console list.

To assign a name to the new channel, see the "Editing a Channel" section on page 3-3.

Removing a Channel

To remove a channel, perform the following steps:

Step 1 Choose **Channels > Channel Console**. The Channels Console screen appears.

Step 2 Check the **Remove** check box next to the channel that you want to remove.

Step 3 Click **Remove Channel**.

Editing a Channel

If you are unclear about the meaning of a channel setting, see Table 3-1.

Table 3-1 Channel Properties

Channel Property	Description
Name	Name of the channel. **Note** The following characters are considered illegal and cannot be used when naming a channel: @, #, %, $, ^, &, *, (), |, \""/, <> .
Description	Channel description.
Size Limit	Maximum amount of media a channel can hold in megabytes (MB) or gigabytes (GB).
Auto Subscribe	When checked, automatically subscribes any new Content Engines to the current channel. **Note** Enabling Auto Subscribe for a channel does not affect Content Engines or Content Routers that have already been added to the system.
Auto Replicate	When checked, automatically replicates new content to subscribed Content Engines. **Note** Enabling of Auto Replicate for a channel does affect the status of content items that have already been placed in that channel.
User	Assigns a user to the channel when the username is chosen from the user list.
Require SSL	Requires Secure Socket Layer (SSL) encryption when transferring media from the Content Distribution Manager to Content Engines or from Content Engine to Content Engine.
Is License	Not supported in ACNS 4.1 software.
Channel Icon	Shows path and filenames for the image in the E-CDN application Channel Previewer.

Table 3-1 Channel Properties (continued)

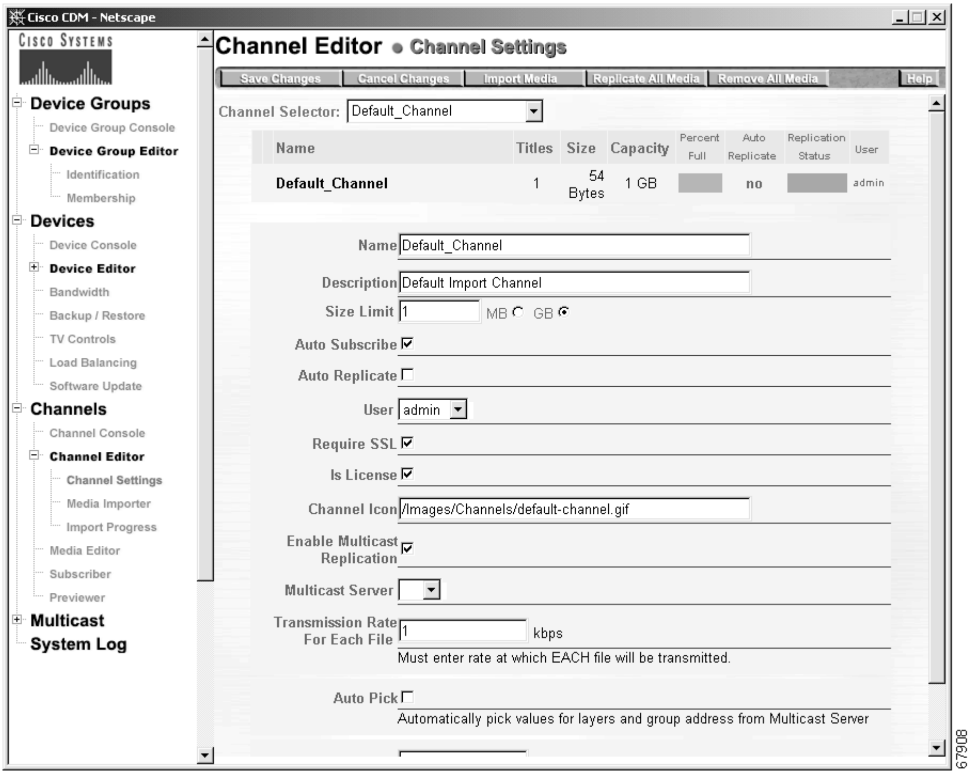
Channel Property	Description
Enable Multicast Replication	Enables Content Engines to replicate files on this channel through multicast, in addition to unicast replication.
Multicast Server	Name of the multicast server.
Transmission Rate For Each File	Sets rate, in kilobits per second, at which each file will be transmitted.
Auto Pick	Enables automatic selection of values for layers and group addresses from the multicast server.
Layers	Limits the total number of groups per channel.
Multicast Group Starting Address	Lowest value in the range of IP addresses representing the devices that are multicast-enabled.

To edit a channel, perform the following steps:

Step 1 Choose **Channels > Channel Console**. The Channels Channel Console screen appears.

Step 2 Click **Edit** next to the channel that you want to edit. The Channel Editor Channel Settings screen appears. (See Figure 3-1.)

Figure 3-1 Channel Editor Channel Settings Screen



Channel Editor ● Channel Settings

Channel Selector: Default_Channel

Name	Titles	Size	Capacity	Percent Full	Auto Replicate	Replication Status	User
Default_Channel	1	54 Bytes	1 GB		no		admin

Name: Default_Channel

Description: Default Import Channel

Size Limit: 1 MB ○ GB ●

Auto Subscribe ☑

Auto Replicate □

User: admin

Require SSL ☑

Is License ☑

Channel Icon: /Images/Channels/default-channel.gif

Enable Multicast Replication ☑

Multicast Server:

Transmission Rate For Each File: 1 kbps

Must enter rate at which EACH file will be transmitted.

Auto Pick □

Automatically pick values for layers and group address from Multicast Server

Step 3 Enter or modify the channel settings as required.

Step 4 Click **Save Changes**.

Enabling Multicasting

Note The multicast server referred to in the E-CDN application documentation is the Digital Fountain Server. Refer to the Digital Fountain documentation for procedures pertaining to the multicast server that cannot be performed through the Content Distribution Manager user interface.

The multicast feature enables you to distribute media efficiently by allowing different devices to receive a stream of media content simultaneously. This is done by setting up a multicast address to which different devices, configured to receive content from the same channel, can subscribe. The delivering device sends content to this multicast address, from which it becomes available to all subscribed receiving devices. Setting up channels that are multicast-enabled allows you to conserve bandwidth.

Adding a Multicast Server

To add a multicast server, perform the following steps:

Step 1 Choose **Multicast > Multicast Console**. The Multicast Console screen appears.

Step 2 Click **Add Multicast Server**.

A new entry for a multicast server appears.

See the next section, “Editing Multicast Server Settings,” to edit the settings of the new multicast server.

Editing Multicast Server Settings

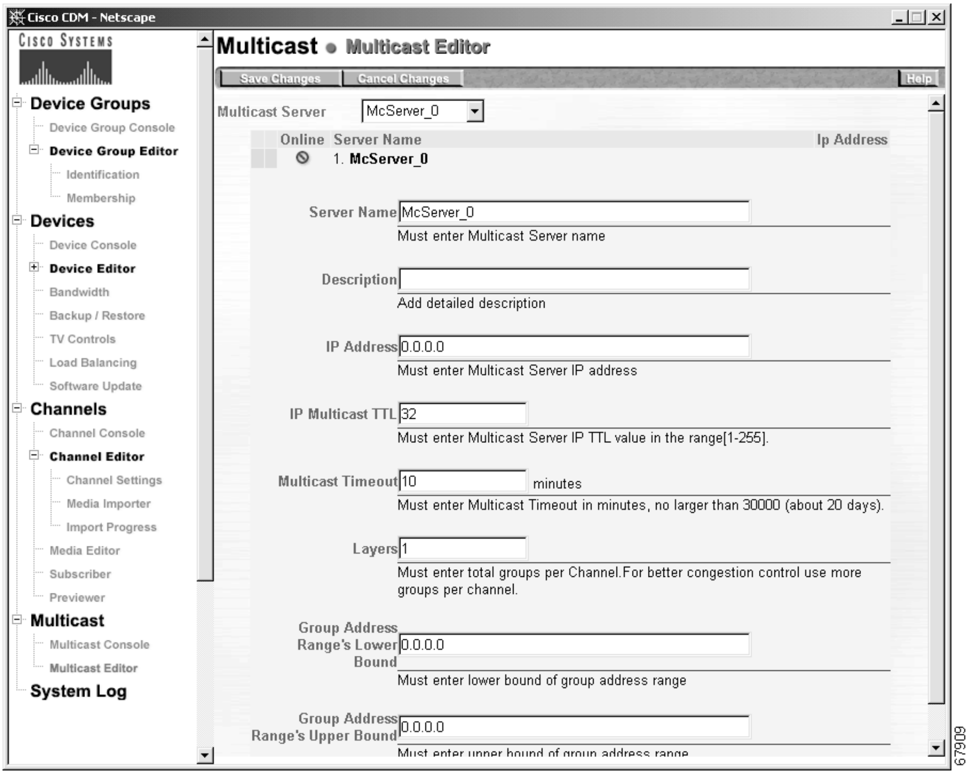
To edit the settings of a multicast server, perform the following steps:

Step 1 Click **Multicast Console** (if you are not already there).

Step 2 Click the **Edit** button next to the multicast server whose settings you want to edit. The Multicast Editor screen appears. (See Figure 3-2.)

Note When editing multicast server settings, make sure that you are working with the correct server. To ensure that you are editing the correct multicast server, always go to the Multicast Console first and proceed from there.

Figure 3-2 Multicast Editor Screen



Multicast Server: McServer_0

Online	Server Name	Ip Address
⦸	1. **McServer_0**	

Server Name: McServer_0
Must enter Multicast Server name

Description:
Add detailed description

IP Address: 0.0.0.0
Must enter Multicast Server IP address

IP Multicast TTL: 32
Must enter Multicast Server IP TTL value in the range[1-255].

Multicast Timeout: 10 minutes
Must enter Multicast Timeout in minutes, no larger than 30000 (about 20 days).

Layers: 1
Must enter total groups per Channel.For better congestion control use more groups per channel.

Group Address Range's Lower Bound: 0.0.0.0
Must enter lower bound of group address range

Group Address Range's Upper Bound: 0.0.0.0
Must enter upper bound of group address range

Step 3 Enter or modify the server settings as required.

Step 4 Click **Save Changes** to save the settings or click **Cancel Changes** to return to the default settings.

Removing a Multicast Server

To remove a multicast server, perform the following steps:

Step 1 Choose **Multicast > Multicast Console**. The Multicast Console screen appears.

Step 2 Check the **Remove** check box next to the multicast server that you want to remove.

Step 3 Click **Remove Multicast Server**.

Multicast Server Properties

Table 3-2 describes multicast server properties.

Table 3-2 Multicast Server Properties

Multicast Server Property	Description
Server Name	Name of the server.
Description	Description of the server.
IP Address	IP address assigned to the device.
IP Multicast TTL	Number of hops that IP packets are allowed to make from device to device. If a packet is not delivered within the maximum number of hops, it is discarded.
Multicast Timeout	Length of time that a Content Engine waits to start receiving multicast traffic. If it receives none within this time period, it reverts to unicast replication. The default is 10 minutes.
Layers	Total number of groups per channel. For better congestion control, use more groups per channel.

Table 3-2 Multicast Server Properties (continued)

Multicast Server Property	Description
Group Address Range's Lower Bound	Lowest value in the range of subscribed IP addresses. Valid address ranges are 224.0.1.0 through 238.255.255.255 (globally scoped), or 239.0.0.0 through 239.255.255.255 (limited scope).
Group Address Range's Upper Bound	Highest value in the range of subscribed IP addresses. Valid address ranges are 224.0.1.0 through 238.255.255.255 (globally scoped), or 239.0.0.0 through 239.255.255.255 (limited scope).

Subscribing a Content Engine to a Channel

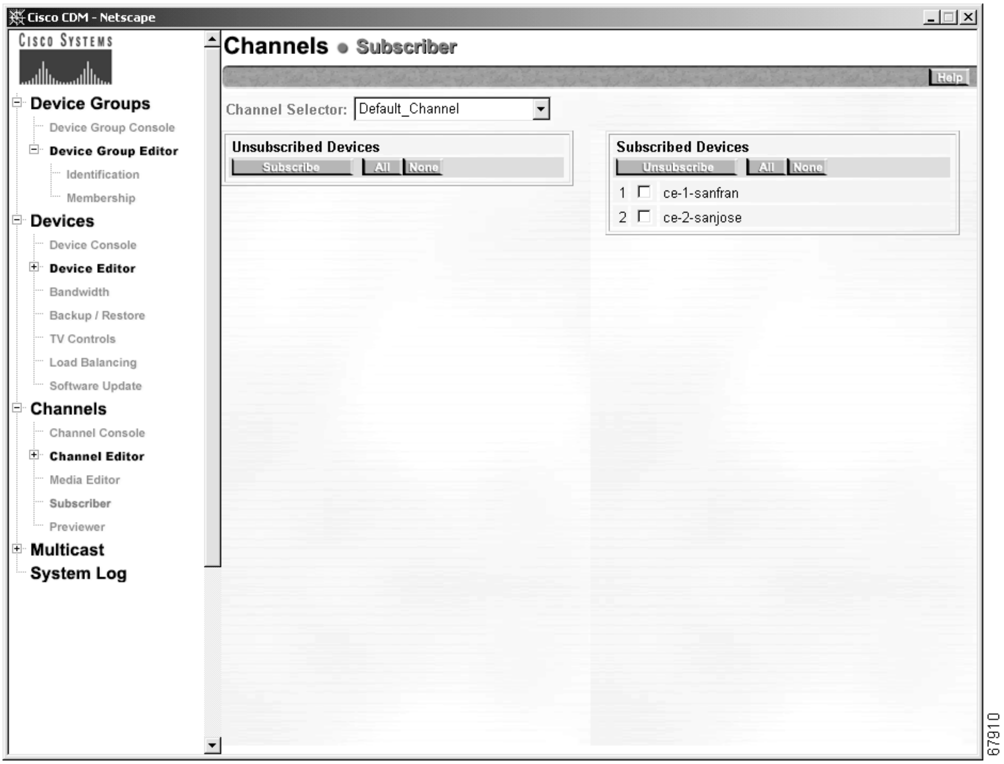
Once you have created a content channel, you subscribe Content Engines to the channel. By subscribing a Content Engine to a channel, you ensure that media files in that channel are replicated to the subscribed Content Engine and that users desiring the content in the channel can be served from the device.

Content Routers do not distribute content to users and, with the exception of the MANUAL_UPGRADE channel, are not subscribed to content channels.

To assign a Content Engine to a channel, perform the following steps:

Step 1 Choose **Channels > Subscriber**. The Channels Subscriber screen appears. (See Figure 3-3.)

Figure 3-3 Channels Subscriber Screen



Channel Selector: Default_Channel

Unsubscribed Devices

Subscribed Devices

1 □ ce-1-sanfran

2 □ ce-2-sanjose

Step 2 Make sure that the correct channel is displayed in the Channel Selector drop-down list. If it is not, choose the correct channel from the drop-down list.

Step 3 Under the heading Unsubscribed Devices, check the check box next to each available Content Engine that you want to subscribe, or click **All** to select all of the available Content Engines; click **None** to clear your selections.

Note Content Routers appear on the list of devices only when the selected channel is the MANUAL_UPGRADE channel. Content Routers cannot subscribe to content channels other than the MANUAL_UPGRADE channel.

Step 4 Click **Subscribe** to add the selected Content Engines to the list of those subscribed to the channel displayed in the Channel Selector drop-down list. Your selection is displayed in the list of subscribed Content Engines.

Removing a Content Engine from a Subscribed Devices List

To remove a Content Engine from the subscribed list, perform the following steps:

Step 1 Choose **Channels > Subscriber**. The Channels Subscriber screen appears. (See Figure 3-3.)

Step 2 Make sure that the correct channel is displayed in the Channel Selector drop-down list. If it is not, choose the correct channel from the drop-down list.

Step 3 Under the heading Subscribed Devices, check the check box next to each Content Engine that you want to remove, or click **All** to choose all Content Engines on the list; click **None** to clear your selections.

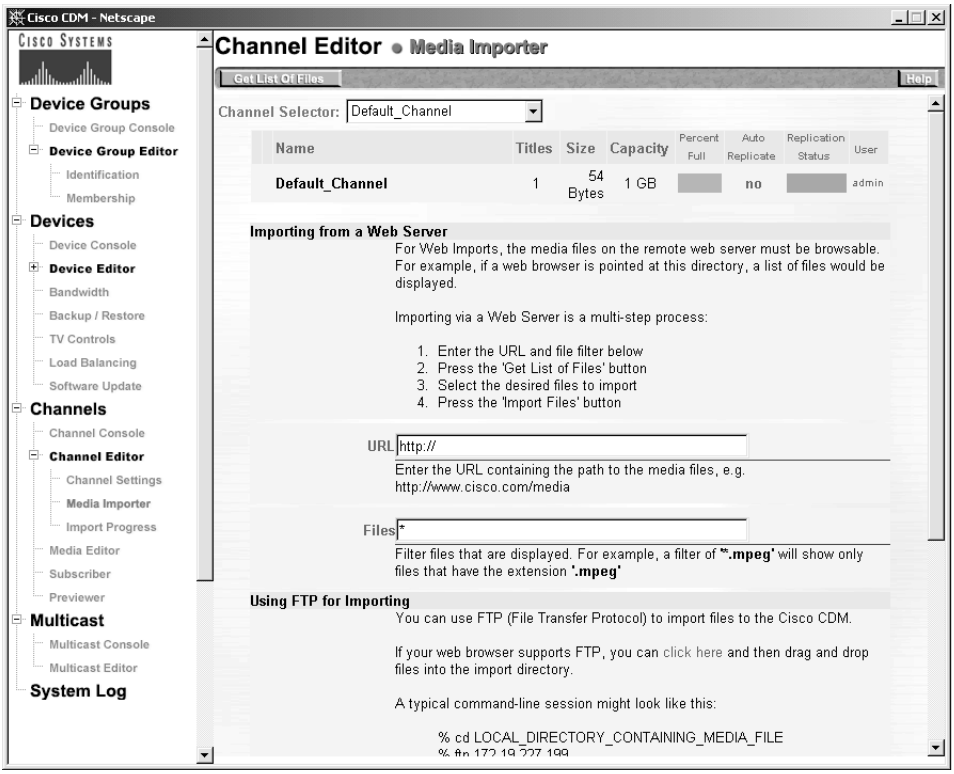
Step 4 Click **Unsubscribe**.

The Content Engine is removed from the list of Content Engines subscribed to the selected channel and moved back to the Unsubscribed Devices list.

Importing Media

The process of importing new media to your E-CDN application is simple. New media files and folders are copied to a predetermined channel directory. Channel directories are named to correspond to the channel they represent, and are located within the Import directory on your Content Distribution Manager. (See Figure 3-4.)

Figure 3-4 Channel Editor Media Importer Screen



Channel Editor ● Media Importer

Channel Selector: Default_Channel

Name	Titles	Size	Capacity	Percent Full	Auto Replicate	Replication Status	User
Default_Channel	1	54 Bytes	1 GB		no		admin

Importing from a Web Server

For Web Imports, the media files on the remote web server must be browsable. For example, if a web browser is pointed at this directory, a list of files would be displayed.

Importing via a Web Server is a multi-step process:

1. Enter the URL and file filter below
2. Press the 'Get List of Files' button
3. Select the desired files to import
4. Press the 'Import Files' button

URL: http://

Enter the URL containing the path to the media files, e.g. http://www.cisco.com/media

Files: *

Filter files that are displayed. For example, a filter of **'*.mpeg'** will show only files that have the extension **'.mpeg'**

Using FTP for Importing

You can use FTP (File Transfer Protocol) to import files to the Cisco CDM.

If your web browser supports FTP, you can click here and then drag and drop files into the import directory.

A typical command-line session might look like this:

```
        % cd LOCAL_DIRECTORY_CONTAINING_MEDIA_FILE
        % ftp 172.19.227.199
```

Periodically, the Content Distribution Manager polls the Import directory. Media files placed in channel directories since the Content Distribution Manager's last polling are marked for import to the appropriate Content Distribution Manager channel. Once they are marked for import, the status of these media files can be viewed using the Import Progress option accessible from the Channels menu.

Once you have imported a file, you can preview the transferred file using the Previewer option on the Channels menu.

There are a number of ways to transfer media to your Content Distribution Manager for import to the E-CDN application. The approved methods for transferring media files and folders are:

- FTP
- Drag and drop (PC folders feature)
- Web server
- Programmatic transfer using the remoteCmd program

Importing Directories to the Content Distribution Manager

When preparing your Content Distribution Manager to import media files that rely on nested directories of supporting files, all directory structures and supporting files must be copied to, or re-created in, the appropriate channel directory on the Content Distribution Manager. This ensures that during import, the Content Distribution Manager properly imports and stores both the media file and any supporting files required for proper playback.

Note Following import, all directories you created remain in the channel directory. These can either be left in place or deleted without affecting playback of the imported media.

For example, if you are importing a Synchronized Multimedia Integration Language (SMIL) media file called myfile.smi, the home directory of the files might contain the media file (myfile.smi) at the root level as well as one or more nested folders containing sound, text, and video. Your channel directory must re-create this structure exactly.

Using FTP to Import Files and Directories

You can use FTP to copy or move files and file directories to the designated channel directory within your Content Distribution Manager Import directory.

Before you transfer files and directories for import using FTP, you need to know the following:

- IP address or DNS name of your Content Distribution Manager machine
- Administrative login and password for your Content Distribution Manager machine
- Name of the channel to which your files will be imported

To move or copy files using FTP, perform the following steps:

Step 1 Begin by locating the local or network directory that contains the media files and directories that you wish to import.

Step 2 Connect to your Content Distribution Manager.

Note If you are using a dedicated FTP application, create a new profile and fill in the Content Distribution Manager connection information, including the IP address, administrative username, and password. If your FTP application permits, enter **/import** as the initial directory.

For example:

```
ftp://ftp.mycompany.com
%ftp 192.168.1.5
```

Step 3 When prompted, log on to your Content Distribution Manager using your administrative username and password.

Step 4 Navigate to the Import directory on your Content Distribution Manager and then to the channel directory for the channel into which you will be importing your media files. For example:

```
ftp> cd import
ftp> cd channel_directory
```

Step 5 If you are importing media that relies on nested directories for playback (such as SMIL files or Macromedia Director files), re-create the directory structure used by the files within your channel directory. You can accomplish this using your FTP client’s “new folder” feature or you can create a folder manually, for example:

```
%mkd /import/channel_folder_name/new_folder_name
```

Step 6 Before transferring media files to your channel directory, verify that you are in "binary transfer" mode rather than ASCII. Many FTP applications use an "auto-detect" feature to determine how to send files. However, if you are provided with transfer options, make sure the "binary" option is selected, or manually type the command:

```
ftp> binary
```

Step 7 Copy media files from their original location to the channel-specific Import directory on your Content Distribution Manager machine. If the media files you copied rely on nested directories, make sure that you have accurately re-created the nested directory structure in your channel import directory and that all dependent files are also copied to the appropriate subdirectory in your channel's Import directory.

Once you have copied media to your channel directory, wait for the Content Distribution Manager to detect the files and then begin the import process. You can view the progress of file imports by launching the Content Distribution Manager and choosing **Channels > Channel Editor > Import Progress**.

Using Drag and Drop to Import Files and Directories

If your workstation is running Microsoft Windows and you can see the Content Distribution Manager device in the Windows Network Neighborhood or My Network Places, you can transfer files to the appropriate channel directory for import simply by dragging and dropping them using Windows Explorer. Files placed in a channel directory in this manner will automatically be imported to the appropriate Content Distribution Manager channel.

Note You must be using Microsoft Windows to drag and drop a file with Windows Explorer, and you must log on to the Content Distribution Manager using a CDN administrator account with the same login name as the account used to access your corporate LAN. This will enable you to access the Import directory when prompted.

To drag and drop media files to your import folder, perform the following steps:

Step 1 Choose **Channels > Channel Editor > Media Importer**.

The instructions for importing media appear.

Under the heading "Using PC Folders for Importing," locate the name of the Content Distribution Manager machine on your network. The name appears in the format CISCO-[xxxx], where [xxxx] refers to the last four characters of the MAC address of the machine.

Step 2 Use Windows Explorer to navigate to the local or network directory containing the media files and directories that you wish to import.

Step 3 Choose the media files and any nested directories that you wish to import.

Step 4 Copy or cut the files you wish to import from their current location.

Step 5 Use Windows Explorer to locate the Content Distribution Manager machine on your LAN and navigate to the \import*channel_name* directory, where *channel_name* is the name of the channel to which you will be importing your media files. If you are prompted to log in, enter the username and password for the CDN administrator account. Remember that the administrative username must match your network login in order to gain access to the import directory.

Step 6 Paste the files you cut or copied into the channel-specific import directory. Verify that all files you wish to import were copied. If you are importing directories, make sure that the full directory structure was copied along with its content.

Step 7 Once you have copied media to your channels import directory, wait for the Content Distribution Manager to detect the files and then begin the import process. You can view the progress of file imports by launching the Content Distribution Manager and choosing **Channels > Channel Editor > Import Progress**.

Using a Web Server to Import Files

From the Media Importer screen, you can copy media files from a web server on the Internet. You must be able to browse and get a directory listing of the media files through the web server.

Note It is not possible to import directories to the Content Distribution Manager using the Importing from a Web Server option in the Media Importer.

To access the Media Importer and initiate a web server transfer, perform the following steps:

Step 1 Choose **Channels > Channel Editor > Media Importer**. The Channel Editor Media Importer screen appears. (See Figure 3-4.)

Step 2 Make sure that the correct channel is displayed in the Channel Selector drop-down list. If it is not, choose the correct channel from the drop-down list. Some general information about the selected channel is displayed.

Step 3 In the URL field, enter the URL containing the path to the media files.

Step 4 In the Files field, specify the name or type of files that you want to import. What you enter here is used to build a list of files from which you select files to import.

Choose all media files by using the asterisk (*) in the Files field, or enter a filter for file types. For example, *.mpg will return all MPEG files in the directory you specified.

Step 5 Click the **Get List of Files** button.

A list of files matching the criteria you entered in the Files field appears.

Step 6 Choose the files you want to import, and then click **Import Files**.

Step 7 Choose **Channels > Channel Editor > Import Progress** to follow the file transfer progress. See the “Monitoring Progress” section on page 3-21 for more detailed information.

Importing Files Programmatically

In addition to the methods for importing media files outlined above, it is possible to edit channel content programmatically using simple scripts and HTML commands passed to a Common Gateway Interface (CGI) program named remoteCmd.

In order to take advantage of this feature, you must have the remoteCmd program installed on the machine serving as your Content Distribution Manager, and you must observe the syntax guidelines explained in the following sections when sending requests to the program.

When requests are received by the remoteCmd program, the program calls the web-based CDN import mechanism to handle the media.

Adding New Media to a Channel Programmatically

Use the following syntax when creating an add-new-media request to programmatically place content in a channel import directory for upload to your Content Distribution Manager.

```
http://<Content_Distribution_Manager>/cgi-bin/remoteCmd?OP=CONTENT&CMD=
IMPORT&CHANNEL-NAME=<mychannel>&URL=<media_file_URL>
```

- Content_Distribution_Manager—Replace this with the DNS name or numeric IP address of the Content Distribution Manager hosting the channel to which you will be uploading new content.
- mychannel—Replace this with the name of the Content Distribution Manager content channel to which the new media file will be imported.
- media_file_URL—Replace this with the web location and full filename of the media file that is being imported, for example:

  ```
  http://www.anywho.com/training/intro.mpg
  ```

Removing Media from a Channel Programmatically

The procedure for removing content from a channel using the remoteCmd program is similar to that for adding new media to a channel.

Use the following syntax when creating a remove-media request:

```
http://<Content_Distribution_Manager>/cgi-bin/remoteCmd?OP=CONTENT&CMD=
REMOVE&CHANNEL-NAME=<mychannel>&FILENAME=<media_file_name>
```

- Content_Distribution_Manager—Replace this with the DNS name or numeric IP address of the Content Distribution Manager hosting the channel from which you will be deleting content.
- mychannel—Replace this with the name of the Content Distribution Manager content channel from which the media file will be deleted.

- media_file_name—Replace this with the name of the file to delete from the channel you named.
  - If the file is at the root level of the channel directory on the Content Distribution Manager machine, the filename with extension is required, for example, intro.mpg.
  - If the file is located in a recursive directory or nested in a directory, the full path name is required, for example:

    ```
    &FILENAME=/foo/bar/intro.mpg
    ```

For instructions on evaluating the status of your remove-media request after it has been sent, see the next section, "Evaluating the Status of Your Add or Remove Request."

Evaluating the Status of Your Add or Remove Request

User requests to add media to a channel or remove media from a channel will result in either a success or an error message. The result of each request you make is captured in a STATUS field and can be displayed in one of three formats:

- JavaScript (JS)—Default display format. Status information is presented using JavaScript.
- HTML (HTML)—Status information is embedded within HTML tags.
- E-CDN application (MX)—Proprietary format makes it easy to parse information.

To display the status of your request, add the following statement at the end of your request URL, where *format* is replaced by one of the three format abbreviations outlined above:

```
&DISPLAY=format
```

For example, a sample remove request asking for results displayed using JavaScript might read:

```
http://<CDM_Address>/cgi-bin/remoteCmd?OP=CONTENT&CMD=REMOVE&CHANNEL-NAME=<mychannel>&FILE
NAME=<media_file_name>&DISPLAY=JS
```

The following message is returned if the request has been posted without error:

```
Status_Success
```

If an error is encountered, the error condition is returned in the STATUS field, along with other error message text.

Monitoring Progress

To monitor the progress of a file transfer, perform the following steps:

Step 1 Choose **Channels > Channel Editor > Import Progress**. The Channel Editor Import Progress screen appears.

Step 2 Status files are automatically updated every 10 seconds. Clicking **Cancel Import** cancels imports currently in progress.

Previewing Imported Media

You use the Content Distribution Manager Previewer option to preview your imported media before distributing these files throughout the CDN.

By clicking the thumbnail image representing a media file, you can play the file from your Content Distribution Manager to verify correct media content and quality before replicating the media file.

After replicating a media file, you can also play the file from a Content Engine. By clicking a thumbnail image or the CE Play link, media is streamed directly from the Content Engine using your preferred media server, for example, the RealMedia or Windows Media servers.

For RealServer playback, a RealServer G2 on the Content Engine streams the media. The RealServer G2 combined with the RealPlayer client on the desktop for playback provides the additional ability to fast-forward and rewind the file while viewing. Similarly, for Windows Media playback, the Windows Media Server running on the Content Engine combines with the Windows Media Player client to deliver viewing and playback options.

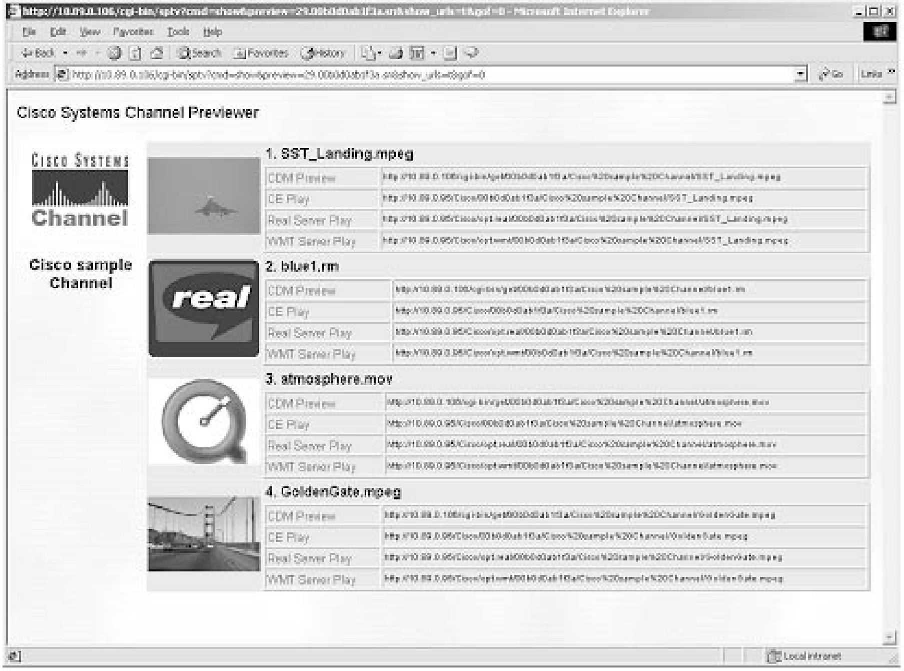
Previewing Media Before Replication

To access the Previewer and preview media directly from the Content Distribution Manager, perform the following steps:

Step 1 Choose **Channels > Previewer**. The Channels Previewer screen appears, listing your E-CDN application channels.

Step 2 Click a channel icon to view the media files of the selected channel in a separate window. (See Figure 3-5.)

Figure 3-5 Channels Previewer Screen



http://10.89.0.106/cgi-bin/sptv?cmd=show&preview=29.00b0d0ab1f3a.sn&show_urls=t&gof=0 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://10.89.0.106/cgi-bin/sptv?cmd=show&preview=29.00b0d0ab1f3a.sn&show_urls=t&gof=0
Go Links
Cisco Systems
Channel
Cisco sample Channel
real
Local intranet
55198

Cisco Systems Channel Previewer

1. SST_Landing.mpeg

CDM Preview	http://10.89.0.106/cgi-bin/get/00b0d0ab1f3a/Cisco%20sample%20Channel/SST_Landing.mpeg
CE Play	http://10.89.0.95/Cisco/00b0d0ab1f3a/Cisco%20sample%20Channel/SST_Landing.mpeg
Real Server Play	http://10.89.0.95/Cisco/opt.real/00b0d0ab1f3a/Cisco%20sample%20Channel/SST_Landing.mpeg
WMT Server Play	http://10.89.0.95/Cisco/opt.wmt/00b0d0ab1f3a/Cisco%20sample%20Channel/SST_Landing.mpeg

2. blue1.rm

CDM Preview	http://10.89.0.106/cgi-bin/get/00b0d0ab1f3a/Cisco%20sample%20Channel/blue1.rm
CE Play	http://10.89.0.95/Cisco/00b0d0ab1f3a/Cisco%20sample%20Channel/blue1.rm
Real Server Play	http://10.89.0.95/Cisco/opt.real/00b0d0ab1f3a/Cisco%20sample%20Channel/blue1.rm
WMT Server Play	http://10.89.0.95/Cisco/opt.wmt/00b0d0ab1f3a/Cisco%20sample%20Channel/blue1.rm

3. atmosphere.mov

CDM Preview	http://10.89.0.106/cgi-bin/get/00b0d0ab1f3a/Cisco%20sample%20Channel/atmosphere.mov
CE Play	http://10.89.0.95/Cisco/00b0d0ab1f3a/Cisco%20sample%20Channel/atmosphere.mov
Real Server Play	http://10.89.0.95/Cisco/opt.real/00b0d0ab1f3a/Cisco%20sample%20Channel/atmosphere.mov
WMT Server Play	http://10.89.0.95/Cisco/opt.wmt/00b0d0ab1f3a/Cisco%20sample%20Channel/atmosphere.mov

4. GoldenGate.mpeg

CDM Preview	http://10.89.0.106/cgi-bin/get/00b0d0ab1f3a/Cisco%20sample%20Channel/GoldenGate.mpeg
CE Play	http://10.89.0.95/Cisco/00b0d0ab1f3a/Cisco%20sample%20Channel/GoldenGate.mpeg
Real Server Play	http://10.89.0.95/Cisco/opt.real/00b0d0ab1f3a/Cisco%20sample%20Channel/GoldenGate.mpeg
WMT Server Play	http://10.89.0.95/Cisco/opt.wmt/00b0d0ab1f3a/Cisco%20sample%20Channel/GoldenGate.mpeg

Step 3 Locate the media file that you wish to preview and click the **CDM Preview** link next to the media thumbnail image.

You are prompted for your username and password.

Step 4 Enter this information and click **OK**.

Media begins to play on your workstation's designated media player.

If an error message appears, see Appendix A, "Error Messages."

Viewing Media After Replication

To view a media file after replication, perform the following steps:

Step 1 Choose **Channels > Previewer**. The Channels Previewer screen appears, listing your E-CDN application channels.

Step 2 Click a channel icon to view the list of media file thumbnail images for the selected channel.

Note In order to be able to test Content Engine, RealServer, or WMT Server playback, the IP address of the machine your browser is running on must be in the coverage zone of a Content Engine.

Step 3 A new window opens, displaying the media files in the selected channel. (See Figure 3-5.) Choose one of the four options for viewing media files:

- To play a media file after import but before replication from the Content Distribution Manager, click the **CDM Preview** link that appears next to the media file thumbnail image.
- To view the media file from the Content Engine after replication, click the **CE Play** link, or simply click the thumbnail image for the media file you wish to play.
- To view the media file from the Content Engine after replication using the RealServer, click the **RealServer Play** link.
- To view the media file from the Content Engine after replication using the Windows Media Server, click the **WMT Server Play** link.

The appropriate viewing client (for example, RealPlayer for RealServer, or the Windows Media Player for the WMT Server) opens. You may be prompted to enter your CDN username and password a second time before viewing the media file.

If an error message appears, see Appendix A, "Error Messages."

Editing Media

From the Channels Media Editor screen (see Figure 3-6), you can edit the data for your imported media before distributing these files throughout the Enterprise CDN. You can change media names, descriptions, bit rates, and thumbnail images; control media replication; and copy, move, and remove media files. See the "Replicating Media" section on page 3-30 for more information. Table 3-3 provides details on the media file properties that can be modified when you edit media.

Table 3-3 Media File Properties

Media Property	Description
Name	Name assigned to the media file.
Description	Description of the content of the media file.
Replicate	Indicates that the media file is marked for replication to a Content Engine.
Bit rate	Rate at which the media file will be streamed during playback in bits per second (bps). The default is 1.5 megabits per second.
Size	Size of the media file, in bytes.
Duration	Total length of the media file playback in h:mm:ss format.

Table 3-3 Media File Properties (continued)

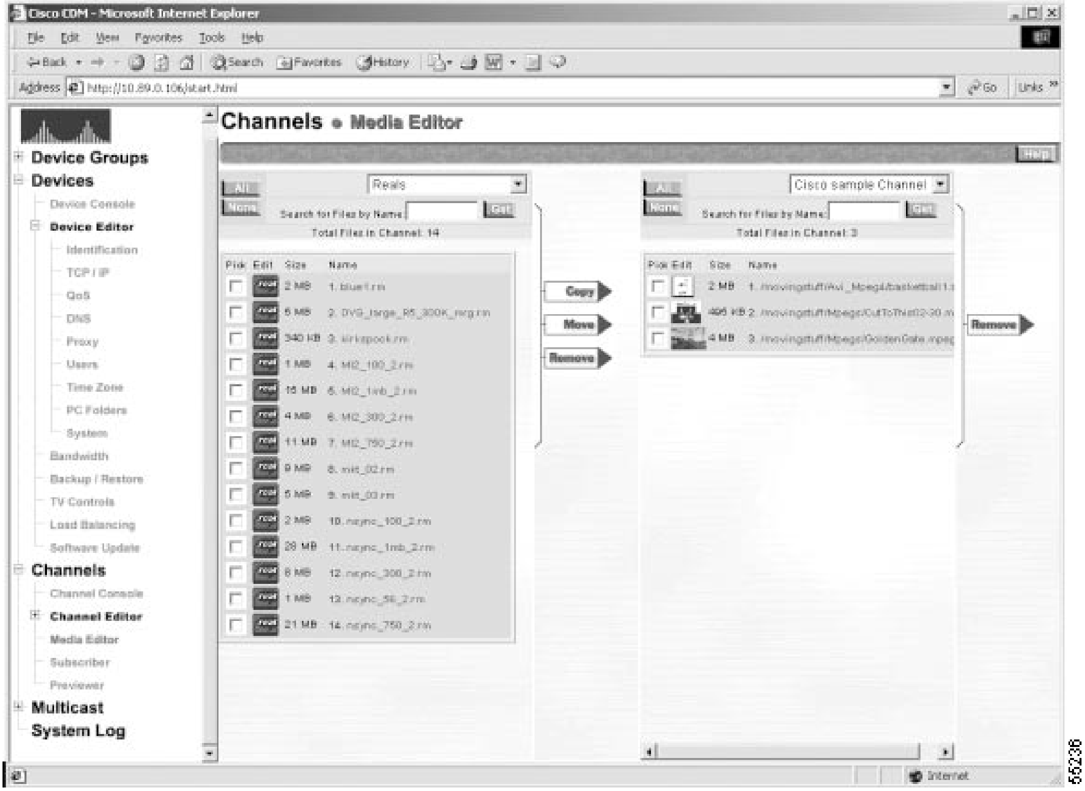
Media Property	Description
Thumbnail	Path and filename for the thumbnail image that represents the media file.
Custom HTML Error Pages	Path and filename for customized error pages: Coverage—Not in the coverage zone of a Content Engine. Content—Content not available on the Content Engine. The Content Engine could be offline. Publish—Content not yet available from the Content Distribution Manager. Bandwidth—Maximum bandwidth reached on the Content Engine.

Editing Media Files

To edit a media name and description, bit rate, or thumbnail, perform the following steps:

Step 1 Choose **Channels > Media Editor**. The Channels Media Editor screen appears. (See Figure 3-6.)

Figure 3-6 Channels Media Editor Screen



Total Files in Channel: 14

Pick	Edit	Size	Name
☐		2 MB	1. blue1.rm
☐		5 MB	2. DVG_large_R5_300K_nrg.rm
☐		340 KB	3. kirkspock.rm
☐		1 MB	4. MI2_100_2.rm
☐		15 MB	5. MI2_1mb_2.rm
☐		4 MB	6. MI2_300_2.rm
☐		11 MB	7. MI2_750_2.rm
☐		9 MB	8. mit_02.rm
☐		5 MB	9. mit_03.rm
☐		2 MB	10. nsync_100_2.rm
☐		28 MB	11. nsync_1mb_2.rm
☐		8 MB	12. nsync_300_2.rm
☐		1 MB	13. nsync_56_2.rm
☐		21 MB	14. nsync_750_2.rm

Total Files in Channel: 3

Pick	Edit	Size	Name
☐		2 MB	1. /movingstuff/Avi_Mpeg4/basketball1.a
☐		495 KB	2. /movingstuff/Mpegs/CutToThe02-20.m
☐		4 MB	3. /movingstuff/Mpegs/GoldenGate.mpeg

Step 2 To search for a file, enter the full or partial name of the file in the Search for Files by Name field. If using the Netscape browser, click **Get**. If using the Internet Explorer browser, click **Get** or press the **Enter** key.

Step 3 Click the **Edit** thumbnail image for the media file you want to change or edit. Fields for the media file's properties appear. (See Table 3-3.)

Step 4 Enter the new name, description, bit rate, or thumbnail.

Note Changing the name also changes the playback URL and invalidates existing web pages that use the old name.

Step 5 Click **Save Changes**.

Clicking **Cancel Changes** returns all values to their previous settings when you last clicked S**ave Changes**.

Copying Media Between Channels

To copy media from channel to channel, perform the following steps:

Step 1 Choose **Channels > Media Editor**. The Channels Media Editor screen appears. (See Figure 3-6.)

Step 2 From the drop-down list on the left, choose the channel from which you want to copy media.

Step 3 To search for a file, enter the full or partial name of the file in the Search for Files by Name field. If using the Netscape browser, click **Get**. If using the Internet Explorer browser, click **Get** or press the **Enter** key.

Step 4 Check the **Pick** check box next to each file that you want to copy.

Step 5 Click **All** to choose all of the files or **None** to clear your selections.

Step 6 From the drop-down list on the right, choose the channel into which you want to copy media.

Step 7 Click **Copy**.

Moving Media from One Channel to Another

To move media from channel to channel, perform the following steps:

Step 1 Choose **Channels > Media Editor**. The Channels Media Editor screen appears. (See Figure 3-6.)

Step 2 From the drop-down list on the left, choose the channel from which you want to move media.

Step 3 To search for a file, enter the full or partial name of the file in the Search for Files by Name field. If using the Netscape browser, click **Get**. If using the Internet Explorer browser, click **Get** or press the **Enter** key.

Step 4 Check the **Pick** check box next to each file that you want to move. Click **All** to choose all of the files or **None** to clear your selections.

Step 5 From the drop-down list on the right, choose the channel into which you want to copy media.

Step 6 Click **Move**.

Removing Media from a Channel

To remove media from a channel, perform the following steps:

Step 1 Choose **Channels > Media Editor**. The Channels Media Editor screen appears. (See Figure 3-6.)

Step 2 Make sure that the correct channel is displayed in the appropriate drop-down list box. If it is not, choose the correct channel from the list.

Step 3 To search for a file, enter the full or partial name of the file in the Search for Files by Name field. If using the Netscape browser, click **Get**. If using the Internet Explorer browser, click **Get** or press the **Enter** key.

Step 4 Check the **Pick** check box next to each file that you want to remove. Click **All** to select all of the files or **None** to clear your selections.

Step 5 Click **Remove**. You are prompted to confirm that you want to remove the selected media.

Defining Custom HTML Error Pages

For any given media file, the Content Distribution Manager administrator has the ability to define custom HTML error pages for the following error conditions:

- Media file is not in a coverage zone (Coverage)

Note A coverage zone is the area that a Content Engine is authorized to serve based upon IP address, typically the local portion of your intranet or subnet.

- Content not available from the Content Distribution Manager (Publish)
- Content not available on the Content Engine (Content)
- Content Engine maximum bandwidth limit reached (Bandwidth)

Before defining custom HTML error messages for the above conditions, create the HTML pages that will be displayed.

To select a file for each of the above conditions, performing the following steps:

Step 1 Choose **Channels > Media Editor**. The Channels Media Editor screen appears. (See Figure 3-6.)

Step 2 Make sure that the correct channel is displayed in the drop-down list. If it is not, choose the correct channel from the drop-down list.

Step 3 Click **Edit** for the file you want to edit.

Fields displaying the media file properties are displayed.

See Table 3-3for a description of each option.

Step 4 Go to the section labeled Custom HTML Error Pages and enter the necessary alternative URL in the text fields provided.

Replicating Media

Using a process called replication, the Content Distribution Manager distributes media to each Content Engine in the network. Once accessed in the Media Editor, individual media files can be replicated from the Content Distribution Manager to a selected Content Engine device.

Note To mark content within a channel for replication, the Content Engine must be subscribed to the channel.

Replicating Selected Media Files from a Channel

To replicate individual media files from a CDN channel to subscribed Content Engines, perform the following steps:

Step 1 Choose **Channels > Channel Editor > Media Editor**. The Channel Editor Media Editor screen appears. (See Figure 3-6.)

Step 2 Make sure that the correct channel is displayed in the appropriate drop-down list. If it is not, choose the correct channel from the drop-down list.

Step 3 Click the **Edit** thumbnail image for the file you want to edit.

Fields displaying the media file properties are displayed.

See Table 3-3 for a description of each option.

Step 4 Check the **Replicate** check box.

Step 5 Click **Save Changes**.

Clicking **Cancel Changes** returns all values to their previous settings when you last clicked **Save Changes**.

The selected file is replicated to all Content Engines subscribed to that channel.

Replicating All Media Files from a Channel

To replicate all media currently in a channel to subscribed Content Engines, perform the following steps:

Step 1 Choose **Channels > Channel Editor > Channel Settings**. The Channel Editor Channel Settings screen appears. (See Figure 3-1.)

Step 2 Make sure that the correct channel is displayed in the Channel Selector field. If it is not, choose the correct channel from the drop-down list.

Some general information about the selected channel is displayed.

Step 3 Click **Replicate All Media**.

How Special Characters Are Handled in Filenames

When the Content Distribution Manager replicates files to the Content Engines, filenames that contain special characters may be altered. Some special characters are removed from the filename; others are replaced with different characters. Table 3-4 summarizes how special characters in filenames are handled during replication.

If a filename does not contain an extension and all the characters in the filename are removed, the file is renamed “content.” For example, a file named **&** would be renamed *content*, but a file named *&.txt* would be renamed *.txt*.

Table 3-4 Special Characters in Filenames

Special Character	Is Removed	Is Replaced with	Is Unchanged
Ampersand [&]	•		
Asterisk [*]	•		
At sign [@]	•		
Backquote [`]	•		
Backslash [\ ]	•		
Caret [^]	•		
Closing brace [}]	•		
Closing bracket [ ]]	•		
Closing parenthesis [ )]	•		
Colon [:]	•		
Comma [,]	•		
Dash [-]			•
Dollar sign [$]	•		
Double-quote ["]	•		
Equal sign [=]	•		
Exclamation point [!]	•		
Forward slash [/]	•		
Greater than [>]	•		
Less than [<]	•		
Opening brace [{]	•		
Opening bracket [[ ]	•		
Opening parenthesis [( ]	•		
Percent sign [%]	•		
Period [.]			•
Plus sign [+]	•		
Pound sign [#]	•		

Table 3-4 Special Characters in Filenames (continued)

Special Character	Is Removed	Is Replaced with	Is Unchanged
Question mark [?]	•		
Semicolon [;]	•		
Single-quote [']	•		
Space [ ]		Underscore [_]	
Tilde [~]	•		
Underscore [_]			•
Vertical-bar [l]	•		

Removing Media from a Content Engine

Note These instructions allow you to only remove content from the subscribed Content Engine on this channel. Content from the Content Distribution Manager is not removed. To remove content from the Content Distribution Manager, see the "Removing Media from a Channel" section.

To remove all media currently in a channel from a subscribed Content Engine, perform the following steps:

Step 1 Choose **Channels > Channel Editor > Channel Settings**. The Channel Editor Channel Settings screen appears. (See Figure 3-1.)

Step 2 Make sure that the correct channel is displayed in the Channel Selector field. If it is not, choose the correct channel from the drop-down list.

Some general information about the selected channel is displayed.

Step 3 Click **Remove All Media**.

You are prompted to confirm your decision to remove all media files from this channel.

Step 4 Click **OK**.

Linking to Media from Web Pages

Once you have successfully imported media files to the channels established on the Content Distribution Manager, you are ready to link that content to your website or corporate LAN.

Note To import media files to the Content Distribution Manager, choose **Channels > Channel > Editor Import Media**. See the "Importing Media" section on page 3-13 for more information.

To embed CDN media URLs in web pages, perform the following steps:

Step 1 Choose **Channels > Previewer**. The Channels Previewer screen appears, listing the channels on the Content Distribution Manager.

Step 2 Click a channel thumbnail image to view the media files that have been added to that channel.

A separate browser window opens, listing all media files subscribed to that channel.

Step 3 Choose the desired URL that appears to the right of the filename for the media.

Step 4 Right-click and choose **Copy**. Alternatively, right-click the **Content Distribution Manager Preview** hypertext link for the media file, and choose the **Copy Shortcut** option from the menu that appears.

Step 5 With the URL for the media copied to your clipboard, open the HTML editor used to maintain your web pages.

Step 6 Locate the position on the web page where you wish the link to the CDN media to appear.

Step 7 Create a new HTML anchor link at the proper location that points to the CDN media. Your link should be in the format:

```
<A HREF=”URL”>image_or_text_file_name</A>
```

where “URL” is the URL you copied from the Channel Previewer and *image_or_text_file_name* is the content the user clicks to activate the CDN media link.

Step 8 Paste the URL you copied into the tag so that the link points to the CDN media. Then save the changes you made to the web page and post the page to the Internet or your intranet.

Playing Video Directly to a TV Monitor

Content Engines equipped with an integrated Moving Picture Experts Group 1 (MPEG-1) decoder can play media files using National Television Standards Committee (NTSC) or Phase Alternation Line (PAL) video signals. This enables the Content Engine to play video directly to a TV monitor in applications such as kiosks, cable TV systems, and video walls. Playback is controlled from any web browser and has VCR-like controls, including the ability to create looping playlists.

Note To use the video-out feature, you must have a device with an integrated MPEG decoder card.

Configuring Content Engines for NTSC or PAL Video Output

Content Engines can be configured to output video using either the NTSC or PAL standard.

To designate the video format that will be used when delivering content from a Content Engine to a video device, perform the following steps:

Step 1 Choose **Devices > Device Editor > Time Zone**. The Device Editor Time Zone screen appears.

Step 2 Choose the name of the Content Engine that you wish to modify from the Device Selector drop-down list.

Step 3 Click **Video Type** and choose the correct video output format for the device you are using. Your options are NTSC or PAL. NTSC is the default.

Note The Video Type field is only displayed if the device has a video-out (TV-out) card.

Step 4 Click **Save Changes**.

Building a Media Playlist for the TV Controller

Playlists enable you to pull together series of media files from different channels and play them in a defined order on any video-out enabled device.

To access the TV controller from the Content Distribution Manager user interface and add media to a playlist, perform the following steps:

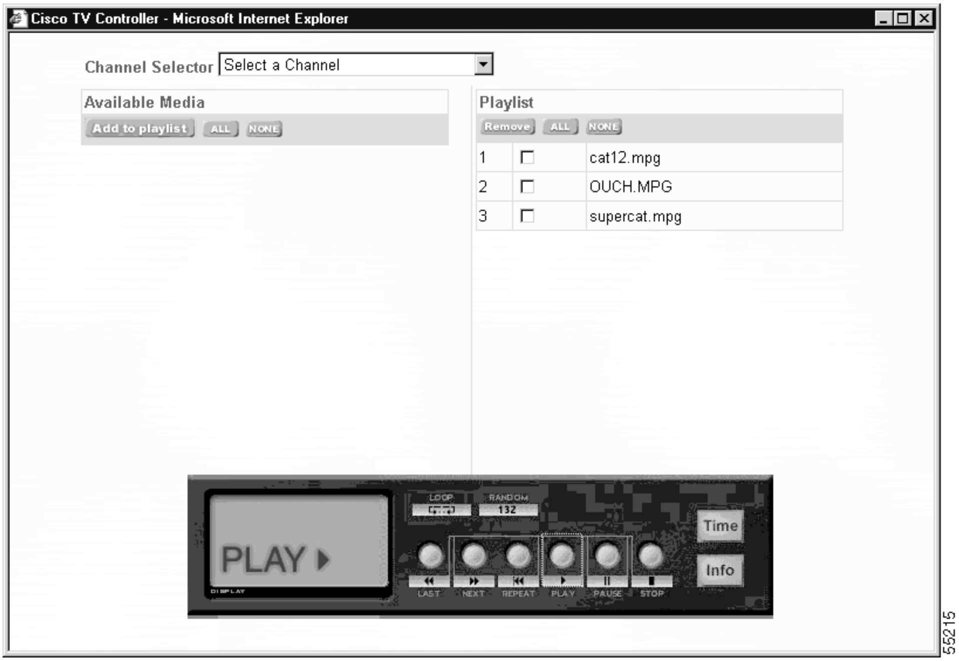
Step 1 Choose **Devices > TV Controls**. The TV Controls screen appears.

Step 2 Click the name of the Content Engine that you want to access. Each Content Engine name is a link.

Step 3 Enter your username and password.

The Content Distribution Manager TV controller appears in a separate window. (See Figure 3-7.)

Figure 3-7 TV Controller Screen



Cisco TV Controller - Microsoft Internet Explorer

Channel Selector: Select a Channel

Available Media

Playlist

1	□	cat12.mpg
2	□	OUCH.MPG
3	□	supercat.mpg

Step 4 Make sure that the correct channel is displayed in the Channel Selector drop-down list. If it is not, choose the correct channel from the drop-down list.

Step 5 Under the heading Available Media, check the check box next to each available media file that you want to add to the playlist. Click **All** to choose all of the files or **None** to clear the selections.

Step 6 Click **Add to playlist**.

Step 7 To add media from another channel to the playlist, click the **Channel Selector** drop-down list and choose a different channel, and then repeat Step 5 through Step 6.

Once you have created your playlist, click the PLAY button on the TV controller to play the media files on the playlist. Use the NEXT, LAST, and REPEAT buttons to move from file to file within the playlist.

See the next section, "Setting the Start and Stop Times for Media Playlists," for information on setting a schedule for your media playlist.

Setting the Start and Stop Times for Media Playlists

To access the playlist time controls and set a schedule of dates on which to play back your media playlist, perform the following steps:

Step 1 Follow the instructions in the "Building a Media Playlist for the TV Controller" section on page 3-36 to access the TV Controller screen and create a media playlist.

Step 2 Once you have created your playlist, click the **Time** button on the TV controller console. The playlist time list appears and, below it, controls for scheduling playback times.

Step 3 In the time controls, place the cursor in the Month field in the row labeled Start time and enter the number of the month on which the scheduled media playback begins.

Step 4 Press the **Tab** key to move the cursor forward, and enter the remaining playback information.

All information must be in numeric format, though it is not necessary to use leading zeros. Click the **AM** or **PM** button to indicate what time of day you wish the playlist to start. For example, a Start time of 6:20 p.m. on October 5, 2000 would appear as:

```
MonthDayYearHourMinuteAMPM
1052000620__X
```

Step 5 Repeat Step 3 and Step 4 for the row labeled Stop time to set the time at which the playlist will discontinue playback.

Step 6 Click **Save Changes** to add the start time and stop time you specified to the playlist time list. The times will appear on the list at the top of the TV Controller screen.

Clicking **Cancel Changes** resets the start time and stop time without adding any new playback times to the playlist time list.

Modifying Playlist Playback Times

Playlist playback times cannot be edited once they are created. To modify a playlist playback time, delete the time setting you wish to change and add a new setting with the correct times specified.

To modify the playlist time list, perform the following steps:

Step 1 With the playlist time list displayed, check the check box next to the playback time setting that you want to change. Click **ALL** to choose all playback time settings on the playlist time list, or **NONE** to clear any time settings that have already been chosen.

Step 2 With your time settings selected, click **Remove** to remove the time settings from the playlist time list. Click **Remove All** to delete all time settings from the playlist time list regardless of whether they are selected or not.

Step 3 You are prompted to confirm your decision to remove playback time settings. Click **OK** to confirm your choice or **Cancel** to return to the TV Controls screen without removing any time settings.

Step 4 See the "Building a Media Playlist for the TV Controller" section on page 3-36 to create a time setting on your playlist with the correct start time and stop time.

Removing Media from a Playlist Using the TV Controller

To access the TV controller from the Content Distribution Manager and remove media from a playlist, perform the following steps:

Step 1 Choose **Devices > TV Controls**. The TV Controls screen appears.

Step 2 Choose a Content Engine name. If multiple TV out-enabled Content Engines are available, make sure to choose the correct Content Engine.

The Content Distribution Manager TV controller appears. (See Figure 3-7.)

Step 3 Make sure that the correct channel is displayed in the Channel Selector drop-down list. If it is not, choose the correct channel from the drop-down list.

Step 4 Under the heading Playlist, check the check box next to each playlist file that you want to remove from the playlist. Click **All** to choose all of the files or **None** to clear your selections.

Step 5 Click **Remove**.

Playing Media on TV-Out Enabled Devices

Once you have created a media playlist using the TV controller, you can play the list of media at any time or schedule playback to occur on specific days and at predetermined times.

To display media from your playlist on a TV-out enabled device, perform the following steps:

Step 1 Follow the instructions in the "Building a Media Playlist for the TV Controller" section on page 3-36 to access the TV Controls screen and create a media playlist.

Step 2 Using the TV controller console, click the **Play** button. If you want the TV controller to loop through the playlist without stopping, click the **LOOP** button on the console.

The TV controller display changes to indicate that the looping feature is enabled. While the looping feature is enabled, the TV controller plays all media files on the playlist in succession. Click the **LOOP** button a second time to toggle off the looping feature.

Step 3 To prevent a media file from being played, check the box next to the filename on the playlist and click **Remove**. The file is removed from the playlist.

Viewing Information About a Media File That Is Playing

To view information about a video that is playing, perform the following steps:

Step 1 Follow the instructions in the "Playing Media on TV-Out Enabled Devices" section on page 3-40 to launch the TV controller from the Content Distribution Manager user interface and play media subscribed to a channel.

Step 2 With a media file from the playlist playing, click **Info** on the TV controller. You will see information on the file that is currently playing appear on the TV Controls screen.

Using Overlay Images with Playlists

This section describes how to perform the following tasks using the TV controller:

- Adding an Overlay Image to a Playlist Using the TV Controller
- Changing the Parameters of a Playlist Overlay Image Using the TV Controller

You can associate one overlay image with each playlist. The end user sees this image displayed in a determinable screen location when the playlist it is associated with is playing. This feature is useful for displaying logos.

Note Overlay images can only be Windows bitmap files with 16 colors. They must have 4 bits per pixel and must be less than 64 KB in size. The width of the image (in pixels) must be divisible by 8. Before associating an overlay image with a playlist, open the image file in an image editor and view its properties to make sure that it meets the above requirements.

Adding an Overlay Image to a Playlist Using the TV Controller

You must first create a playlist to be able to associate an overlay image with it. For instructions on how to create a playlist using the TV controller, see the "Adding Programs to the Playlist" section on page 3-46.

To add an overlay image from the Content Distribution Manager, perform the following steps:

Step 1 Choose **Devices > TV Controls**. (See Figure 3-8.)

Step 2 Click the TV-out enabled device that has the playlist to which you want to add an overlay image.

Step 3 If prompted, enter a username and password and click **OK**.

Step 4 From the Channel Selector drop-down list, choose the channel that contains the image file you wish to use as an overlay image. A list of available media appears on the left.

Step 5 Check the check box next to the image file that you want to use as an overlay image.

Step 6 Click the **Add Overlay** button. The names of the image file and the channel from which it is obtained appear under the heading Overlay Image, which appears under the list of files with the heading Playlist.

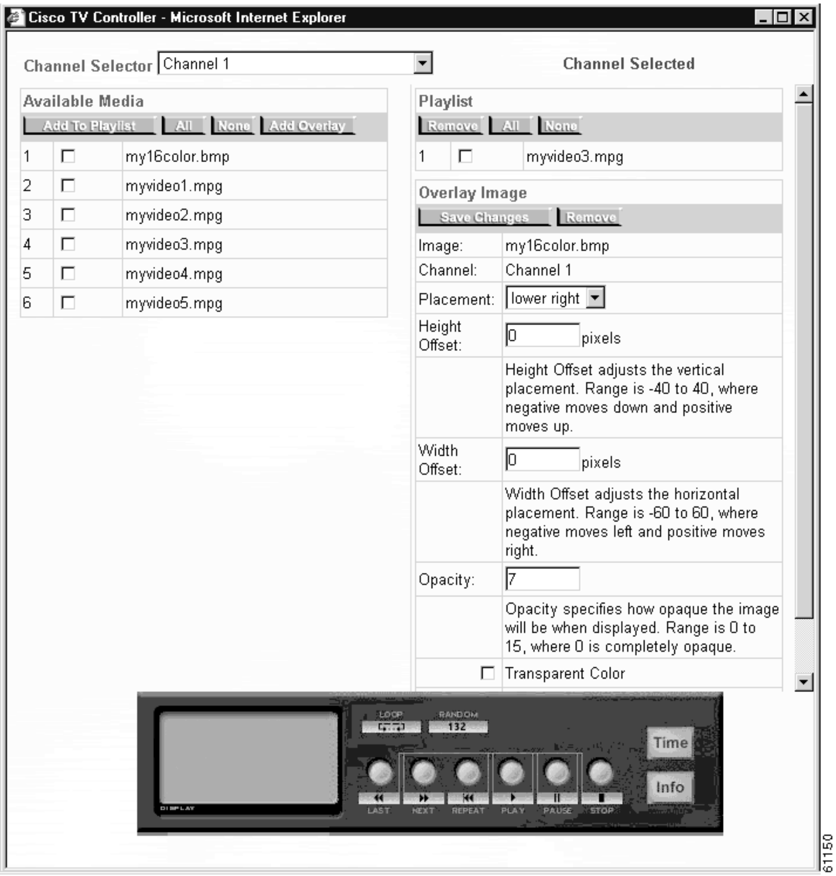
You can now edit the parameters of the overlay image by specifying and adjusting where on the TV monitor it should appear, specifying the overall opacity of the image, and choosing whether or not you want to set one color to be transparent. For information on how to change the parameters, see the "Removing an Overlay Image from a Playlist" section on page 3-52 or the "Changing the Parameters of a Playlist Overlay Image Using the TV Controller" section on page 3-43.

Changing the Parameters of a Playlist Overlay Image Using the TV Controller

Step 1 Choose **Devices > TV Controls**. The TV Controller screen appears. (See Figure 3-8.)

Step 2 Click the TV-out enabled device that has the playlist whose overlay image you want to modify.

Figure 3-8 TV Controller Screen



Cisco TV Controller - Microsoft Internet Explorer

Channel Selector: Channel 1 | Channel Selected

Available Media

1	□	my16color.bmp
2	□	myvideo1.mpg
3	□	myvideo2.mpg
4	□	myvideo3.mpg
5	□	myvideo4.mpg
6	□	myvideo5.mpg

Playlist

1	□	myvideo3.mpg

Overlay Image

Image:	my16color.bmp
Channel:	Channel 1
Placement:	lower right
Height Offset:	0 pixels
	Height Offset adjusts the vertical placement. Range is -40 to 40, where negative moves down and positive moves up.
Width Offset:	0 pixels
	Width Offset adjusts the horizontal placement. Range is -60 to 60, where negative moves left and positive moves right.
Opacity:	7
	Opacity specifies how opaque the image will be when displayed. Range is 0 to 15, where 0 is completely opaque.
□	Transparent Color

Step 3 If prompted, enter a username and password.

Step 4 Under the Overlay Image heading, modify the parameters described in Table 3-5.

Table 3-5 Overlay Image Parameters

Image Parameter	Description
Placement	Specifies where the overlay image should appear on the TV-out monitor. Your options are upper left, upper right, lower left, lower right, and center.
Height offset	Adjusts placement along the vertical axis. The valid range is from –40 to 40 pixels. –40 = Moves the image to the lowest possible position on the display. 40 = Moves the image to the uppermost position on the display.
Width offset	Adjusts placement along the horizontal axis. The valid range is from –60 to 60 pixels. –60 = Moves the image to the left-most possible position on the display. 60 = Moves the image to the right-most possible position on the display.
Opacity	Adjusts the opacity of the overlay image. The valid range is from 0 to 15. 0 = Renders the image completely opaque. 15 = Renders the image nearly transparent.

Table 3-5 Overlay Image Parameters (continued)

Image Parameter	Description
Transparency	Enables or disables the use of transparency. When enabled, the color of the pixel in the lower left corner of the image is transparent over the entire image. When a transparency-enabled image is placed over a video, the background color of the overlay image is not visible against the video playing behind it. This is useful if you want to use a nonrectangular image as your overlay. 0 = Disables the use of transparency. 1 = Enables the use of transparency.

Using the TV Controller and Playlist Programmatically

This section describes how to perform the following tasks using the TV controller and playlist programmatically:

- Adding Programs to the Playlist
- Deleting Programs from the Playlist
- Clearing the Playlist
- Adding Schedules to the Playlist
- Removing Schedules from the Playlist
- Clearing the Playlist Schedule
- Playing Programs from the Playlist
- Stopping Playback
- Pausing Playback
- Playing the Next Program in the Playlist
- Playing the Previous Program in the Playlist

- Restarting Playback
- Looping Through the Playlist
- Using Random Play
- Enabling or Disabling Soft Stop
- Adding an Overlay Image to a Playlist
- Removing an Overlay Image from a Playlist
- Changing the Parameters of a Playlist's Overlay Image

Adding Programs to the Playlist

To add a list of media files from a channel to the play list, enter the following URL:

```
http://<CE_IP>/cgi/videocontrol?OP=PLAYLIST&CMD=ADD-BY-NAME&CHANNEL-NAME=channel_name
&FILENAME=<file1,file2,...>
```

where:

- CE_IP is the IP address of the Content Engine.
- channel_name is the name of the channel from which media files are to be added to the playlist.
- file1,file2 is the name of the media files to be added to the playlist. Filenames must be separated by commas.

Deleting Programs from the Playlist

To delete the list of media files belonging to the playlist, enter the following URL:

```
http://<CE_IP>/cgi/videocontrol?OP=PLAYLIST&CMD=REMOVE-BY-NAME&CHANNEL-NAME=<channel_name>
&FILENAME=<file1,file2,...>
```

where:

- CE_IP is the IP address of the Content Engine.
- channel_name is the name of the channel to which the media files belong.
- file1,file2 is the name of media files to be removed from the playlist. Filenames should be separated by commas.

Clearing the Playlist

To clear the playlist, enter the following URL:

```
http://<CE_IP>/cgi/videocontrol?OP=PLAYLIST&CMD=CLEAR
```

where:

CE_IP is the IP address of the Content Engine.

Adding Schedules to the Playlist

To define start and stop times for playing the playlist, enter the following URL:

```
http://<CE_IP>/cgi/videocontrol?OP=PLAYTIMES&CMD=ADD&EVENT=<start_time>,<stop_time>
```

where:

- CE_IP is the IP address of the Content Engine.
- start_time is the start time in seconds since 1970.
- stop_time is the stop time in seconds since 1970.

Note The start or stop time (in seconds from epoch) must be based on accurate Greenwich mean time (GMT)/Coordinated Universal Time (UTC); this is then translated into the local time of the TV-out device.

Removing Schedules from the Playlist

To remove defined schedules from the playlist, enter the following URL:

```
http://<CE_IP>/cgi/videocontrol?OP=PLAYTIMES&CMD=REMOVE&EVENT=<start_time>,<stop_time>
```

where:

- CE_IP is the IP address of the Content Engine.
- start_time is the start time in seconds since 1970.
- stop_time is the stop time in seconds since 1970.

Note The start or stop time (in seconds from epoch) must be based on accurate Greenwich mean time (GMT)/Coordinated Universal Time (UTC); this is then translated into the local time of the TV-out device

Clearing the Playlist Schedule

To clear all schedules defined for the playlist, enter the following URL:

```
http://<CE_IP>/cgi/videocontrol?OP=PLAYTIMES&CMD=CLEAR
```

where:

CE_IP is the IP address of the Content Engine.

Playing Programs from the Playlist

To play the programs from the playlist, enter the following URL:

```
http://<CE_IP>/cgi/videocontrol?OP=CONTROL&CMD=PLAY
```

where:

CE_IP is the IP address of the Content Engine.

Stopping Playback

To stop playback, enter the following URL:

```
http://<CE_IP>/cgi/videocontrol?OP=CONTROL&CMD=STOP
```

where:

CE_IP is the IP address of the Content Engine.

Pausing Playback

To pause playback, enter the following URL:

```
http://<CE_IP>/cgi/videocontrol?OP=CONTROL&CMD=PAUSE
```

where:

CE_IP is the IP address of the Content Engine.

Playing the Next Program in the Playlist

To play the next program, enter the following URL while the playlist is playing:

```
http://<CE_IP>/cgi/videocontrol?OP=CONTROL&CMD=NEXT
```

where:

CE_IP is the IP address of the Content Engine.

Playing the Previous Program in the Playlist

To play the previous program, enter the following URL while the playlist is playing:

```
http://<CE_IP>/cgi/videocontrol?OP=CONTROL&CMD=BACK
```

where:

CE_IP is the IP address of the Content Engine.

Restarting Playback

To restart playback, enter the following URL:

```
http://<CE_IP>/cgi/videocontrol?OP=CONTROL&CMD=RESTART
```

where:

CE_IP is the IP address of the Content Engine.

Looping Through the Playlist

To set the playlist to loop to the beginning of the playlist when it reaches the end, enter the following URL:

```
http://<CE_IP>/cgi/videocontrol?OP=FEATURE&CMD=LOOP&VALUE=<flag>
```

where:

CE_IP is the IP address of the Content Engine.

flag is set to 1 or 0, to enable or disable the loop setting, respectively.

Using Random Play

To set the playlist to play programs in random order, enter the following URL:

```
http://<CE_IP>/cgi/videocontrol?OP=FEATURE&CMD=RANDOM&VALUE=<flag>
```

where:

CE_IP is the IP address of the Content Engine.

flag is set to 1 or 0, to enable or disable the random order setting, respectively.

Enabling or Disabling Soft Stop

By default, Soft Stop is not enabled and the STOP command causes the currently playing video to abort before the playlist has been stopped. If you enable Soft Stop, a STOP command stops the currently playing song immediately, or stops after the currently playing song ends. To enable Soft Stop, enter the following URL:

```
http://<CE_IP>/cgi/videocontrol?OP=FEATURE&CMD=SOFTSTOP&VALUE=<flag>
```

where:

CE_IP is the IP address of the Content Engine.

flag is set to 1 or 0, to enable or disable the Soft Stop setting, respectively.

Adding an Overlay Image to a Playlist

You must first create a playlist to be able to associate an overlay image with it. For instructions on how to create a playlist using the TV controller, see the "Adding Programs to the Playlist" section on page 3-46.

To add an overlay image to a playlist and set its properties, enter the following URL:

```
http://<CE_IP>/cgi/videocontrol?OP=PLAYLIST&CMD=ADD-OVERLAY&OVL-IMAGE-CHN=<channel_name>
&OVL-IMAGE=<file_name>&OVL-PLACEMENT=<placement>&OVL-IMAGE-HEIGHT=-<height_offset>
&OVL-IMAGE-WIDTH=<width_offset>&OVL-OPACITY=<opacity>
&OVL-TRANSCOLOR=<transparent_color_flag>
```

where:

CE_IP is the IP address of the Content Engine.

channel_name is the name of the channel from which the overlay image file is to be added to the playlist.

file_name is the name of the overlay image file.

placement is the region of the display where the overlay image should appear. Options are:

- 0 = Upper left
- 1 = Upper right
- 2 = Lower left
- 3 = Lower right
- 4 = Center

height_offset adjusts placement along the vertical axis. The valid range is from –40 to 40 pixels.

- –40 = Moves the image to the lowest possible position on the display.
- 40 = Moves the image to the uppermost position on the display.

width_offset adjusts placement along the horizontal axis. The valid range is from –60 to 60 pixels.

- –60 = Moves the image to the left-most possible position on the display.
- 60 = Moves the image to the right-most possible position on the display.

opacity adjusts the opacity of the overlay image. The valid range is from 0 to 15.

- 0 = Renders the image completely opaque.
- 15 = Renders the image nearly transparent.

transparent_color_flag is set to 1 or 0 to enable or disable the use of transparency, respectively. When enabled, the color of the pixel in the lower-left corner of the image is transparent over the entire image. When a transparency-enabled image is placed over a video, the background color of the overlay image is not visible against the video playing behind it. This is useful if you want to use a nonrectangular image as your overlay.

Removing an Overlay Image from a Playlist

To remove an overlay image file from a playlist, enter the following URL:

```
http://<CE_IP>/cgi/videocontrol?OP=PLAYLIST&CMD=REMOVE-OVERLAY&OVL-IMAGE-CHN=
[<channel_name>]&OVL-IMAGE=[<file_name>]
```

where:

CE_IP is the IP address of the Content Engine.

channel_name is the name of the channel from which the overlay image file is to be removed from the playlist. Because only one overlay image file is supported at any time, this is optional.

file_name is the name of the overlay image file to be removed from the playlist Because only one overlay image file is supported at any time, this is optional.

Changing the Parameters of a Playlist's Overlay Image

You can modify the properties of an overlay image while the playlist is playing, but the modified settings do not take effect until the next video in the playlist starts playing. To modify the properties of an overlay image, enter the following URL:

```
http://<CE_IP>/cgi/videocontrol?OP=PLAYLIST&CMD=ADD-OVERLAY&OVL-IMAGE-CHN=
<channel_name>&OVL-IMAGE=<file_name>&OVL-PLACEMENT=<placement>
&OVL-IMAGE-HEIGHT=-<height_offset>&OVL-IMAGE-WIDTH=<width_offset>&OVL-OPACITY=<opacity>
&OVL-TRANSCOLOR=<transparent_color_flag>
```

where:

CE_IP is the IP address of the Content Engine.

channel_name is the name of the channel from which the overlay image file was added to the playlist.

file_name is the name of the overlay image file.

placement is the region of the display where the overlay image should appear. Your options are:

- 0 = Upper left
- 1 = Upper right
- 2 = Lower left
- 3 = Lower right
- 4 = Center

height_offset adjusts placement along the vertical axis. The valid range is from –40 to 40 pixels.

- –40 = Moves the image to the lowest possible position on the display.
- 40 = Moves the image to the uppermost position on the display.

width_offset adjusts placement along the horizontal axis. The valid range is from –60 to 60 pixels.

- –60 = Moves the image to the left-most possible position on the display.
- 60 = Moves the image to the right-most possible position on the display.

opacity adjusts the opacity of the overlay image. The valid range is from 0 to 15.

- 0 = Renders the image completely opaque.
- 15 = Renders the image least opaque or nearly transparent.

transparent_color_flag is set to 1 or 0 to enable or disable the use of transparency, respectively. When enabled, the color of the pixel in the lower-left corner is transparent over the entire image.

Live Media Splitting

This section discusses live splitting for both RealServer and WMT broadcasts. It also discussses enabling CDN back-channel multicasting on a LAN.

Splitting Live RealServer Broadcasts

Note For information about enabling RealSubscriber and setting up a publisher RealServer, refer to the *Cisco Content Delivery Networking Products Getting Started Guide*. RealSubscriber is simply another name for RealServer that runs in a subscriber-only mode.

To use the E-CDN application to split live RealServer broadcasts, the client (Content Engine) must specify the URL in the following format to contact the Content Distribution Manager:

http://<cdm_ip_address:cdm_port>/Cisco/<StudioID>/<ChannelID>/RealLive/<source_IP>:<source_port>/<source_mount_point>/<source_filename>

For example,

http://mycdm.mycompany.com:80/Cisco/0002b31b62cb/RealLive/realserver.mycompany.com:554/encoder/Livestream

Note RealSubscriber only works on streams where the origin RealServer has the Stream Splitting option enabled.

For live streaming to work, the local Content Engine must be subscribed to the channel listed in the URL. The Content Distribution Manager automatically redirects the client to link to the split stream on a local Content Engine.

The first time the Content Engine receives a request, there will be an initial transaction between the Content Engine and the RealServer to establish the data flow for the split stream. Subsequent client requests will not require this transaction to recur.

This allows multiple clients to request the same content while not consuming more bandwidth on the back end than a single client would require.

By default, clients receive the split stream from the Content Engine by unicast. To multicast the split stream from the Content Engine to clients that are configured to receive multicast, the RealServer multicast feature can be enabled on the Content Engine.

For more information, see the next section, “Enabling CDN Back-Channel Multicasting on a LAN.”

Enabling CDN Back-Channel Multicasting on a LAN

The Cisco E-CDN application includes support for LAN-based back-channel multicasting of media as part of its support for RealNetworks’ RealServer Version 8.01.

This feature, which is built into the RealServer Version 8.01 release, enables CDN installations to conserve network bandwidth by sending a single media stream to multiple clients on a LAN, rather than streaming media to each requesting client individually.

Back-channel multicasting streams content between the RealServer and clients while maintaining a simultaneous accounting control channel between each client and the RealServer. This extra control channel is used to transmit authentication information as well as client commands like “start” and “stop.” Back-channel multicasting enables the RealServer to track client behavior and display statistics during viewing, including real-time data on the number of clients receiving a presentation.

Once enabled, back-channel multicasting is applied to all streams broadcast from your RealServer. Clients that have been preconfigured to use multicasting will do so, maximizing the bandwidth available to multicasting and unicasting clients alike.

Enabling Multicasting on the Content Distribution Manager

Although you typically use the built-in administrative features of the RealServer to configure multicasting, it is possible to enable multicasting remotely from your Content Distribution Manager interface.

To use the Content Distribution Manager to enable multicasting:

Step 1 Launch your web browser and navigate to the Enable Multicast screen at the following address:

```
http://your_Content_Distribution_Manager_ip_address/cgi-bin/mc
```

where *your_Content_Distribution_Manager_ip_address* represents the IP address or DNS domain name of your Content Distribution Manager.

Step 2 With the Enable Multicast options displayed in your browser window, click the **Enable Multicast** drop-down list and choose **Yes**.

This enables the multicasting feature on the RealServer used by your Content Distribution Manager.

Step 3 In the IP Address Range fields, enter the range of addresses to which you will be sending multicast streams.

Step 4 Remember that broadcasts of video content require two addresses—one for video content and one for audio content. The RealServer uses the first available address in the range you specify. Refer to the *RealServer Administration Guide Version 8.0* at the following URL for more information: http://www.service.real.com/help/library/guides/server8/realsrvr.htm.

Step 5 Set the maximum distance that streamed packets can travel over a network, as measured in hops from one multicast-enabled router to another, by entering a Time To Live value in the Time to Live field provided.

Each time a multicast data packet passes through a multicast-enabled router, its Time To Live value is decreased by 1. Once the value reaches 0, the multicast-enabled router discards the packet.

Note For typical networks, a Time To Live value of 16 is adequate to keep packets within the network.

Step 6 Click **Set** when you are finished.

The multicast settings are saved back to the RealServer used by your Content Distribution Manager.

Splitting Live WMT Broadcasts

Note For information on enabling a WMT license, refer to the *Cisco Content Delivery Networking Products Getting Started Guide.*

An E-CDN application user who does not have WCCP may require splitting of live requests for better performance. Such splitting is done by a Content Engine that is preferably nearest to the client. Dynamic routing of live media requests serves this purpose. The administrator needs to specify a URL in the following form:

http://<CDM-hostname:CDM-port>/Cisco/opt.wmt.<protocol>/<StudioID>/<ChannelName>/wmtlive/<originServer:originPort>/<path>/<livestream>.asfx

For example:

http://10.5.201.32:80/Cisco/opt.wmt.http/0006d7031ac/Test_Channel/wmtlive/stream-ce.cisco.com/vod-14.asf.asfx

When you create a WMT multicast station configuration that points to pre-positioned E-CDN content which resides on the same Content Engine, use the following URL to access the content:

mms://<ce-ip>:<wmt-port>/preposition/<Channel_Name>/<file_name>

CHAPTER 4

Administering the System Software

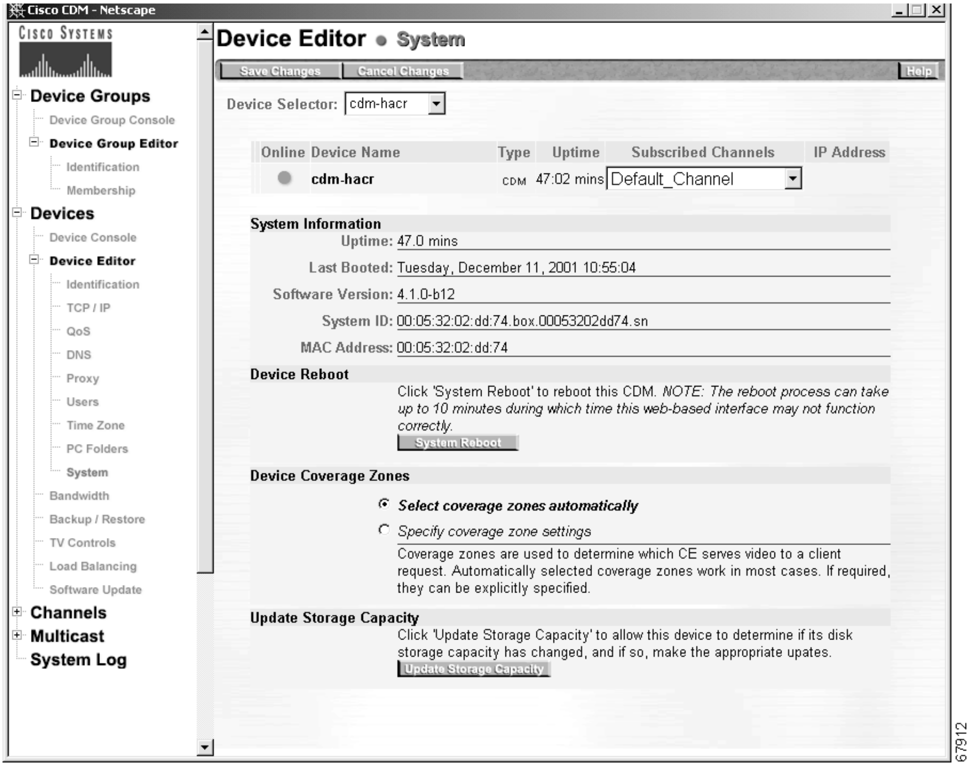
This chapter provides information how on to administer E-CDN application software. This chapter contains the following sections:

Rebooting E-CDN Application Devices

The System screen provides options for rebooting your device and reconfigure your system. (See Figure 4-1.) To reboot a CDN device, perform the following steps:

Step 1 Choose **Devices > Device Editor > System**. The Device Editor System screen appears. (See Figure 4-1.)

Figure 4-1 Device Editor System Screen (Content Distribution Manager Selected)



Device Selector: cdm-hacr

Online	Device Name	Type	Uptime	Subscribed Channels	IP Address
●	cdm-hacr	CDM	47:02 mins	Default_Channel	

System Information

Uptime: 47.0 mins

Last Booted: Tuesday, December 11, 2001 10:55:04

Software Version: 4.1.0-b12

System ID: 00:05:32:02:dd:74.box.00053202dd74.sn

MAC Address: 00:05:32:02:dd:74

Device Reboot

Click 'System Reboot' to reboot this CDM. *NOTE: The reboot process can take up to 10 minutes during which time this web-based interface may not function correctly.*

Device Coverage Zones

◉ *Select coverage zones automatically*

○ *Specify coverage zone settings*

Coverage zones are used to determine which CE serves video to a client request. Automatically selected coverage zones work in most cases. If required, they can be explicitly specified.

Update Storage Capacity

Click 'Update Storage Capacity' to allow this device to determine if its disk storage capacity has changed, and if so, make the appropriate upates.

Step 2 Make sure that the correct device is displayed in the Device Selector drop-down list.

Step 3 To reboot the selected device, click **System Reboot**. It may take up to 10 minutes for your device to reboot.

Reconfiguring CDN Devices Following a Content Distribution Manager IP Address Change

Use any of the following procedures to reconfigure your Content Distribution Manager, Content Routers, and Content Engines when the Content Distribution Manager IP address has changed. It is critical that you have some plan for redirecting your Content Engines and Content Routers to your Content Distribution Manager before changing the Content Distribution Manager IP address, and that you monitor the status of your Content Engines and Content Routers throughout the transition period to confirm that all devices are ultimately able to connect to the Content Distribution Manager at its new address.

The four approved methods for reconfiguring your E-CDN application devices following a Content Distribution Manager change of address are:

- DNS-based reconfiguration
- Content Distribution Manager-based reconfiguration
- Installation Wizard-based reconfiguration
- E-CDN application CLI (command-line interface) commands

Note Refer to the *Cisco Application and Content Networking Software Command Reference* for a description of E-CDN CLI commands. Note that any settings in the E-CDN CLI commands must match corresponding settings in the E-CDN GUI-based interface.

DNS-Based Reconfiguration

This reconfiguration option is available to customers using Domain Name System (DNS) to connect to their E-CDN application devices.

Note If you are using DNS, reconfiguring your Content Engines, Content Routers, and Content Distribution Manager using the DNS-based solution is preferable to the other methods discussed here, because it is simpler to implement and requires little or no administrative intervention.

To reconfigure your Content Engines and Content Routers if you are using DNS, perform the following steps:

Step 1 Change the IP address of the Content Distribution Manager to the new IP address. You can change the Content Distribution Manager IP address using either the Content Distribution Manager Device Editor or the Cisco E-CDN application Installation Wizard. See the “Editing TCP/IP Settings” section on page 2-11.

Step 2 Access the administrative user interface of your DNS server software and change the IP address of the Content Distribution Manager DNS name to match the new IP address of the Content Distribution Manager.

Step 3 Return to the Content Distribution Manager and choose **Devices > Device Editor > System**. The System screen appears.

Step 4 Make sure that the Content Distribution Manager is listed in the Device Selector field. If it is not, expand the drop-down list and choose the Content Distribution Manager from the devices listed.

Step 5 Click **System Reboot** to reboot your Content Distribution Manager and reconnect it to your network using the new IP address.

Step 6 Wait until your Content Engine and Content Router devices are pointed to the new address of the Content Distribution Manager.

Approximately 45 minutes after your Content Distribution Manager comes back online at its new address and is no longer available at its prior address, your Content Engines and Content Routers will begin going offline. The Content Engines and Content Routers automatically use the DNS name of the Content Distribution Manager to locate the device at its new IP address.

Step 7 Click **Device Console**. Monitor your Content Engines and Content Routers and verify that each device is able to locate the Content Distribution Manager and come back online.

Step 8 If some devices are not able to resolve the new address, use the Installation Wizard to manually point them to the location of the Content Distribution Manager. See the "Installation Wizard-Based Reconfiguration" section on page 4-7. Refer to the *Cisco Content Delivery Networking Products Getting Started Guide* for more information about the Installation Wizard.

Content Distribution Manager-Based Reconfiguration

If you are not using DNS on your network, you can provide your Content Engines and Content Routers with the new address of the Content Distribution Manager using the Alternate IP Address field on the TCP/IP screen. This field stores the new address of the Content Distribution Manager before the Content Distribution Manager has actually changed addresses. Content Engines and Content Routers that are unable to connect to the Content Distribution Manager at its original address look for the alternate IP address, and then try to reach the Content Distribution Manager at that location.

To configure the alternate IP address for your Content Distribution Manager:

Step 1 Choose **Devices > Device Editor > TCP/IP**. The TCP/IP screen appears.

Step 2 Verify that the Content Distribution Manager appears in the Device Selector drop-down list. If the Content Distribution Manager does not appear, expand the drop-down list and choose the Content Distribution Manager.

Step 3 Click the **Specify an IP address, port, subnet mask, and gateway** option.

The current IP address of the Content Distribution Manager appears in the IP Address field.

Step 4 Without changing any of the information displayed, place the cursor in the Alternate IP Address field and enter the new IP address for the Content Distribution Manager in valid "dotted quad" format, for example:

```
192.168.200.0
```

Step 5 Click **Save Changes** to save the address.

Step 6 Wait approximately 1 hour before moving the Content Distribution Manager to the address you entered in the Alternate IP Address field.

When an hour has passed, you can change the actual Content Distribution Manager IP address by using the Content Distribution Manager Device Editor or the Cisco E-CDN application Installation Wizard, or by reconfiguring your DHCP server. Enter the new IP address of the Content Distribution Manager into the IP Address field in the TCP/IP screen. This address should match the address in the Alternate IP Address field.

See the “Editing TCP/IP Settings” section on page 2-11 for further instructions on changing the IP address of CDN devices.

Step 7 Click **Save Changes**.

Step 8 Choose **Devices > Device Editor > System**. The System screen appears.

Step 9 Make sure that the Content Distribution Manager is listed in the Device Selector drop-down list. If it is not, expand the drop-down list and choose the Content Distribution Manager from the devices listed.

Step 10 Click **System Reboot** to reboot the Content Distribution Manager and reconnect it to your network using the new IP address.

Step 11 Wait for the Content Engine and Content Router devices to point to the new address of the Content Distribution Manager.

Approximately 45 minutes after your Content Distribution Manager comes back online at its new address and is no longer available at its prior address, your Content Engines and Content Routers will begin going offline. The Content Engines and Content Routers automatically use the DNS name of the Content Distribution Manager to resolve the address of the Content Distribution Manager to its new IP address.

Step 12 Click **Device Console**. Monitor your Content Engines and Content Routers and verify that each device is able to locate the Content Distribution Manager and come back online.

Step 13 If one or more devices are not able to resolve the new address of the Content Distribution Manager, use the Installation Wizard to manually point them to the location of the Content Distribution Manager. See the next section, “Installation Wizard-Based Reconfiguration.”

Installation Wizard-Based Reconfiguration

The Cisco E-CDN application Installation Wizard can be used to reconfigure your Content Distribution Manager, Content Routers, or Content Engines. Use the Installation Wizard if you are unable to successfully move your Content Distribution Manager to a new IP address using the Content Distribution Manager user interface, or if one or more Content Engines failed to locate the Content Distribution Manager at its new address after you followed the instructions in the "DNS-Based Reconfiguration" section on page 4-4 or the "Content Distribution Manager-Based Reconfiguration" section on page 4-5.

To manually reconfigure a Content Distribution Manager, Content Router, or Content Engine using the Installation Wizard, perform the following steps:

Step 1 Launch the E-CDN application Installation Wizard. For more information about the Installation Wizard, refer to the *Cisco Content Delivery Networking Products Getting Started Guide.*

The Installation Wizard screen appears.

Step 2 Click **Next** to advance to the next step in the Installation Wizard.

The Select a Device screen lists all CDN devices on the subnet by their device ID or by a user-friendly name previously assigned using the Installation Wizard.

Step 3 Choose the first device you want to configure and click **Next** to advance to the next step in the Installation Wizard.

The Name screen appears.

Step 4 If you have not already done so, enter a user-friendly name in the field provided.

This name supplements the alphanumeric device ID or MAC address and makes it easier to identify the device when you use the Installation Wizard or Content Distribution Manager user interface.

Step 5 Click **Next** to advance to the next step in the Installation Wizard.

The Content Distribution Manager screen appears.

- If the device you selected is a Content Engine or Content Router, proceed to Step 6.
- If the device you selected is a Content Distribution Manager, go to Step 8.

Step 6 Use the fields provided to point your Content Engine or Content Router to the Content Distribution Manager's new IP address on your network. You must complete this step in order for your device to be able to communicate with the rest of the E-CDN application and begin receiving media. Do one of the following:

- Choose **Name** to identify the Content Distribution Manager by its DNS name, and enter the DNS name in the field provided.
- Choose **IP address** to identify the Content Distribution Manager by its IP address, and enter the IP address in the field provided in valid "dotted quad" format, for example:

  ```
  192.168.200.223
  ```

Step 7 Click **Next** to advance to the next step in the Installation Wizard to indicate whether or not you are using a DHCP server.

The Obtain Network Settings Automatically (DHCP) screen appears.

Step 8 Perform one of the following actions:

- If you are using DHCP, choose **Yes** and then click **Next** to proceed to the next step in the Installation Wizard to configure a Domain Name System (DNS) server.
- If you are not using DHCP and are configuring CDN devices manually, choose **No** and then click **Next**.

  The Network Settings screen appears.

  - Place your cursor in the IP address field and enter the network IP address, using the arrow key to move from block to block.
  - Press the **Tab** key to advance to the next fields and enter the subnet mask, if one is being used, as well as the gateway address used by the selected Content Engine, Content Router, or Content Distribution Manager.

The DNS-Domain Name Server screen appears.

Step 9 Perform one of the following actions:

- If you are using a DNS server, choose **Yes**, and then click **Next** to advance to the DNS Servers screen and provide the IP addresses of DNS servers referenced by your CDN devices.

  Click **Next** to advance to the next step in the Installation Wizard to identify your proxy server (if one exists).

- If you are not using DNS, choose **No** and then click **Next** to advance to the next step in the Installation Wizard to identify your proxy server (if one exists).

The Proxy Server screen appears.

Step 10 Perform one of the following actions:

- If you are using a proxy server, choose **Yes**, and then click **Next** to advance to the next step in the Installation Wizard to identify proxy settings. The Proxy Settings screen appears.
  - In the fields provided, enter the IP address of the proxy server and the number of the designated port through which traffic will pass (usually 80).
  - Click **Next** to advance to the next step in the Installation Wizard to identify a secure proxy server (if one exists).
- If you are not using a proxy server, choose **No** and then click **Next** to advance to the next step in the Installation Wizard to identify a secure proxy server (if one exists).

The Secure Proxy Server screen appears.

Step 11 Perform one of the following actions:

- If you are using a secure proxy server, choose **Yes**, and then click **Next**. The Secure Proxy Settings screen appears.
  - Using the fields provided, enter the IP address, port number, and proxy server username and password.
  - Click **Next** to advance to the next step in the Installation Wizard to specify addresses that will be treated as proxy exceptions.
- If you are not using a secure proxy server, choose **No** and click **Next** to advance to the next step in the Installation Wizard to specify addresses that will be treated as proxy exceptions.

The Proxy Exceptions List screen appears.

Step 12 Perform one of the following actions:

- If you do not have addresses you wish to treat as proxy exceptions, choose **No**, and then click **Next** to advance to the next step in the Installation Wizard to review the configuration settings for your selected device.
- If you have addresses that you do not want to connect through your proxy or secure proxy server, choose **Yes** and then click **Next**.

  The Proxy Exceptions screen appears.

  - Enter the IP address of your first exception in the field provided, and then click **Add** to add it to the list of exceptions immediately below.
  - Repeat this step for each exception. If you make a mistake, click the exception address in the list of exceptions, and then click **Remove** to remove the address from the list.
  - When you have finished adding exceptions, click **Next** to advance to the next step in the Installation Wizard to review the configuration settings for your CDN device.

The Settings screen appears.

Step 13 Review the configuration settings for your CDN device.

- If the information is not accurate, click **Back** to step back in the Installation Wizard and change the configuration information.
- Otherwise, click **Finish** to configure the Content Engine or Content Distribution Manager using the settings displayed and advance to the next step in the Installation Wizard to confirm configuration of the CDN device.

Tip If you want to copy the information for use in another application, document, or e-mail, click **Copy info** to copy the configuration settings to your Windows clipboard. You can then paste the information into another Windows application.

The Configuration Status screen appears.

Step 14 Perform one of the following actions:

- If this is a Content Distribution Manager or is not a new Content Engine or Content Router, proceed to Step 15 and wait for the device status to change to "online" before exiting the Installation Wizard.
- If this is a new Content Engine or Content Router, the device is reconfigured using the settings provided with the Installation Wizard, and then awaits approval. You must manually approve the new device.
  - Log on to the Content Distribution Manager and click **Device Console**. The Content Distribution Manager lists all associated CDN devices. The new device appears with a caution status indicator in the online column.
  - Click **Edit** to edit the device settings. From the Identification screen, check the **Approve** check box.
  - Click **Save Changes**. Return to the Installation Wizard and wait for the Content Distribution Manager approval to register.

Note It may take a few moments for the device to integrate the new configuration settings and come back online. Monitor the status messages provided in the Configuring screen and verify that your device is able to come online properly.

The machine status indicator located beneath the Copy info button will turn green and read "online."

Step 15 Once the device status is "online," click **More** to return to the Select a Device screen and configure another of your CDN devices, or click **Exit** to close the Installation Wizard.

If the device fails to come online, click **Back** to step backward in the Installation Wizard and review your configuration settings.

After initial device configuration, the Content Distribution Manager user interface can be used to modify the configuration settings on any of your devices. See the "Setting Up Content Delivery Network Devices" section on page 2-3 for detailed instructions on configuring your Content Distribution Manager, Content Routers, or Content Engines using the Content Distribution Manager user interface.

Moving Devices Between Administrative Domains

This section describes the procedure for moving Content Engines and Content Routers from one Content Distribution Manager administrative domain to another.

To move a device between administrative Content Distribution Manager domains, you must perform the following actions:

1. Reset the device to factory settings.
2. Remove the device from the current administrative Content Distribution Manager domain.
3. Assign a new administrative Content Distribution Manager domain, using the Installation Wizard graphical user interface (GUI) or ACNS 4.1 software command-line interface (CLI).
4. Approve the device in the new administrative Content Distribution Manager domain.

Resetting the Device to Factory Settings

To reset the device to factory settings, perform the following steps:

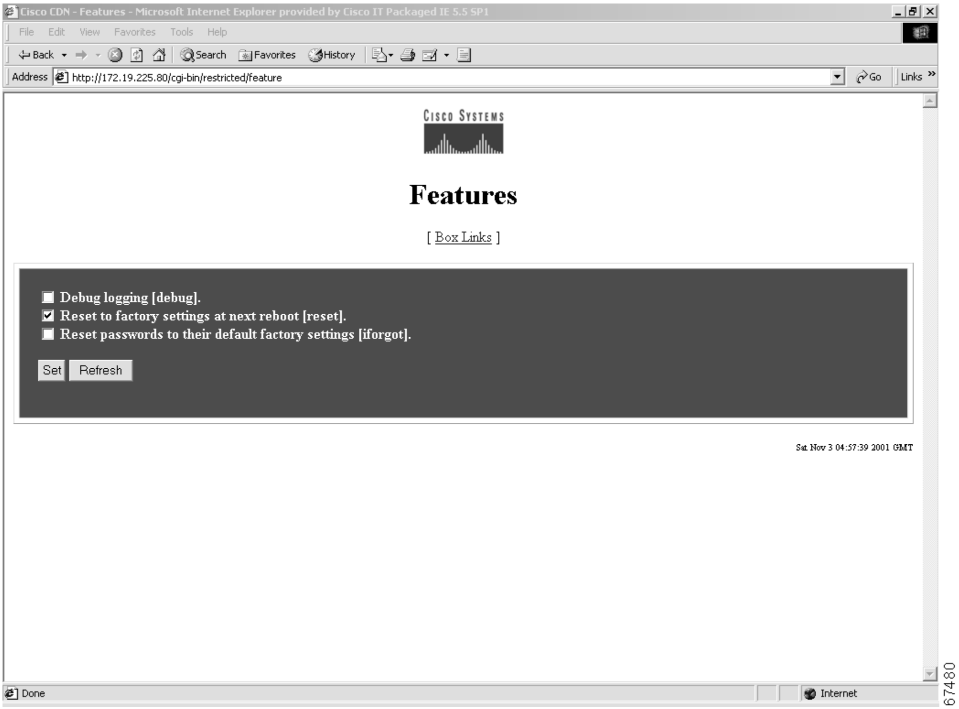
Step 1 Enter the following URL in your web browser:

```
http://device-ip-address/cgi-bin/restricted/feature
```

where *device-ip-address* is the IP address of the device that you wish to move to a new domain.

Step 2 Enter the administrator username and password and then click **OK**. The Features screen for the device appears. (See Figure 4-2.)

Figure 4-2 Features Screen



Cisco CDN - Features - Microsoft Internet Explorer provided by Cisco IT Packaged IE 5.5 SP1
File Edit View Favorites Tools Help
Back
Search
Favorites
History
Address
Go
Links
Done
Internet
67480

Address: http://172.19.225.80/cgi-bin/restricted/feature

Cisco Systems

Features

[Box Links]

☐ Debug logging [debug].
☑ Reset to factory settings at next reboot [reset].
☐ Reset passwords to their default factory settings [iforgot].

Set Refresh

Sat Nov 3 04:57:39 2001 GMT

Step 3 On the Features screen, check the **Reset to factory settings at reboot [reset]** check box to reset the device to factory settings and click **Set**.

Step 4 Reset the device using one of the following methods:

- Power cycle the device.
- Reboot the device by entering the following URL in your web browser:

  `http://device-ip-address/cgi-bin/restricted/reboot`

  where *device-ip-address* is the IP address of the device that you want to reboot.

- Use the **reload** EXEC command in the ACNS 4.1 software CLI for the device.

```
CE590-1# reload
System configuration has been modified. Save?[yes]:
Proceed with reload?[confirm]
Restarting system.
```

- Use the Content Distribution Manager GUI to reset the device.

Removing the Device from the Current Administrative Domain

To remove the device from the current administrative Content Distribution Manager domain, perform the following steps:

Step 1 Enter the following URL in your web browser:

```
http://cdm-ip-address
```

where *cdm-ip-address* is the IP address of the Content Distribution Manager currently associated with the device that is being moved to a new domain.

Step 2 Enter the administrator username and password and then click **OK**. The Cisco Content Distribution Manager screen appears.

Step 3 Click **Device Console** to view all devices associated with this Content Distribution Manager.

Step 4 On the Device Console screen, click the **Edit** button for the device that is being moved to a new domain. The Identification screen appears.

Step 5 On the Identification screen, click the **Remove Device** button.

Step 6 Click **Yes** to confirm removal of the device.

Assigning a New Administrative Domain

There are two ways to assign a new administrative Content Distribution Manager domain:

- Using the Installation Wizard
- Using the ACNS CLI

Assigning a New Administrative Domain Using the Installation Wizard

To assign a new administrative Content Distribution Manager domain using the Installation Wizard, perform the following steps:

Step 1 Insert the Installation Wizard CD-ROM into the CD-ROM drive on your workstation.

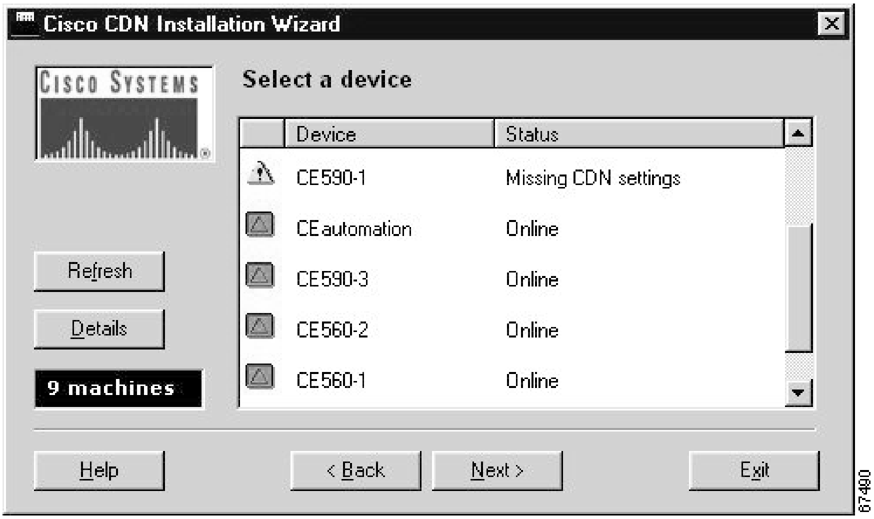
Step 2 Locate the *setup.exe* file and double-click it to install the Installation Wizard.

Step 3 After the Installation Wizard has been automatically installed, go to C:/Program Files/Cisco Systems/CDN Wizard/cdnwiz.exe. Double-click the *cndwiz.exe* file to launch the Installation Wizard. The Cisco Content Delivery Network Installation Wizard screen appears.

Step 4 Click **Next** to advance to the Select a Device screen, which lists all E-CDN application devices on the subnet by their device ID or by a user-friendly name previously assigned when the Installation Wizard was used to initially install the E-CDN application (See Figure 4-3.)

Note The Installation Wizard shows you only devices that are connected to the same local segment as the Windows PC that is running the Installation Wizard program.

Figure 4-3 Select a Device Screen



Cisco CDN Installation Wizard

Select a device

	Device	Status
⚠	CE590-1	Missing CDN settings
△	CEautomation	Online
△	CE590-3	Online
△	CE560-2	Online
△	CE560-1	Online

9 machines

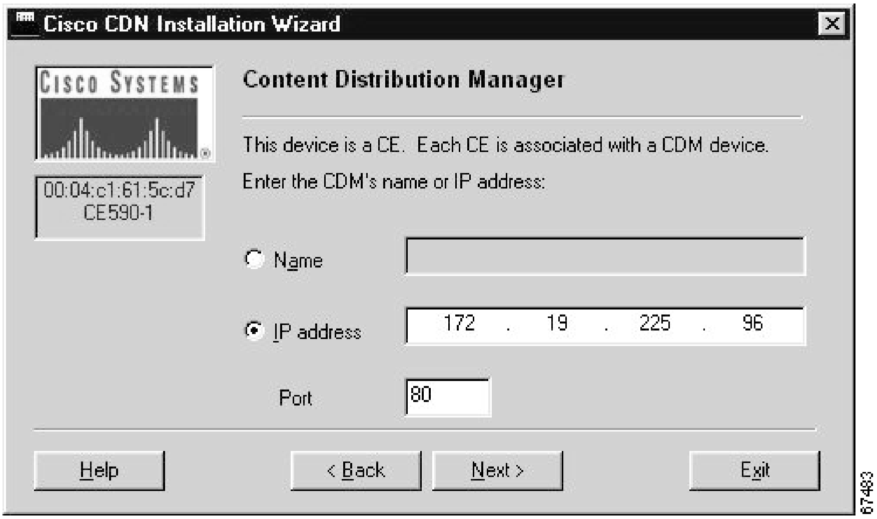
Step 5 When the device that you removed begins rebooting (because you reset the device to factory settings), a red circle appears next to the device name. After the device has rebooted and is running, a yellow triangle appears next to the device name in the Installation Wizard console with the following message:

```
Missing CDN settings
```

Choose the device and click **Next** to advance to the Name screen.

Step 6 Click **Next** to accept the Name screen settings and advance to the Content Distribution Manager screen. (See Figure 4-4.)

Figure 4-4 Content Distribution Manager Screen



Cisco CDN Installation Wizard

00:04:c1:61:5c:d7
CE590-1

Content Distribution Manager

This device is a CE. Each CE is associated with a CDM device.

Enter the CDM's name or IP address:

○ Name

● IP address 172 . 19 . 225 . 96

Port 80

Step 7 From the Content Distribution Manager screen, perform one of the following actions:

- Choose **Name** to identify the Content Distribution Manager by its Domain Name System (DNS) name, and enter the DNS name in the field provided.
- Choose **IP address** to identify the Content Distribution Manager by its IP address, and enter the IP address in the field provided in valid “dotted quad” format, for example:

```
192.168.0.0
```

Step 8 If the port number of the Content Distribution Manager is other than the default of 80, enter the new port number in the field provided.

Step 9 Click **Next** to advance to the Obtain Network Settings Automatically (DHCP) screen.

Step 10 Click **Next** to accept the Obtain Network Settings Automatically (DHCP) screen settings and advance to the DNS-Domain Name System screen.

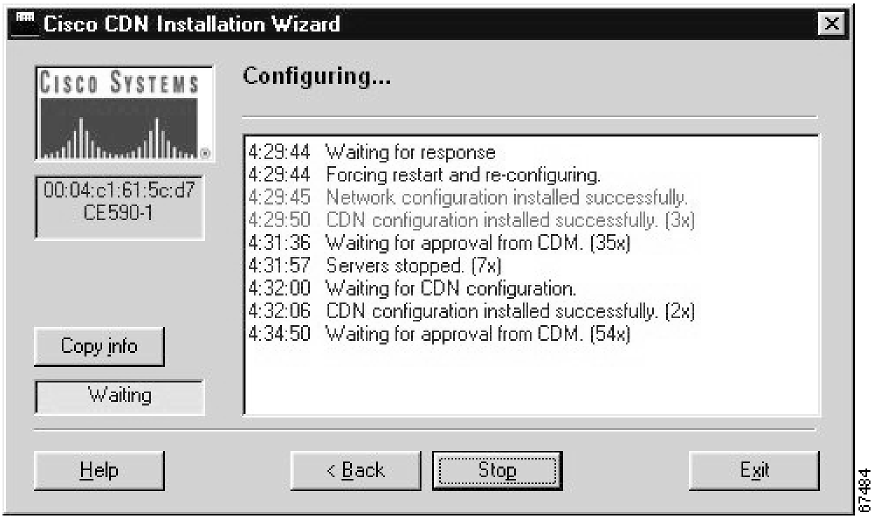
Step 11 Click **Next** to accept the DNS-Domain Name System screen settings and advance to the Proxy Server screen.

Step 12 Click **Next** to accept the Proxy Server screen settings and advance to the Secure Proxy Server screen.

Step 13 Click **Next** to advance to the Settings screen to review the configuration settings for your Content Engine or Content Router.

- If the information is not accurate, click **Back** to step back through the Installation Wizard and change the configuration information.
- Otherwise, click **Finish** to configure the device using the settings displayed and advance to the Configuration Status screen to confirm configuration of the device. (See Figure 4-5.)

Figure 4-5 Configuration Status Screen



Cisco CDN Installation Wizard

Configuring...

00:04:c1:61:5c:d7
CE590-1

```
4:29:44  Waiting for response
4:29:44  Forcing restart and re-configuring.
4:29:45  Network configuration installed successfully.
4:29:50  CDN configuration installed successfully. (3x)
4:31:36  Waiting for approval from CDM. (35x)
4:31:57  Servers stopped. (7x)
4:32:00  Waiting for CDN configuration.
4:32:06  CDN configuration installed successfully. (2x)
4:34:50  Waiting for approval from CDM. (54x)
```

Waiting

After you click **Finish** in the Installation Wizard, a status box appears with configuration information. Ultimately, you see the device status as “online.” However, if the device is a new Content Engine or Content Router, or if it previously existed but was moved to a different Content Distribution Manager administrative domain, then it must first be approved within the Content Distribution Manager GUI before the device status changes to online.

Step 14 From the Configuration Status screen, perform one of the following actions:

- Click **Back** and review your configuration settings.
- Click **Exit** to close the Installation Wizard.

You are now ready to approve the device in the new administrative domain using the Content Distribution Manager GUI.

Assigning a New Administrative Domain Using the ACNS 4.1 Software CLI

To assign a new administrative Content Distribution Manager domain using the ACNS 4.1 software CLI, perform the following steps:

Step 1 When the device reboots (because you reset the device to factory settings), verify that there is no Content Distribution Manager assigned to this device by using the **show running-config** EXEC CLI command on the device. There should be no Content Distribution Manager IP address listed.

Step 2 Use the **ecdn cdm ip** command in global configuration mode to associate the device with the IP address and (optionally) the port number of the new Content Distribution Manager. For example,

```
ContentEngine(config)# ecdn cdm ip 1.1.1.1 port 110
```

You are now ready to approve the device in the new administrative domain using the Content Distribution Manager GUI.

Approving the Device in the New Administrative Domain

To approve the device in the new administrative Content Distribution Manager domain, perform the following steps:

Step 1 Enter the following URL in your web browser:

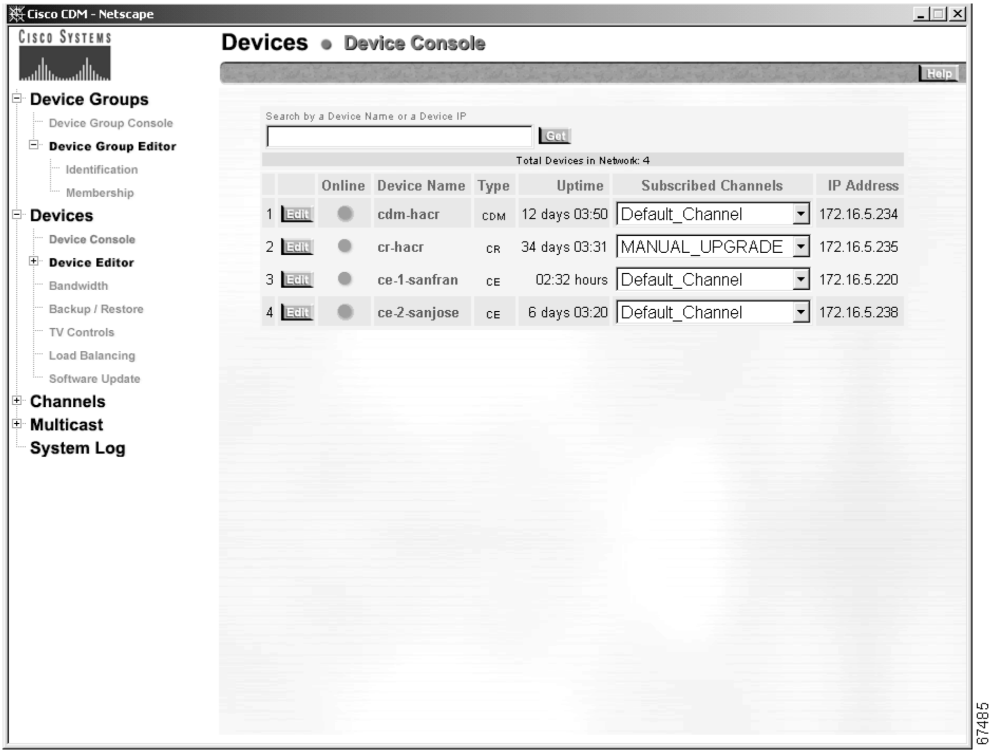
```
http://cdm-ip-address
```

where *cdm-ip-address* is the IP address of the new Content Distribution Manager that you wish to associate with the device being moved.

Enter the administrator username and password and then click **OK**. The Cisco Content Distribution Manager screen appears.

Step 2 Choose **Devices > Device Console** to view all devices associated with the new Content Distribution Manager. (See Figure 4-6.)

Figure 4-6 Devices Device Console Screen



Total Devices in Network: 4

		Online	Device Name	Type	Uptime	Subscribed Channels	IP Address
1	Edit	●	cdm-hacr	CDM	12 days 03:50	Default_Channel	172.16.5.234
2	Edit	●	cr-hacr	CR	34 days 03:31	MANUAL_UPGRADE	172.16.5.235
3	Edit	●	ce-1-sanfran	CE	02:32 hours	Default_Channel	172.16.5.220
4	Edit	●	ce-2-sanjose	CE	6 days 03:20	Default_Channel	172.16.5.238

Step 3 On the Devices Device Console screen, click the **Edit** button for the device that you moved to the Content Distribution Manager domain. The Device Editor Identification screen appears.

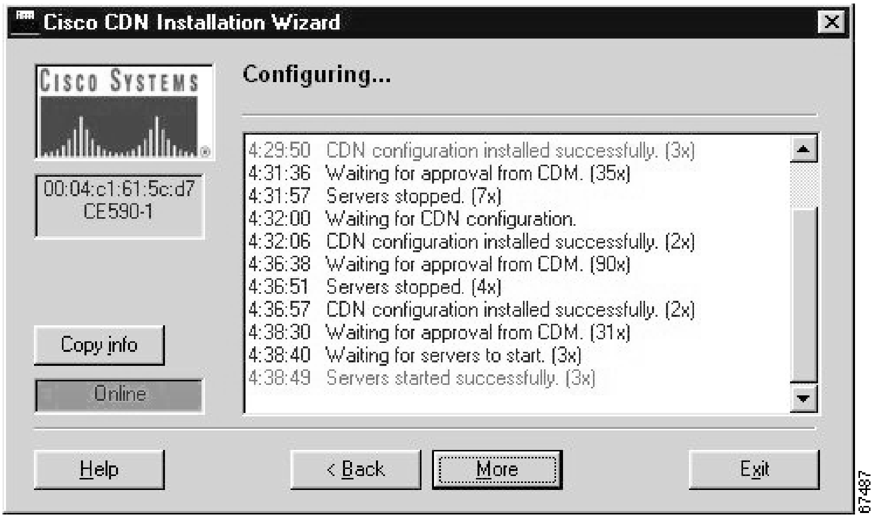
Step 4 On the Device Editor Identification screen, check the **Approve** check box and then click the **Save Changes** button.

Step 5 Choose **Devices > Device Console** to verify that the status of the device that you moved is online (a green light icon is displayed).

Step 6 You can also view the Configuration Status screen (see Figure 4-7) for that device in the Installation Wizard to confirm that the device was moved successfully. The following message indicates a successful move:

```
Servers started successfully
```

Figure 4-7 Configuration Status Screen

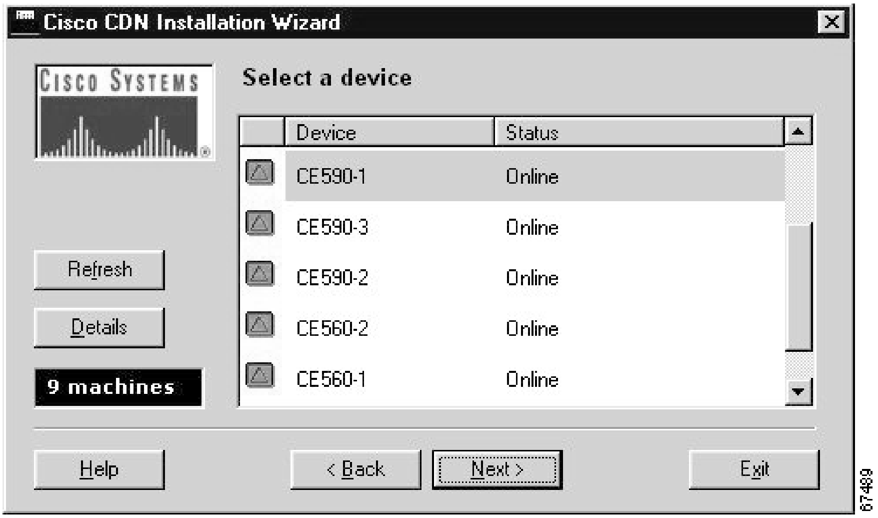


```
4:29:50  CDN configuration installed successfully. (3x)
4:31:36  Waiting for approval from CDM. (35x)
4:31:57  Servers stopped. (7x)
4:32:00  Waiting for CDN configuration.
4:32:06  CDN configuration installed successfully. (2x)
4:36:38  Waiting for approval from CDM. (90x)
4:36:51  Servers stopped. (4x)
4:36:57  CDN configuration installed successfully. (2x)
4:38:30  Waiting for approval from CDM. (31x)
4:38:40  Waiting for servers to start. (3x)
4:38:49  Servers started successfully. (3x)
```

Step 7 Click **Exit**. The Select a Device screen appears. (See Figure 4-8.)

Step 8 Verify that the status of the device that you moved is online (a green triangle is next to the device name).

Figure 4-8 Select a Device Screen



Cisco CDN Installation Wizard

Select a device

Device	Status
CE590-1	Online
CE590-3	Online
CE590-2	Online
CE560-2	Online
CE560-1	Online

9 machines

Backing Up and Restoring E-CDN Application Data

The Content Distribution Manager provides the capability for tape backup and restoration to protect against lost data and to provide service recovery.

We recommend that you do a backup before performing any software upgrades.

Note You must be running an X11 server on your PC client to use the Backup/Restore Utility (BRU). In this procedure, we use Reflection X as an example of an X11 server.

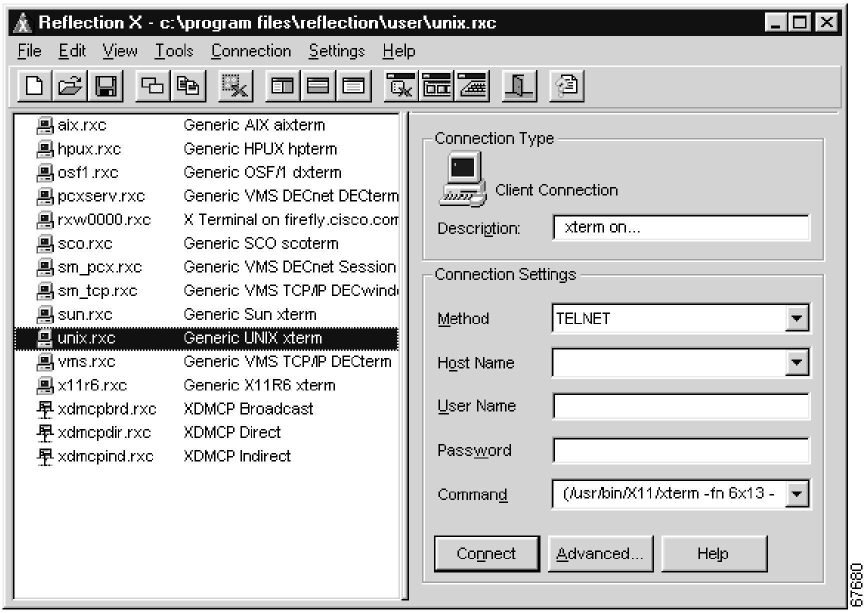
To use the backup feature, perform the following steps:

Step 1 Be sure that the Content Distribution Manager has been rebooted since the DLT7000 tape drive was installed and powered on. Otherwise, the Content Distribution Manager will not recognize the tape drive and the backup will fail.

Step 2 Load the DLT tape IV cartridge into the DLT7000 tape drive on your device.

Step 3 In order to access the backup interface, you must first launch an X11 server application on your PC client. If you are using Reflection X, the X Client Manager screen appears. (See Figure 4-9.)

Figure 4-9 X Client Manager Screen


Reflection X - c:\program files\reflection\user\unix.rxc
File Edit View Tools Connection Settings Help
Connection Type
Client Connection
Connection Settings
Connect
Advanced...
Help
67680

aix.rxc	Generic AIX aixterm
hpux.rxc	Generic HPUX hpterm
osf1.rxc	Generic OSF/1 dxterm
pcxserv.rxc	Generic VMS DECnet DECterm
rxw0000.rxc	X Terminal on firefly.cisco.com
sco.rxc	Generic SCO scoterm
sm_pcx.rxc	Generic VMS DECnet Session
sm_tcp.rxc	Generic VMS TCP/IP DECwind
sun.rxc	Generic Sun xterm
unix.rxc	Generic UNIX xterm
vms.rxc	Generic VMS TCP/IP DECterm
x11r6.rxc	Generic X11R6 xterm
xdmcpbrd.rxc	XDMCP Broadcast
xdmcpdir.rxc	XDMCP Direct
xdmcpind.rxc	XDMCP Indirect

Description: xterm on...

Method: TELNET

Host Name:

User Name:

Password:

Command: (/usr/bin/X11/xterm -fn 6x13 -

Step 4 Click **Generic UNIX xterm**.

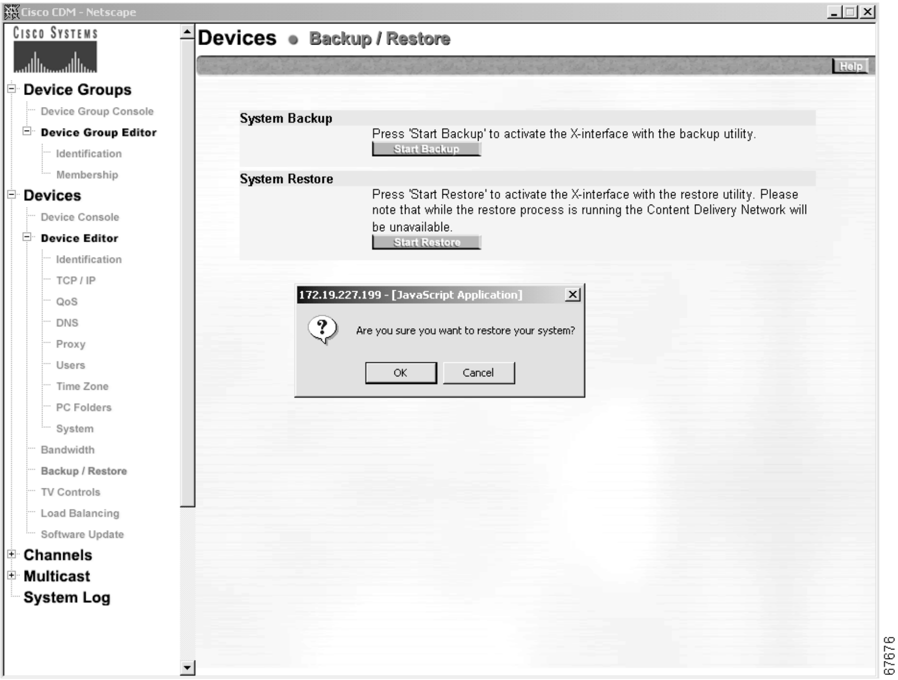
Step 5 On the same PC client as your X11 server application, launch your web browser and enter the following URL, where *cdm-ip-address* is the IP address of the Content Distribution Manager that contains the tape backup hardware:

```
http://cdm-ip-address
```

Enter the administrator username and password and then click **OK**. The Cisco Content Distribution Manager screen appears.

Step 6 Choose **Devices > Backup/Restore**. The Devices Backup/Restore screen appears. (See Figure 4-10.)

Figure 4-10 Devices Backup/Restore Screen



Press 'Start Backup' to activate the X-interface with the backup utility.

Press 'Start Restore' to activate the X-interface with the restore utility. Please note that while the restore process is running the Content Delivery Network will be unavailable.

Are you sure you want to restore your system?

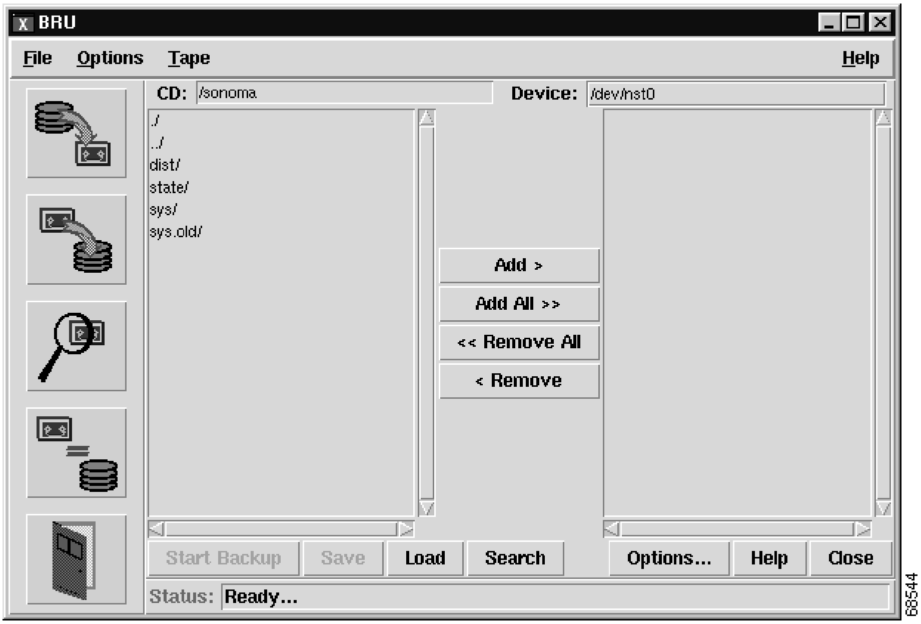
Step 7 On the Devices Backup/Restore screen, click the **Start Backup** button, and then click **OK** to confirm. The Backup/Restore Utility main screen may take up to a minute to open.

Note If the Backup/Restore Utility main screen does not appear, verify that you have an X11 server running on your PC.

Step 8 The Backup/Restore Utility main screen appears. Click the first icon in the left column, which represents backing up from disk to tape. The File Listing screen appears. (See Figure 4-11.)

Caution Do *not* click the **Full** button. Clicking the **Full** button automatically backs up temporary system files. If you then perform a restore operation, the temporary system files from the backup will overwrite any subsequent temporary system files. If this occurs, your system will fail.

Figure 4-11 File Listing Screen



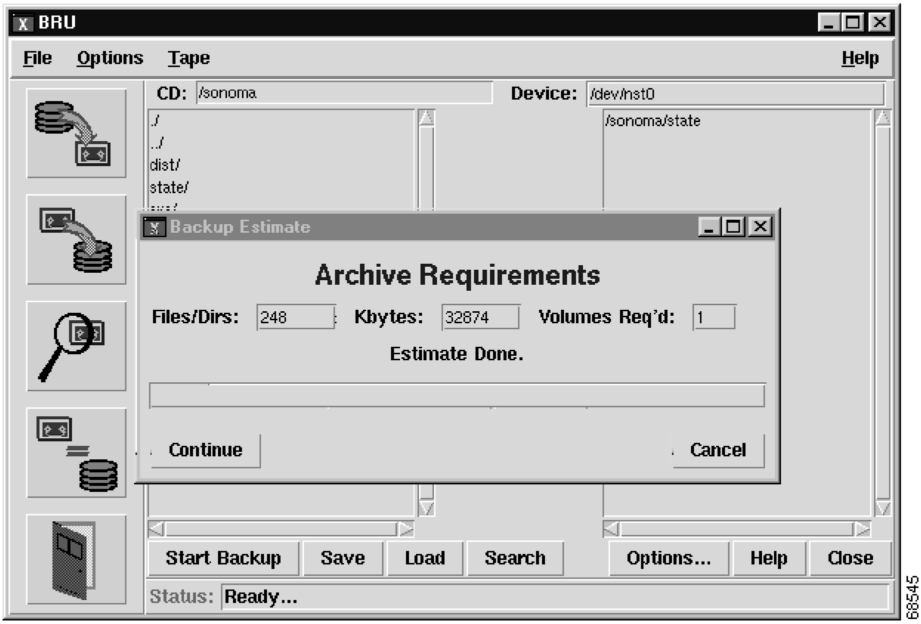
Step 9 You must perform the backup in the /sonoma directory. Choose all folders listed in the left-hand column that contain the name "state" and add them to the backup list. (Click **Add** to include these folders in the right-hand column backup list.)

Note In order to back up all of your data, you must add to the backup list all folders in the /sonoma directory that contain the name "state" (/sonoma/state, /sonoma/state1, and so forth).

Step 10 Click **Start Backup**. The Backup Progress screen appears.

Step 11 On the Backup Progress screen, enter an archive label for your backup and restore tape that is shorter than 52 characters and then click **Create Backup**. The Backup Estimate screen appears. (See Figure 4-12.)

Figure 4-12 Backup Estimate Screen



CD: /sonoma

Device: /dev/nst0

./
../
dist/
state/

/sonoma/state

Archive Requirements

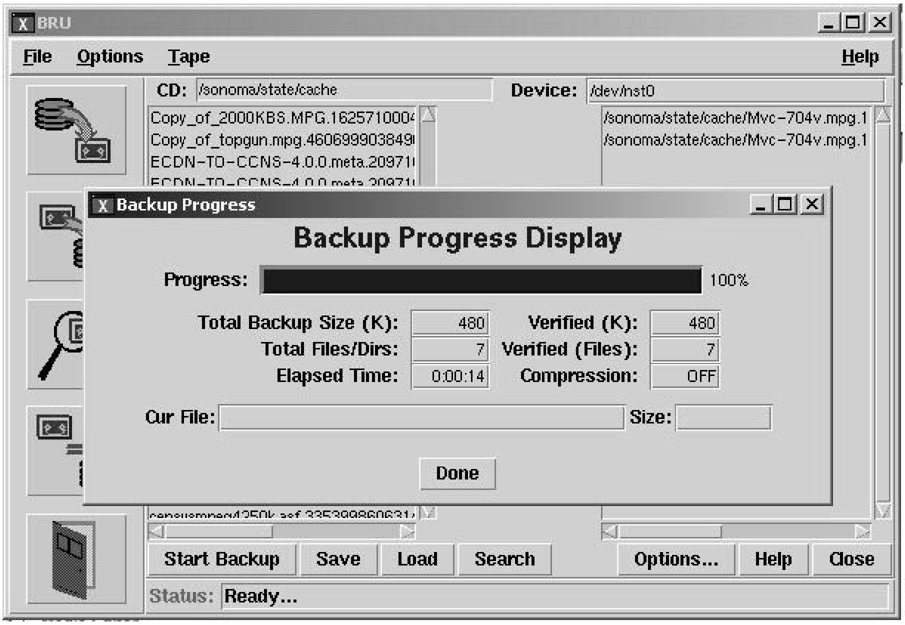
Files/Dirs: 248 Kbytes: 32874 Volumes Req'd: 1

Estimate Done.

Status: Ready...

Step 12 The Backup/Restore Utility always estimates the number of cartridges necessary to complete the operation as one. Therefore, you must manually estimate the number of needed cartridges by dividing the total amount of data by 35 GB. Each cartridge can store up to 35 GB of data. Click **Continue** to begin the backup. The Backup Progress screen appears. (See Figure 4-13.)

Figure 4-13 Backup Progress Screen



CD: /sonoma/state/cache

Device: /dev/nst0

Copy_of_2000KBS.MPG.16257100004
Copy_of_topgun.mpg.460699903849
ECDN-TO-CCNS-4.0.0.meta.20971
ECDN-TO-CCNS-4.0.0.meta.20971

/sonoma/state/cache/Mvc-704v.mpg.1
/sonoma/state/cache/Mvc-704v.mpg.1

Backup Progress Display

Progress: 100%

Total Backup Size (K): 480 Verified (K): 480
Total Files/Dirs: 7 Verified (Files): 7
Elapsed Time: 0:00:14 Compression: OFF

Cur File: Size:

Status: Ready...

The Status line at the bottom of the Backup/Restore Utility screen indicates the status of the backup.

Step 13 When the progress bar in the Backup Progress screen reaches 100 percent, the backup has been completed. Click the **Done** button and then remove the tape by pressing the unload button on the DLT7000 tape drive.

To use the restore feature, follow these steps:

Step 1 Launch your X11 server application on your PC client. If you are using Reflection X, the X Client Manager screen appears. (See Figure 4-9.)

Step 2 Click **Generic UNIX xterm**.

Step 3 Insert the tape cartridge containing the backup into the Content Distribution Manager.

Step 4 On the same PC client as your X11 server application, launch your web browser and enter the following URL, where *cdm-ip-address* is the IP address of the Content Distribution Manager that contains the tape backup hardware:

```
http://cdm-ip-address
```

Enter the administrator username and password and then click **OK**. The Cisco Content Distribution Manager screen appears.

Step 5 Choose **Devices > Backup/Restore**. The Backup/Restore screen appears. (See Figure 4-10.)

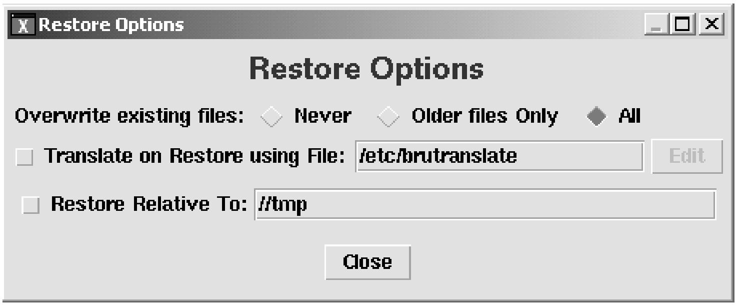
Step 6 On the Backup/Restore screen, click the **Start Restore** button, and then click **OK** to confirm. The Backup/Restore Utility main screen may take up to a minute to open.

At this time, the Content Distribution Manager stops serving media to users.

Note If the Backup/Restore Utility main screen does not appear, verify that you have an X11 server running on your PC.

Step 7 To set the Restore option, choose **Options > Restore Options** to display the Restore Options screen. Change the **Overwrite existing files** option from **Older files Only** to **All** and click **Close** to save the changes. (See Figure 4-14.) The Backup/Restore Utility main screen appears.

Figure 4-14 Restore Options Screen



Restore Options

Overwrite existing files: ○ Never ○ Older files Only ● All

□ Translate on Restore using File: /etc/brutranslate

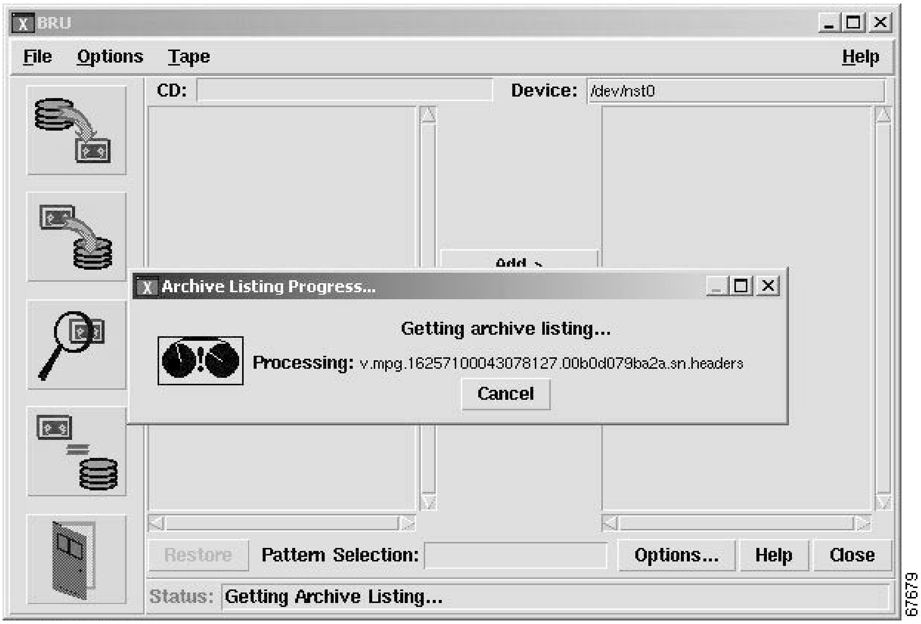
□ Restore Relative To: //tmp

Step 8 On the Backup/Restore Utility main screen, click the second icon in the left column, which represents restoring from tape to disk.

A Device Info screen appears on top of the Backup/Restore Utility main screen.

Step 9 On the Device Info screen, click **OK**. The Archive Listing Progress screen appears. (See Figure 4-15.)

Figure 4-15 Archive Listing Progress



Device: /dev/nst0

Getting archive listing...

Processing: v.mpg.16257100043078127.00b0d079ba2a.sn.headers

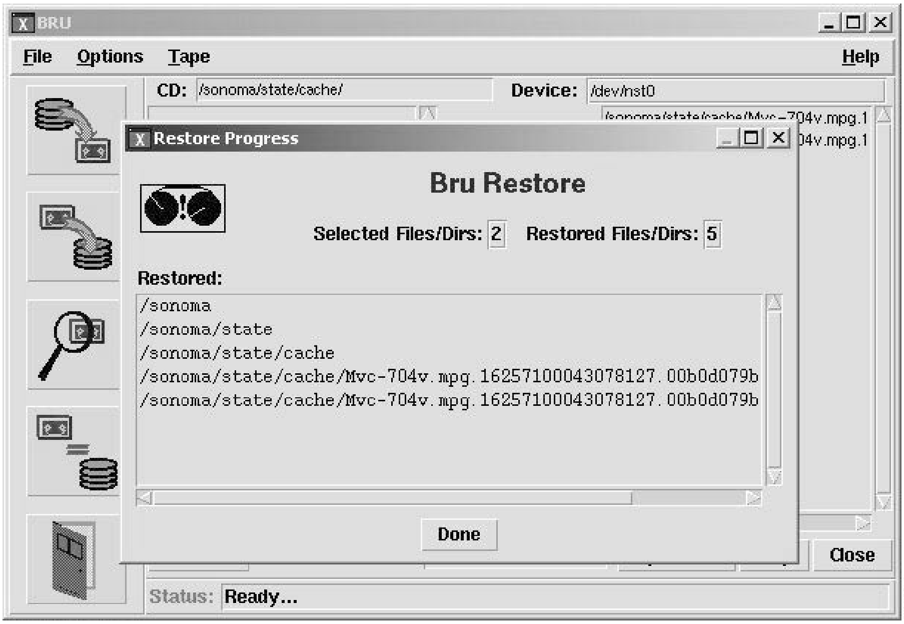
Status: Getting Archive Listing...

Wait while the Backup/Restore Utility creates an archive listing.

Step 10 After the archive listing has appeared, click the **Add All** button to restore all files and then click the **Restore** button.

The Restore Progress screen appears and displays the files being restored. (See Figure 4-16.)

Figure 4-16 Restore Progress Screen



CD: /sonoma/state/cache/

Device: /dev/nst0

Bru Restore

Selected Files/Dirs: 2 Restored Files/Dirs: 5

Restored:

```
/sonoma
/sonoma/state
/sonoma/state/cache
/sonoma/state/cache/Mvc-704v.mpg.16257100043078127.00b0d079b
/sonoma/state/cache/Mvc-704v.mpg.16257100043078127.00b0d079b
```

Status: Ready...

Step 11 When the restore process ends, this error message may appear:

```
Warning BRU exited abnormally
```

Ignore this error message and click **Cancel**. The Backup/Restore Utility main screen remains.

Step 12 On the Backup/Restore Utility main screen, click the **Done** button.

Step 13 To exit the Backup/Restore Utility, click the icon representing an open door.

The Content Distribution Manager then reconciles all the records of the old Content Distribution Manager MAC address with the MAC address of the new Content Distribution Manager.

Step 14 Launch your web browser and enter the following URL, where *cdm-ip-address* is the IP address of the Content Distribution Manager that contains the tape backup hardware:

http://*cdm-ip-address*

Enter the administrator username and password and then click **OK**. The Cisco Content Distribution Manager screen appears.

In the Content Distribution Manager GUI, verify the following items:

- All the Content Engines appear in the device console in red print and are offline.
- All the channels and their content appear.

Backup and Restore Error Messages

The following error message appears as a popup window. The message corresponds to an error condition encountered by the Content Distribution Manager in attempting to carry out a requested action.

Error Message `Rewinding Failed! Perhaps you have an incorrect setting for ‘rewindcmd’ in your /etc/brutab file.`

Explanation Generally, this message is displayed if the external DLT tape drive is not recognized by the Content Distribution Manager. If the Content Distribution Manager is rebooted when the DLT tape drive is powered off, the Content Distribution Manager does not recognize the tape drive. In Content Distribution Managers with internal tape drives, this message appears only if the tape drive is defective, if the power or SCSI cable needs to be reseated, or if the SCSI bus is not properly configured.

Recommended Action Insert the tape to fix the problem, and then reboot the Content Distribution Manager.

Explanation The tape drive is empty: the tape has not been inserted yet.

Recommended Action Check to see whether the tape has been inserted into the drive. If not, insert the tape.

Explanation The tape is dirty or the heads in the tape drive are dirty.

Recommended Action Use a cleaning tape to clean the heads.

Explanation For a CDM-4630 with an external tape drive, you must reboot the CDM-4630 while the tape drive is powered down.

Recommended Action Power up the tape drive and reboot the CDM-4630.

Maintaining the DLT Tape Drive

To maintain your DLT tape drive in good condition, use the cleaning cartridge provided with the DLT tape drive. An LED on the front of the DLT tape drive illuminates to indicate when it is time to use the cleaning cartridge.

Application Log Files

The following files log ACNS 4.1 software information:

- System log
- E-CDN application log
- Content access log
- Windows Media Technologies (WMT) access log

System Log

You can view system error messages from the System Log screen. If you perform an operation that fails, a file import for example, a message appears in the system log explaining why the import failed.

Once viewed, messages can be removed from the system log.

To view and remove system log error messages, perform the following steps:

Step 1 Click **System Log**. The system-generated error messages are displayed on the System Log screen.

Step 2 Check the check box next to error messages that you want to remove from the system log. Check **All** to choose all of the files or **None** to clear your selections.

Step 3 Click **Remove**.

E-CDN Application Log

The E-CDN application log contains detailed information regarding the E-CDN application and can be viewed in two different ways:

- To display the contents of the ecdn.log file on the screen, use the **type** or **type-tail** EXEC CLI commands in the CLI. Refer to the *Cisco Cache Software Command Reference, Release 3.1.1* for additional information on the **type** EXEC CLI command. Refer to the *Cisco Application and Content Networking Software Command Reference* for additional information on the **type-tail** EXEC CLI command.
- To access the log file from a browser, you must log in as administrator and enter the following URL, where *device-ip-address* is the address of the device:

  ```
  http://device-ip-address/cgi-bin/restricted/showlog
  ```

Content Access Log

The content access log is located on the Content Distribution Manager and contains information regarding content that has been accessed through all Content Engines by a client through HTTP (Content Engine Play and Content Distribution Manager Play options), RealMedia (RealPlay option), or with the TV-out feature (in the case of Content Engines that support this feature).

The log file is created every day shortly after midnight and contains the following entries: content title, content identifier, client address, server name, server identifier, start time, end time, aborted, server type, and appliance IP address.

Note This log file does not contain access to WMT played content. For a log of WMT played content, see the WMT access log.

The content access log can be accessed from a client through any of the following methods, where *cdm-ip-address* is the IP address of the Content Distribution Manager:

- To use FTP, specify the following:

  ftp://*admin@cdm-ip-address*/export

- To use HTTP, specify the following:

  http://*cdm-ip-address*/export

- To use a mapped drive, map a drive to the following:

  \\*cdm-ip-address*\export

WMT Access Log

This log contains Windows Media Technologies (WMT) played content and is created at each individual device that streams Windows media. It is not included in the content access log.

This is a standard Windows Media type log file, conforming to the W3C standard for an enhanced log file. The contents of this log file are defined in each file's header as follows:

```
#Fields: c-ip date time c-dns cs-uri-stem c-starttime x-duration
c-rate c-status c-playerid c-playerversion c-playerlanguage
cs(User-Agent)cs(Referer) c-hostexe c-hostexever c-os c-osversion
c-cpu filelength filesize avgbandwidth protocol transport audiocodec
videocodec channelURL sc-bytes c-bytes s-pkts-sent c-pkts-received
c-pkts-lost-client c-pkts-lost-net c-pkts-lost-cont-net c-resendreqs
c-pkts-recovered-ECC c-pkts-recovered-resent c-buffercount
c-totalbuffertime c-quality s-ip s-dns s-totalclients s-cpu-util
```

To access the file, use Windows to map a drive to the Content Engine and change to the vod_out directory.

Note For Windows NT, you may need to use the Content Distribution Manager user interface to create a user called "nobody" and log in as that user before mapping a drive from Windows to the Content Engine.

APPENDIX A

Error Messages

This appendix describes error messages that you may encounter when using the Content Distribution Manager. These messages may appear as popup windows or be listed in the system log.

Each message corresponds to an error condition encountered by the Content Distribution Manager or Content Engine in attempting to carry out a requested action.

The same error message may be produced by more than one action. The exact message text may differ slightly in your system log as a result of system-supplied variables inserted into the message text that are specific to your installation.

Error Message `Error in bandwidth specification.`

Explanation This error occurs when administrators, using the bandwidth feature of the Content Distribution Manager, attempt to add a new replication bandwidth value for a Content Engine. An incorrect (usually nonnumeric) value has been entered in the Bandwidth field.

Recommended Action In the Bandwidth field, enter the bandwidth value that you want the Content Engine to use when replicating media. This value must be a nonnegative integer and no greater than 100 (for example, 0, 10, 90, and so on). Click **Save Changes** when you have finished.

Error Message `Error in time specification.`

Explanation This error occurs when administrators, using the bandwidth feature of the Content Distribution Manager, attempt to set the start time (From) and end time (To) for replication at a particular bandwidth on a selected Content Engine. An unacceptable time value has been entered in the From or To field. Invalid values may be nonnumeric or an invalid hour or minute based on the 12-hour clock.

Recommended Action In the From and To fields, enter correct start and end times with hour and minute specifications based on a 12-hour clock. Valid start and end times are between 12:00 a.m. and 11:59 p.m. Click **Save Changes** to save your work when you are finished.

Error Message `Gateway not specified. Gateway should be in dotted quad format, for example: 127.0.0.1.`

Explanation This error occurs when administrators, using the TCP/IP feature of the Content Distribution Manager, attempt to specify a TCP/IP address for a selected Content Engine or Content Distribution Manager (in lieu of obtaining the TCP/IP settings using DHCP). A valid IP address has not been entered in the Gateway field, which identifies the network gateway device (or router) through which traffic must pass to reach the selected device.

Recommended Action Enter an IP address for the gateway device in the Gateway field. IP addresses must be numeric, nonnegative integers and must be entered in “dotted quad” format, for example, 172.16.0.0. Click **Save Changes** when you have finished.

Error Message `Improper DNS domain name specified. The name can contain only alphanumeric characters, periods, dashes, and underscores, e.g., ‘My-DNS-Server.MyCompany.com’.`

Explanation This error occurs when administrators, using the DNS feature of the Content Distribution Manager, attempt to identify a device (Content Distribution Manager or Content Engine) on the network with a user-friendly “alias” provided by a domain name server (DNS). A name has been entered in the Domain field that cannot be validated by the DNS servers listed. Domain names are typically alphanumeric and must reference an existing domain that has been established by the network administrator.

Recommended Action Enter a correct name for the defined network domain. Domain names are normally alphanumeric but can also contain periods and dashes.Other nonstandard characters are not accepted.

If the name is entered correctly, make sure that you have properly identified the domain name server in the DNS Server fields that contain the alias information for the domain you specified. You can add DNS names by clicking **Add Server**, entering the full name or IP address (in "dotted quad" format) of the DNS server that will validate the device name you entered, and clicking **Save Changes.**

Error Message `Improper DNS host name specified. The name can contain only alphanumeric characters, e.g., 'MyCDM'.`

Explanation This error occurs when administrators, using the DNS feature of the Content Distribution Manager, attempt to identify an E-CDN device (Content Distribution Manager or Content Engine) on the network with a user-friendly "alias" provided by a domain name server (DNS). A name has been entered in the Host field that cannot be validated by the DNS servers you listed. Host names are typically alphanumeric and must reference an existing device name listed on one of the network domain name servers.

Recommended Action Enter a correct host name for the device in the Host field. Host names must be made up of alphanumeric characters.

If the host name is entered correctly, make sure that you have properly identified the domain name server in the DNS Server field that contains the alias information for the host you specified. You can add DNS names by clicking **Add Server**, entering the full name or IP address (in "dotted quad" format) of the DNS server that will validate the device name you entered, and then clicking **Save Changes**.

Error Message `Improper DNS server address specified. The address must be in dotted quad format, for example: 127.0.0.1.`

Explanation This error occurs when administrators, using the DNS feature of the Content Distribution Manager, attempt to identify a domain name server (DNS) that stores "alias" information for one or more E-CDN devices. An address has been entered in the DNS Server field that is invalid. Incorrect values are nonnumeric or may have been entered in the incorrect format.

Recommended Action Enter a correct IP address for the machine acting as your DNS server in the DNS Server field. IP addresses must be numeric, nonnegative integers, and must be entered in "dotted quad" format, for example, 172.16.0.0. Click **Save Changes**.

Error Message `Improper gateway specified. Gateway should be in dotted quad format, for example: 127.0.0.1.`

Explanation This error occurs when administrators, using the TCP/IP feature of the Content Distribution Manager, attempt to specify a TCP/IP address for a selected Content Engine or Content Distribution Manager (in lieu of obtaining the TCP/IP settings using DHCP). An invalid number has been entered in the Gateway field, which identifies the network gateway device (or router) through which traffic must pass to reach the selected device. Incorrect values entered are nonnumeric, or may have been entered in the incorrect format.

Recommended Action Enter a correct IP address for the gateway device in the Gateway field. IP addresses must be numeric, nonnegative integers, and must be entered in "dotted quad" format, for example, 192.16.0.0. Click **Save Changes** when you have finished.

Error Message `Improper IP address specified. The address should be in dotted quad format, for example: 127.0.0.1.`

Explanation This error occurs when administrators, using the TCP/IP feature of the Content Distribution Manager, attempt to specify a TCP/IP address for a selected Content Engine or Content Distribution Manager (in lieu of obtaining the TCP/IP settings using DHCP). An invalid number has been entered in the IP Address field, which identifies the network address of the selected device. Incorrect values are nonnumeric, or may have been entered in the incorrect format.

Recommended Action Enter a correct IP address for the device in the IP Address field. IP addresses must be numeric, nonnegative integers, and must be entered in “dotted quad” format, for example, 192.16.0.0. Click **Save Changes** when you have finished.

Error Message `Improper media name specified. The following characters are not allowed: (,), +, =, },{, [,],″, \, |,:`

Explanation This error occurs when administrators, using the Media Importer option from the Channel Editor menu of the Content Distribution Manager, attempt to import a media file with an invalid name to a Content Distribution Manager. Filenames cannot contain the following characters: (,), +, =, },{, [,],”, \, |,:

Recommended Action Verify that the filename is correct. If not, in the Files field, enter the correct name for the media files that you are trying to import.

If the files are named correctly but have filenames that include invalid characters, you need to rename the media files you are attempting to import, replacing any nonsupported characters with alphanumeric characters or other supported characters, such as the underscore (_) character. An asterisk (*) character in the Files field returns all files in the destination specified by the URL. Click **Get List of Files** when you have finished to display the matching filenames and begin the import process.

Error Message `Improper proxy exception specified. The exception should be in the following format: 127.0.0.0/8.`

Explanation This error occurs when administrators, using the proxy server feature of the Content Distribution Manager, attempt to specify the TCP/IP address for a selected Content Engine or Content Distribution Manager that does not use the established proxy server to access the Internet. An invalid number has been entered in the Exceptions field. Incorrect values may be nonnumeric, or may have been entered in the incorrect format.

Recommended Action Enter a correct IP address for the device in the Exceptions field, and click **Save Changes**. IP addresses must be numeric, nonnegative integers and must be entered in "dotted quad" format, for example, 192.16.0.0.

Error Message `Improper proxy port specified. The port should be a numerical value, for example: 8086.`

Explanation This error occurs when administrators, using the proxy server or TCP/IP features of the Content Distribution Manager, attempt to specify the port number used by the proxy server or by the selected device. Traffic sent to and from the device passes through this port. An invalid number has been entered in the Port field. Incorrect values are nonnumeric, or may have been entered in the incorrect format, or may point to a nonexistent port number.

Recommended Action Enter a correct port number for the selected device, or the HTTP or secure address for the proxy server in the Port field, for example, 80 or 8086. A colon is not required before the port number. Click **Save Changes** when you have finished.

Error Message `Improper subnet mask specified. The mask should be in dotted quad format, for example: 255.255.0.0.`

Explanation This error occurs when administrators, using the TCP/IP feature of the Content Distribution Manager, attempt to specify an address for the local-area network subnet. An invalid number has been entered in the Subnet Mask field, which identifies the subnet address. Incorrect values are nonnumeric, or may have been entered in the incorrect format.

Recommended Action Enter a correct address for your network subnet in the Subnet Mask field. Subnet addresses must be numeric, nonnegative integers and must be entered in "dotted quad" format, for example, 255.255.255.224. Click **Save Changes** when you have finished.

Error Message `No DNS domain name specified.`

Explanation This error occurs when administrators, using the DNS feature of the Content Distribution Manager, forget to identify a domain name server (DNS). The DNS stores "alias" information for one or more E-CDN devices so that they may be referred to and "called" with user-friendly names, rather than numeric IP addresses. A name has not been entered in the DNS Server field.

Recommended Action Enter an IP address for the machine acting as your DNS server in the DNS Server field. IP addresses must be numeric, nonnegative integers and must be entered in "dotted quad" format, for example, 192.16.0.0. Click **Save Changes** when you have finished.

Error Message `No DNS host name specified.`

Explanation This error occurs when administrators, using the DNS feature of the Content Distribution Manager, attempt to identify an E-CDN device (Content Distribution Manager or Content Engine) on the network with a user-friendly "alias" provided by a domain name server (DNS). A name has not been entered in the Host Name field. Host names are typically alphanumeric and must reference an existing device name that is being tracked by a network domain name server.

Recommended Action Enter a correct name for the device in the Host Name field, and then click **Save Changes**. Host names must be made up of alphanumeric characters.

Error Message `No DNS server specified.`

Explanation This error occurs when administrators, using the DNS feature of the Content Distribution Manager, attempt to identify a domain name server (DNS) that stores "alias" information for one or more E-CDN devices. A name has not been entered in the DNS Server field.

Recommended Action Enter a correct IP address for the machine acting as your DNS server in the DNS Server field. IP addresses must be numeric, nonnegative integers and must be entered in "dotted quad" format, for example, 192.16.0.0. Click **Save Changes** when you have finished.

Error Message `No STUDIO-ADDRESS-INFO record found.`

Explanation This error occurs if one or more of your Content Distribution Manager's has lost contact with your network. Loss of contact may be due to media failure on the machine hosting your Content Distribution Manager, power loss, or some other event.

Recommended Action Try rebooting your Content Distribution Manager manually, or using the System reboot feature found on the System screen. If rebooting the Content Distribution Manager fails to resolve the problem, contact the Cisco Systems Technical Assistance Center.

Error Message `Passwords do not match. Please try again.`

Explanation This error occurs when users or administrators, working with the Users option from the Device Editor menu of the Content Distribution Manager, attempt to add or edit a password for an existing user. The E-CDN requires that the new password be entered twice to confirm its correct spelling. The two passwords entered do not match each other.

Recommended Action Reenter the password in both the Enter Password and Re-Enter Password fields to ensure that you have spelled the intended password correctly. When you have entered it correctly in each column, click **Add User** (if this password is for a new CDN user), or click **Change** (if this is an update to an existing user password).

Error Message `Please enter password in both text boxes.`

Explanation This error occurs when users or administrators, working with the Users option from the Device Editor menu of the Content Distribution Manager, attempt to edit a password for an existing user. The E-CDN application requires that the new password be entered twice to confirm its spelling. The password was entered into only one of the two required fields.

Recommended Action Reenter the password in both the Enter Password and Re-Enter Password fields to ensure that you have spelled the intended password correctly. When you have entered it correctly in each column, click **Change**.

Error Message `Please enter the new user password in both text boxes.`

Explanation This error occurs when administrators, working with the Users option from the Device Editor menu of the Content Distribution Manager, attempt to register a password for a new user. The E-CDN application requires that the new password be entered twice to confirm its spelling. The password was entered in only one of the two required fields.

Recommended Action Reenter the password in both the Enter Password and Re-Enter Password fields to ensure that you have spelled the intended password correctly. When you have entered it correctly in each column, click **Add User**.

Error Message `Please specify a User Name.`

Explanation This error occurs when users or administrators, working with the Users option from the Device Editor menu of the Content Distribution Manager, attempt to create a new user. The E-CDN application requires that all new users be assigned a username consisting of alphanumeric characters. A username has not been entered in the User Name field.

Recommended Action Enter a name for your new user in the field adjacent to the Add User button. The name cannot contain any spaces, though most other characters (alphanumeric and otherwise) are acceptable. After you have entered a name for the new user, enter the password in both the Enter Password and Re-Enter Password fields and click **Add User**.

Error Message `Please specify a User Name other than 'admin'.`

Explanation This error occurs when users or administrators, working with the Users option from the Device Editor menu of the Content Distribution Manager, attempt to create a new user with the name "admin." The E-CDN application requires that all new users have unique names. The "admin" username is already used as the default login.

Recommended Action Enter a unique name for your new user in the field adjacent to the Add User button. The name cannot contain any spaces, though most other characters (alphanumeric and otherwise) are acceptable. After you have entered a name for the new user, enter the password in both the Enter Password and Re-Enter Password fields and click **Add User**.

Error Message `Please verify that you have entered a correct bandwidth value.`

Explanation This error occurs when administrators, using the Bandwidth option from the Devices menu of the Content Distribution Manager, attempt to modify the default replication bandwidth for a Content Engine. The default bandwidth is the first listed replication setting for any Content Engine. An incorrect (usually nonnumeric) value has been entered in the Bandwidth field.

Recommended Action With the correct device selected, click the **Edit** button for the device default replication setting (the first listed setting). Enter an acceptable bandwidth value in the Bandwidth field. Bandwidth values must be nonnegative integers. Click **Save Changes** when you have finished.

Error Message `Please verify that you have entered a correct playback bandwidth value.`

Explanation This error occurs when administrators, using the Bandwidth option on the Devices menu of the Content Distribution Manager, attempt to add a new default playback bandwidth value for a Content Engine. An incorrect (usually nonnumeric) value has been entered in the Playback field.

Recommended Action In the Playback field, enter the bandwidth value that you want the Content Engine to use when streaming media for playback. This value must be a nonnegative integer. Click **Save Changes** when you have finished.

Error Message `Start and stop time must be different.`

Explanation This error occurs when administrators, using the Bandwidth feature of the Content Distribution Manager, attempt to set the start time (From) and end time (To) for replication at a particular bandwidth on a selected Content Engine. An identical time value has been entered into the From and To fields. You must designate a valid duration using the From and To fields, in which the start time (From) value is earlier than the end time (To). Replication jobs cannot span days (that is, run later than 11:59 p.m.).

Recommended Action Enter a valid start and end time in the From and To fields provided, with a start time earlier than the end time, and all times specified between 12:00 a.m. and 11:59 p.m. Click **Save Changes** when you have finished.

Error Message `Start time must be before stop time.`

Explanation This error occurs when administrators, using the Bandwidth option on the Devices menu of the Content Distribution Manager, attempt to set the start time (From) and end time (To) for replication at a particular bandwidth on a selected Content Engine. A start time value has been entered in the From field that is later than the value entered for the end time in the

To field. You must designate a valid duration using the From and To fields, with the start time earlier than the end time. Replication jobs cannot span days (that is, run later than 11:59 p.m.).

Recommended Action Enter a valid start and end time in the From and To fields provided, with the start time earlier than the end time, and all times specified between 12:00 a.m. and 11:59 p.m. Click **Save Changes** when you have finished.

Error Message `User Name cannot contain spaces.`

Explanation This error occurs when administrators, working with the Users option from the Device Editor menu of the Content Distribution Manager, attempt to create a new user. The E-CDN application requires that all new users be assigned a username consisting of alphanumeric characters. Blank spaces are not allowed. A username has been entered in the User Name field that contains spaces.

Recommended Action Enter a name for your new user in the field adjacent to the Add User button. The name cannot contain any spaces, though most other characters (alphanumeric and otherwise) are acceptable. After you have entered a name for the new user, enter the password in both the Enter Password and Re-Enter Password columns and click **Add User**.

Error Message `You have to specify Remote Announce address in the dotted quad format, for example: 127.0.0.1.`

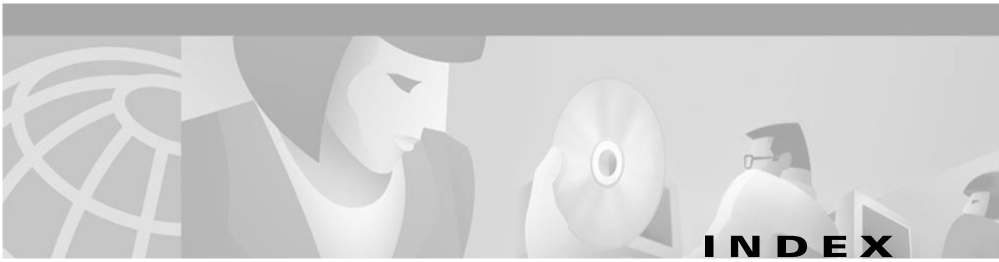
Explanation This error occurs when administrators, working with the PC Folders option from the Device Editor menu of the Content Distribution Manager, attempt to specify the network address of the remote announce machine or the subnet on which it resides. The remote announce option guarantees that machines in a different subnet from the CDN devices can communicate with the E-CDN server to coordinate media import. An address for the machine or the subnet that it was on was not specified.

Recommended Action Enter a correct address for the machine that will be serving as your remote announce machine, or enter the address of the subnet in the Remote Announce field. Addresses must be numeric, nonnegative integers and must be entered in "dotted quad" format, for example, 192.16.0.0. Click **Save Changes** when you have finished.

Error Message `You have to specify WINS server address in the dotted quad format, for example: 127.0.0.1.`

Explanation This error occurs when administrators, working with the PC Folders option from the Device Editor menu of the Content Distribution Manager, attempt to specify the network address of the Windows Internet Naming Service (WINS) server that is used to match IP addresses with NetBIOS names. Either an address was not specified for the WINS server, or the address that was specified is invalid.

Recommended Action Enter a correct IP address for the machine that will be serving as your WINS server in the WINS Server field. Addresses must be numeric, nonnegative integers and must be entered in "dotted quad" format, for example, 10.10.10.1. Click **Save Changes** when you have finished.



INDEX