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 ____% 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 Internet CDN Software User Guide

Part Number: 78-13576-01 S/W Release (if applicable): 2.1

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 document is complete.

______ The information is well organized.

______ The information is accurate.

______ The information I wanted was easy to find.

______ 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**.

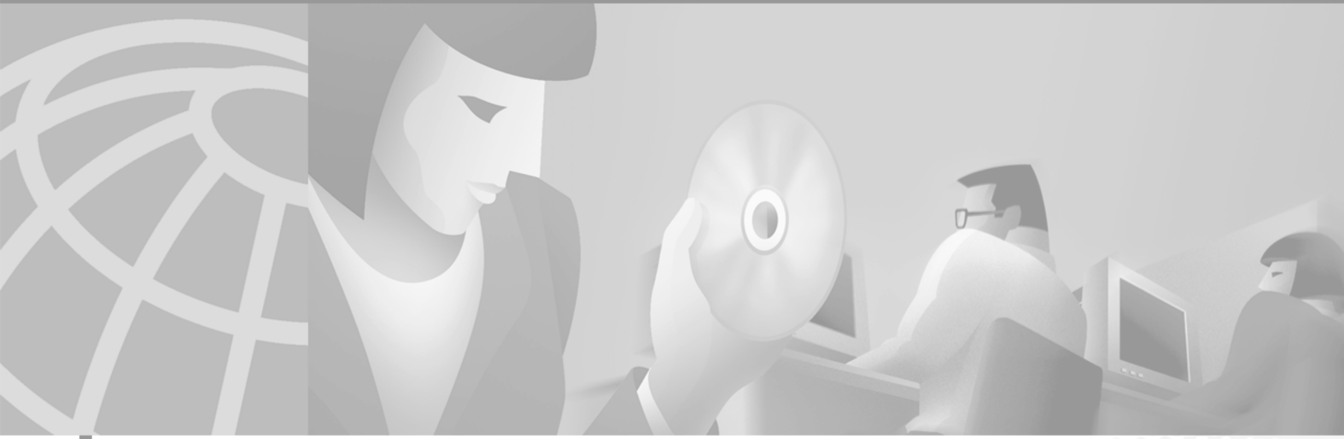
NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

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



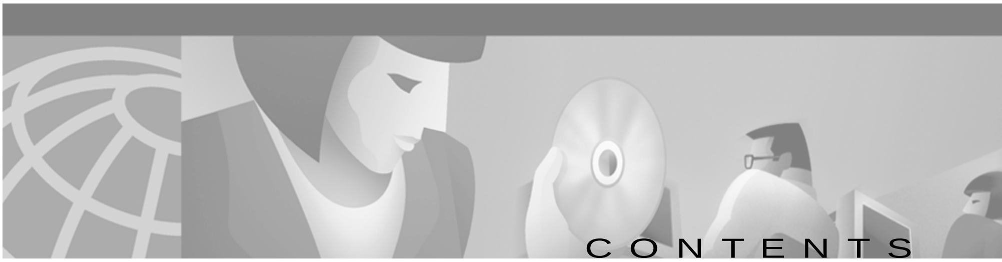
Cisco Internet CDN Software User's Guide

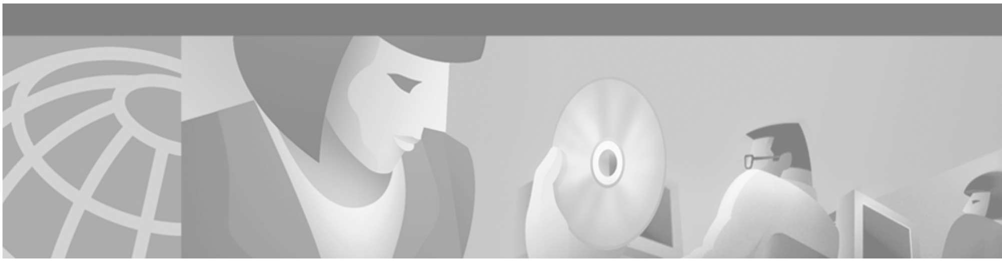
Version 2.1

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-7813576=
Text Part Number: 78-13576-01

Cisco Internet CDN Software User’s Guide


CONTENTS



Preface

This preface describes who should read the *Cisco Internet CDN Software User Guide*, how it is organized, and its document conventions.

This preface contains the following sections:

Document Objectives

This user guide describes how you use the Cisco Internet CDN Software to create and work with Content Delivery Networks (CDNs) to provide high-performance Internet content delivery services.

Before using this guide, you need to follow the instructions in the *Cisco Internet CDN Software Configuration Guide* for setting up your CDN devices.

Audience

This guide is intended for network administrators and content managers. The person responsible for managing the Content Distribution Manager, Content Routers, and Content Engines should be experienced with:

- IP network configuration
- Domain Name Server (DNS) configuration
- Oracle 8i installation and backup

Organization

This document is organized in the following manner:

Chapter	Title	Description
Chapter 1	Introduction to Cisco Internet CDN Software	Introduces Cisco Internet CDN Software.
Chapter 2	Creating Content Delivery Networks	Provides a tour of the software to give an overview of the key product features.
Chapter 3	Working with Cisco Internet CDN Software	Describes the user interface and the procedures you need to know to work with the software.
Chapter 4	Maintaining Cisco Internet CDN Software	Describes the use of the various system monitoring and maintenance features of the software.
Appendix A	Error and Event Messages	Describes the system messages you may encounter in your CDN system log and suggests actions for responding to each message.
Appendix B	Deploying SNMP on Content Delivery Networks	Describes the CISCO-CONTENT-NETWORK-MIB, SNMP traps, and using SNMP to monitor CDN device activity.
Appendix C	CDN Supported Time Zones	Provides a list of time zone abbreviations supported by Cisco Internet CDN Software. These abbreviations can be used when creating a CDN manifest file.

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.

Notes use the following conventions:

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

Related Documentation

The following documentation provides additional information about the Cisco Internet CDN hardware and software:

- *Cisco Internet CDN Documentation Roadmap*
- *Cisco Internet CDN Software Configuration Guide*
- *Cisco Internet CDN Software Command Reference*
- *Release Notes for Cisco Internet CDN Software Version 2.1*
- *Cisco Content Distribution Manager 4670 Product Description Note*
- *Cisco Content Engine 7320 Product Description Note*
- *Cisco Content Router 4450 Product Description Note*
- *Cisco Content Engine 500 Series Hardware Installation Guide*
- *Release Notes for Cisco Content Engine 500 Series Hardware Installation Guide*
- *Hardware Installation Guide for the Seven-Rack Unit Chassis*
- *Cisco Content Smart Switch Quick Configuration Guide*
- *Cisco Content Smart Web Switch Installation and Operation Guide*
- *Cisco Storage Array 6 Installation and Configuration Guide*
- *Release Notes for the Cisco Storage Array 6*
- *Cisco Storage Array 12 Installation and Configuration Guide*
- *Site Preparation and Safety Guide*
- *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

Introduction to Cisco Internet CDN Software

This chapter describes Cisco Internet CDN Software and tells you how to use your web browser to access the Cisco Internet CDN Software user interface.

This chapter contains the following sections:

About Cisco Internet CDN Software

Meeting the Needs of Internet Users and Service Providers

When end users experience technical problems the first time they go to a website, they often lose patience. Many users go to another site and never return to the original site.

The most basic technical problem that users encounter is slow content delivery. To help solve the problem of slow content delivery, Cisco Internet CDN Software enables you, the service provider, to create and maintain Content Delivery Networks (CDNs) for your customers, who are content providers. When content providers use CDNs, they benefit because end users can quickly and reliably access their content. You benefit because CDNs are a premium revenue-generating Internet service that you can offer your customers.

What a CDN Does

A Cisco Content Delivery Network (CDN) is a collection of hardware devices and proprietary software that, together, significantly improves the delivery of web content to users of the Internet

The Cisco Internet CDN allows web content to be distributed to caches at various locations on the Internet and then accessed from those caches. Service providers can ensure better access to their content because end users are able to obtain it from a cache that is both closer to them (in terms of network distance) and less heavily loaded than the web server where the content originates. In addition, these caches reduce the load on the web server belonging to the content provider where content originates (the origin server).

Hosted Domains

You can define one or more hosted domains for a content provider. From the perspective of a content provider, a hosted domain is a set of related content that the content provider wants to treat as a unit for the purposes of caching. All content for a hosted domain is stored on the same set of Content Engine caches.

For each hosted domain, a content provider must define an origin server, which is the Domain Name System (DNS) name of the web server where the actual content for that hosted domain is stored.

If live, video-on-demand, or pre-positioned content will be distributed from the hosted domain, an XML-format file, referred to as a *manifest* file, is also required. The manifest file identifies which live, video-on-demand, and static content on the origin server will be accessible from the hosted domain

From the perspective of an end user, a hosted domain is identified by its DNS name. The end user accesses content either by entering a URL in a web browser or by clicking a link on a web page. When the user requests content, the DNS server returns the IP address of a cache that is storing the requested content and the user receives the content. As a service provider, you must provide the authoritative DNS for each hosted domain that your customers, the content providers, will be using.

The Cisco Internet CDN Software routing system provides a way of translating a fourth-level hosted domain name into the IP address of a cache that stores content and is a good choice for the client making the request. The client can then send Hypertext Transfer Protocol (HTTP) requests directly to the selected cache. If the cache does not already contain the cached content, the cache obtains the content from the origin server for the requested hosted domain.

Alternatively, fourth-level hosted domain names can be mapped to valid third-level domain names using the hosted domain aliasing feature.

For more information, see the "Routing End User Requests to Content Engines" section on page 1-12.

Web Browser-Based User Interface

CDNs can change dynamically at runtime: new Content Engines can be added to the system, content providers come and go, new hosted domains are defined, and assignments of hosted domains to caches can change. The Cisco Internet CDN is designed to make it easy to handle such changes through interaction with the web browser-based Content Distribution Manager graphical user interface. It is not necessary to log on to particular nodes in the system to change what they do; instead, devices can be managed remotely through the Content Distribution Manager.

Security

The Cisco Internet CDN Software uses Secure Socket Layer (SSL) for Java to encrypt all interdevice communications.

Developed by Netscape, the SSL protocol is supported by both the Netscape and Microsoft browsers and is a widely accepted and deployed encryption technology on the Internet. SSL uses the sockets method of communication between client and server, coupled with RSA Security's public key encryption technology to secure data using digital certificates as it is transmitted between CDN devices over the Internet.

About Cisco Internet CDN Software Version 2.1

Version 2.1 of the Cisco Internet CDN Software extends the capabilities of earlier releases in several ways by:

- Support for Microsoft Windows Media Technologies (WMT) including support for ASF and ASX file formats
- Multiple login accounts with three separate login levels: administrator, operations, and guest
- Static- as well as dynamic routing of CDN content, providing administrators with fine control of request routing
- Secure transfer of log files to remote logging server
- Content-based security using Symmetric Key Content Authorization on a hosted domain-by-hosted domain basis

CDN Components

Cisco Internet CDN Software is preinstalled on three or, optionally, five types of hardware platforms from the Cisco CDN product line:

- Cisco Content Distribution Manager 4670 ICDN-K9
- Cisco Content Engine 590 ICDN-K9 or 7320 ICDN-K9 Series
- Cisco Content Router 4450 ICDN-K9
- Cisco Content Services Switch 11800 (optional)
- Cisco Catalyst 4000 Family or 5000 Family switch (optional)

In addition, an external Oracle 8i database is used.

Cisco CDN Devices

A CDN contains five types of Cisco devices:

- Content Distribution Manager
- Content Router
- Content Engine
- Content Services Switch (optional)
- Catalyst switch (optional)

A configuration of the system consists of 1 Content Distribution Manager, some Content Routers (2 to 8), and many Content Engines (up to 2000). Additionally, Content Engines can be grouped into clusters behind a Content Services Switch, forming *supernodes* that provide fault tolerance and load balancing for the hosted domains located on the clustered Content Engines.

Every device runs a Simple Network Management Protocol (SNMP) agent, allowing you to obtain information about the system through an SNMP console.

Content Distribution Manager

The Content Distribution Manager provides a central point of control for system administrators. A web browser-based graphical user interface makes it easy for administrators to perform system management such as adding and monitoring CDN devices and managing the CDN itself.

Using the Content Distribution Manager graphical user interface, administrators can perform actions including:

- Controlling content placement in the system (adding and removing content providers, adding and removing hosted domains, assigning hosted domains to Content Engines)
- Controlling the membership of the system (adding and removing Content Engines and Content Routers)
- Controlling the members of the system (upgrading software, rebooting Content Engines and Content Routers)
- Controlling the system configuration and changing system parameters, such as the partitioning and allocation of disk storage on Content Engines for pre-positioned video-on-demand and static content

The Content Distribution Manager uses an Oracle 8i policy database to store device configuration information and content serving policy information that you provide to it. For more information, see the "Oracle 8i Policy Database" section on page 1-9.

The Oracle 8i database belongs to you, the service provider. You are not required to use a separate database; the database can be used for your other database needs as well.

Content Router

A Content Router is a device that selects suitable Content Engines within a distribution network to serve end user requests. Content Routers redirect requests to an appropriate Content Engine based on geographic location, network location and conditions, and content placement. Content Routers are deployed to provide redundant configuration for multinetwork, wide-area fault tolerance and load balancing.

Content Routers send the Content Distribution Manager frequent "keepalive," or "heartbeat," messages that are used to determine which Content Routers in the system are down. You can view this information in the web-based user interface.

A CDN can contain between two and eight Content Routers. If a Content Router fails, DNS proxies that would have communicated with it begin communicating with another Content Router, and the system continues to function normally. When a Content Router is down, the load at other Content Routers is likely to increase, but Content Routers are able to handle a large number of DNS requests, so no performance problems should occur.

Content Engine

A Content Engine stores cached media. Content Engines are responsible for on-demand caching of static HTTP content and pre-positioned video-on-demand content, and for delivering content to end users. Content Engines provide access to content through HTTP, RealServer, and QuickTime and participate in routing under the direction of the Content Routers.

A CDN can have 1 or more Content Engines, up to a maximum of 2000.

Content Engines are located at the edge of the network (Internet service provider points of presence [ISP POPs]). Through the Content Distribution Manager graphical user interface, you control the distribution of content by assigning particular Content Engines to store the static and video-on-demand content of particular hosted domains. Only these Content Engines can store and serve this content. Although live, streamed content can also be delivered from hosted domains, by its very nature this content is not stored on Content Engines but delivered directly from the streaming server to the requesting client.

If a Content Engine fails, the routing subsystem routes around it for DNS requests. For example, a DNS proxy that has received the Content Engine in one of its name server records does not route to it because its probe message fails. Instead, it returns the IP address of some other Content Engine that it received in one of the other name server records sent to it.

In addition, Content Engines can be grouped into “clusters” behind Content Services Switches, which help manage user requests to the device using load balancing and which provide next-click failover if a Content Engine goes offline, meaning that if one Content Engine fails while trying to serve a user request, other Content Engines in the same cluster can be used to fulfill the user request.

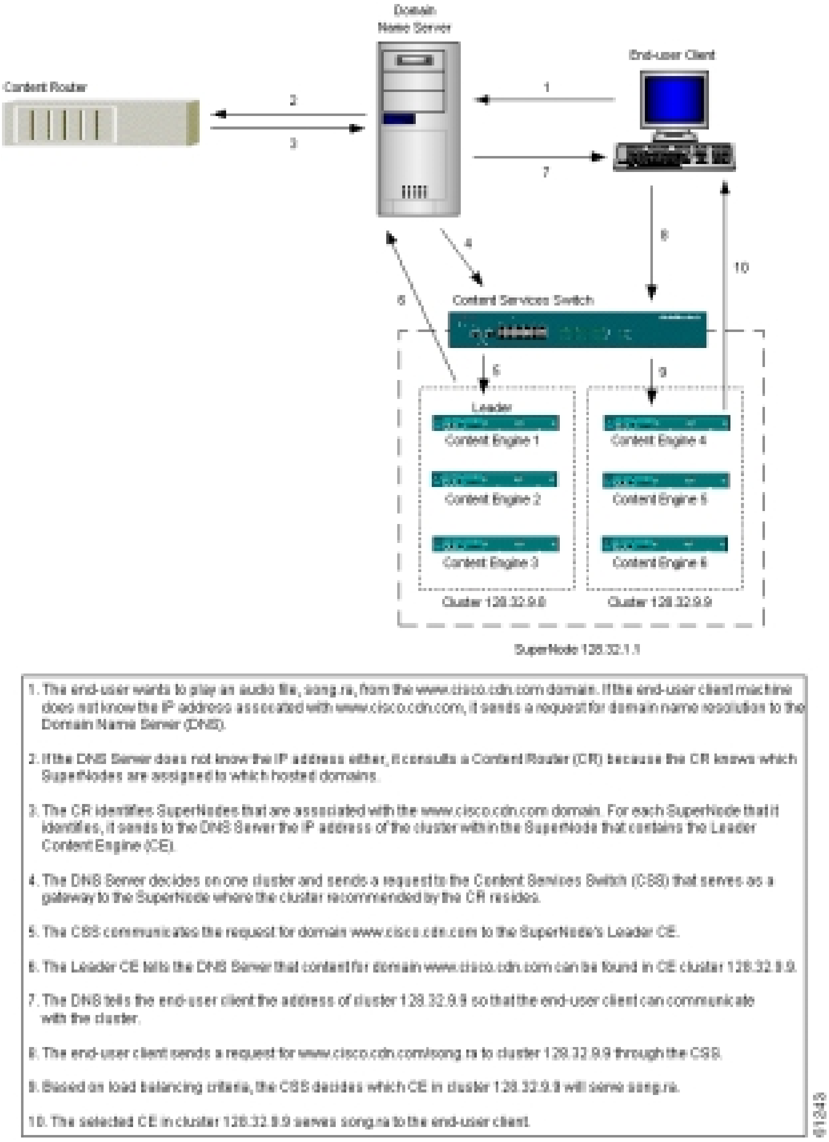
A Content Engine logs information about all the HTTP requests that it handles and can send this information to a remote logging site periodically. Using the Cisco Internet CDN Software web-based user interface, you can control both the identity of the site and the logging period. You can then use the information for billing content providers.

Content Services Switch

The Cisco Content Services Switch is an optional component of the CDN. When deployed, the Content Services Switch makes it possible to group (or cluster) Content Engines hosting the same content, and then to balance requests among the Content Engines and recover quickly should a Content Engine unexpectedly go offline.

Through the use of load-balancing technology and the fail-safe routing that detects problems with Content Engines and routes requests around them, the Content Services Switch can cut response time and improve the reliability of content delivery to customers accessing a particular hosted domain. Figure 1-1 shows how user requests are routed to a supernode.

Figure 1-1 Routing End User Requests to a Supernode



1. The end-user wants to play an audio file, song.ra, from the www.cisco.cdn.com domain. If the end-user client machine does not know the IP address associated with www.cisco.cdn.com, it sends a request for domain name resolution to the Domain Name Server (DNS).

2. If the DNS Server does not know the IP address either, it consults a Content Router (CR) because the CR knows which SuperNodes are assigned to which hosted domains.

3. The CR identifies SuperNodes that are associated with the www.cisco.cdn.com domain. For each SuperNode that it identifies, it sends to the DNS Server the IP address of the cluster within the SuperNode that contains the Leader Content Engine (CE).

4. The DNS Server decides on one cluster and sends a request to the Content Services Switch (CSS) that serves as a gateway to the SuperNode where the cluster recommended by the CR resides.

5. The CSS communicates the request for domain www.cisco.cdn.com to the SuperNode's Leader CE.

6. The Leader CE tells the DNS Server that content for domain www.cisco.cdn.com can be found in CE cluster 128.32.9.9.

7. The DNS tells the end-user client the address of cluster 128.32.9.9 so that the end-user client can communicate with the cluster.

8. The end-user client sends a request for www.cisco.cdn.com/song.ra to cluster 128.32.9.9 through the CSS.

9. Based on load balancing criteria, the CSS decides which CE in cluster 128.32.9.9 will serve song.ra.

10. The selected CE in cluster 128.32.9.9 serves song.ra to the end-user client.

Supernode

A supernode is a collection of Content Engines clusters grouped behind a Content Services Switch and joined to a CDN.

As opposed to standalone Content Engines (referred to as standalone nodes), supernodes make it possible to provide improved response time for user requests through the use of load balancing among clusters of Content Engines hosting the same content.

In addition, supernodes provide data redundancy and next-click failover, meaning that if one Content Engine fails while trying to serve a user request, other Content Engines in the same cluster can be used to fulfill the user request.

Cluster

Clusters are groups of Content Engines hosting identical content and grouped behind a Content Services Switch. Grouping Content Engines into clusters allows content providers to better service end user requests with the load balancing and next-click failover features of the Content Services Switch.

Oracle 8i Policy Database

The Content Distribution Manager uses an external Oracle 8i database to store current CDN policies. The term “policies” refers to the information that you provide to the Content Distribution Manager using its graphical user interface. The database also stores information about CDN use and CDN status.

Because the database provides persistent storage, modifications you make are not lost in system failures. Because the database also provides transaction processing, modifications that consist of several changes are certain to occur either completely or not at all.

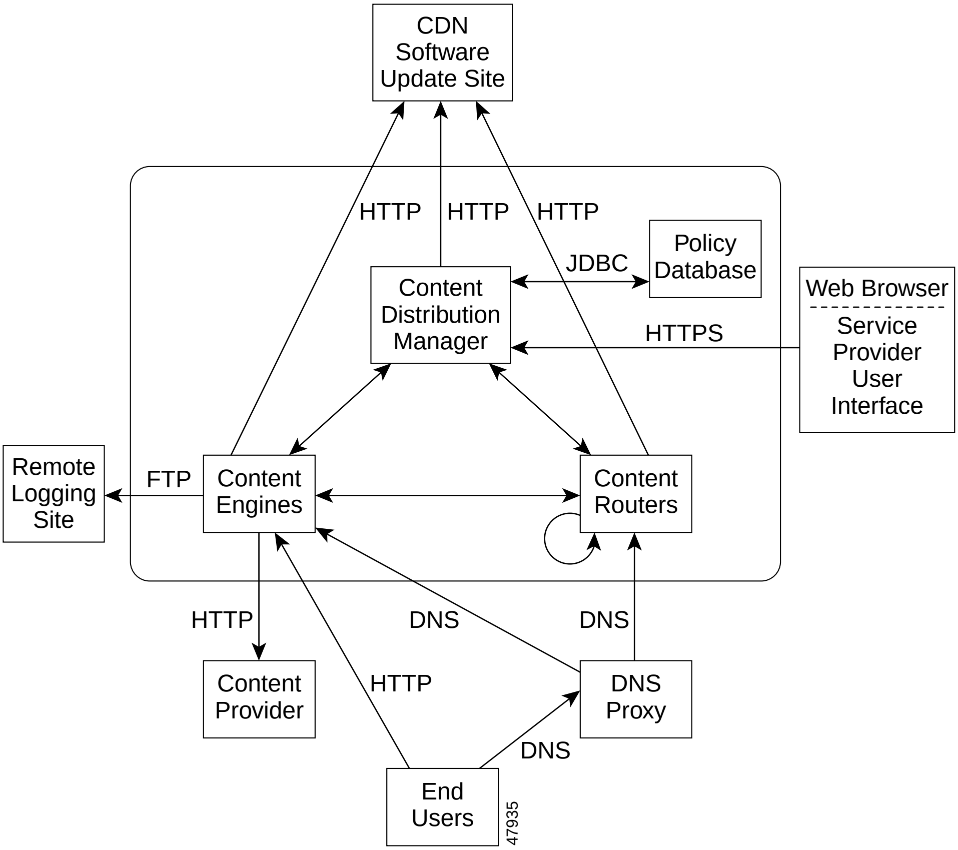
The Oracle database management system does not come with Cisco Internet CDN Software. You use an Oracle 8i database management system from Oracle, create the database, and configure it. For information about configuring the database, refer to the *Cisco Internet CDN Software Configuration Guide*.

Because the Oracle policy database is an integral part of your CDN, you the service provider should also develop formal procedures for backing up the CDN policy database, and a schedule according to which backups will take place once your CDN is online.

CDN Architecture

Figure 1-2 shows CDNs in the context of a larger network that includes origin servers, clients, DNS servers, and other sites.

Figure 1-2 Content Delivery Network Architecture



In addition to what is shown in Figure 1-2, each Cisco device (Content Distribution Manager, Content Engines, and Content Routers) runs an SNMP agent and servers for Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS), which allow administrators to query individual devices securely with a variety of tools.

CDN Terminology

Table 1-1 defines terms that you need to know when you work with CDNs.

Table 1-1 Content Distribution Network Terms

Action	Description
Content Delivery Network (CDN)	Coordinated network of devices (Content Engines, Content Distribution Manager, Content Routers, and Content Services Switches) that cache content for end users.
Service provider	Cisco customer that provides the infrastructure for a CDN.
Content provider	Service provider customer that deploys content on a CDN.
Hosted domain	Set of content to be cached on a CDN, defined by a DNS name.
Origin server	Web server that serves the original content from a content provider for a hosted domain.
Content Distribution Manager	Cisco device that administers a CDN, gathers statistics, and provides a management user interface that you can access using your web browser.
Content Engine	Cisco device that caches content for a CDN and satisfies HTTP requests from end users.
Content Router	Cisco device that routes requests for content in a CDN by means of DNS records.
Content Services Switch	Optional device that serves as the public interface for groups (or “clusters”) of Content Engines located behind it. Requests for content are received by the Content Services Switch and passed on to the Content Engine that is best suited to serve the request.

Routing End User Requests to Content Engines

A Cisco CDN can contain up to 2000 Content Engines distributed across a geographically dispersed area. In such an environment, it is vital that client requests for cached content be handled by Content Engines that are suitable for the client, which means that they are online, nearby, and cheap to communicate with. The selected Content Engines must also be authorized to store the requested content (the hosted domain). Thus, the job of the routing subsystem is to choose the most suitable Content Engines to handle a particular client request.

Cisco Internet CDN Software does routing as part of the DNS lookup that occurs when a client machine does not know the IP address associated with a particular DNS name (a hosted domain). The client communicates with a DNS proxy, which either knows how to route the client request to a Content Engine (because of prior communication with one of the Content Routers) or communicates with one of the Content Routers. The Content Routers act as authoritative DNS servers for the hosted domains served by Cisco CDNs. Modifications are not needed for the software running on clients, DNS proxies, other servers within the DNS system, or the content provider servers.

When a client request arrives at a DNS proxy that does not know how to translate the requested DNS name, the proxy consults other DNS servers on the Internet. Normal DNS mechanisms lead the proxy to communicate with one of the Content Routers in the CDN. The Content Router then chooses Content Engines that are suitable for the client request. It returns information about the selected Content Engines to the DNS proxy in the form of name server (NS) records.

Each record identifies a Content Engine that can cache the desired content. The Content Router also returns address (“glue”) records for the Content Engines so that the DNS proxy knows the IP addresses of the Content Engines.

Several NS records are sent in the reply. The number of records returned and the length of time that they can be used by the proxy (the Time To Live, or TTL value) are controlled by the Content Router. The Content Router adjusts these values depending on how confident it is that its choices are suitable. For example, if the Content Router is certain that particular Content Engines are appropriate for the client, then just two or three name server records are provided to the DNS proxy, with relatively long Time To Live values. If, however, the Content Router is uncertain about which Content Engines can best provide the requested content, then up to eight name server records are provided to the DNS proxy, with relatively short Time To Live values.

The Content Routers make their decision based on the IP address of the DNS proxy that sends the request. The routing subsystem is based on the assumption that choices which are suitable for a DNS proxy are also suitable for the client which is using the proxy to resolve the DNS name.

When this assumption is not appropriate, the CDN administrator has the option of enabling static routing. See the "Static Routing" section on page 1-15.

End Users Requesting Content

When an end user client machine needs to access content in a hosted domain served by a Cisco CDN, the client communicates with a local DNS proxy if it does not already have an IP address of a Content Engine. If the proxy also does not know how to route the hosted domain, it communicates through normal DNS mechanisms with one of the Content Routers.

Routing a Request

Routing a request is a two-step process. The first step is communication between the DNS proxy and a Content Router, and the result is a number of name server records with associated Time To Live values. The second step occurs at the DNS proxy, which contacts the Content Engine identified in one of the returned records. The contacted Content Engine replies with an actual IP address used by its supernode in the form of an address (A) record. When the DNS proxy receives a response from the contacted Content Engine, the DNS proxy returns the IP address provided by that Content Engine to the requesting client. If the DNS proxy receives no response, it tries another Content Engine (one listed in one of the other name server records). The record has a very short Time To Live value (20 seconds), so the DNS proxy continues to probe the Content Engines in the name server records for subsequent requests.

If the DNS proxy receives subsequent requests for the same DNS name before the Time To Live values on the name server records expire, it continues to contact the Content Engines identified in the name server records it has already received. Returning several name server records to the DNS proxy allows the DNS software to fine-tune the response to the client, recording which servers respond most quickly and directing future requests to those servers. All name server records identify appropriate Content Engines for the client request, so returning several name server Content Engine records provides additional fault tolerance and load balancing; the DNS proxy does not select a Content Engine that fails to reply, and if several Content Engines are equally close to the DNS proxy, it cycles through them.

Routing Decisions

The success of the routing decisions depends on what happens at the Content Routers, since this outcome controls which Content Engines are ultimately selected. The Content Routers base their decisions on a database of proxy tables that contain information about the proximity of Content Engines to particular DNS proxies. Each proxy table actually stores information for a group of proxies, which provides a way of keeping the number of proxy tables under control. All proxies in a group are considered to be nearby one another; proxies with IP addresses that agree in the most significant 24 bits are considered to be in the same group.

A proxy table ranks the appropriateness of locations for the proxy group. A location contains a number of Content Engines that are geographically nearby, for example at a single POP or a closely related group of POPs. Storing information for locations rather than individual Content Engines enables control of the size of the tables. Cisco Internet CDN Software allows a maximum of 192 locations. Content Engines are assigned to locations when they are first added to a CDN.

The proxy tables are maintained automatically. Periodically, a Content Router directs certain Content Engines to communicate with particular DNS proxies. Only one Content Engine per location is asked to do these probes. This Content Engine is the leader of the location. Leaders communicate with the specified proxies by pinging them. If ping messages fail, leaders send the proxies DNS requests, compute the time taken to complete the exchange, and send the collected information back to the Content Routers. The Content Routers then update their proxy tables using the new information.

Data collection for routing occurs during each routing period, approximately every 2 minutes. All leaders communicate with all Content Routers during each routing period to report their probe results. The reply to the communication gives the leader its probe instructions for the next period.

Standalone Content Engines and supernode leaders also communicate with the Content Routers during each routing period. This communication provides a list of the hosted domains that a Content Engine or supernode is authorized to serve. Content Routers use this information to ensure that Content Engines are selected that are authorized to serve the requested content. If the Content Routers do not receive this information from a Content Engine, they conclude that this Content Engine is not currently serving content.

Since Content Engines communicate with all Content Routers in each routing period, location leaders carry out probe requests chosen by all the Content Routers, and the Content Routers learn the results of all the probes, even those requested by different Content Routers. The communication is not synchronized, and therefore it is possible that the proxy tables at different Content Routers may diverge. Divergence is not a serious concern, however, because routing depends only on having reasonably accurate information, and it does not matter that different Content Routers might make different decisions.

Additionally, the communication from Content Engines to Content Routers is offset in time. The goal is to have the communication occur evenly across the routing period, so that Content Routers do not become overwhelmed with the communications from the Content Engines.

Static Routing

The preceding discussion of CDN routing explains the way that the Cisco Internet CDN software takes advantage of DNS in routing end user requests to Content Engines through Content Routers, which choose from among the Content Engines or supernodes hosting the content being requested, selecting those that are close to the requesting client. In conventional CDN routing, sometimes called *dynamic routing*, the IP address of the DNS proxy making the request is used to make an approximation of the location of the actual requesting client.

Given a configuration in which the DNS proxy is not in close proximity to the requesting client, however, dynamic routing may assign the task of serving a user request to a Content Engine that is not close to the source of the request—even when a better positioned Content Engine hosting that content exists on the CDN. Particularly when serving live or video-on-demand content, this discrepancy could affect the quality of the served content.

Cisco Internet CDN Software provides a way for content providers to adjust for such irregularities in their network topography through *static routing*. Using static routing:

- Each location in a CDN is assigned to a coverage zone, a set of address ranges that it is well positioned to serve.

- DNS proxies from which requests should be specially handled are identified.
- End user (client) machines are mapped to the CDN Content Engines (based on location) that are well positioned to serve them

Coverage zone information is provided in a special text file, maintained on a machine controlled by the content provider. This file is fetched and periodically updated on each Content Router and Content Engine on the CDN.

With coverage zones deployed, the CDN software can use a combination of both dynamic and static routing, referred to as *hybrid routing*. Using hybrid routing, DNS proxy requests are compared by the Content Router against the list of DNS proxies in the coverage zone file.

- If the DNS proxy is not listed in the coverage zone file, the request is processed using standard CDN routing.
- If the DNS proxy is listed in the coverage zone file, the Content Router chooses, at random, one or two supernodes which host the requested content and which are in locations listed in the coverage zone file. The Content Router then returns these addresses to the DNS proxy in the form of NS records. The DNS proxy then communicates with the supernodes and chooses which supernode to use, passing its address back to the requesting client's browser.

When the selected Content Engine receives the request from the client, it determines whether it is best situated to serve the request, consulting the coverage zone information to determine if it is identified as a well-situated Content Engine for this client.

- If the Content Engine is well situated, it serves the request.
- If the Content Engine finds that it is not well situated to the end user, it generates a redirection response to the Content Router. The host name in this response encodes the address of the client.

The Content Router then makes a selection from the supernodes hosting the requested content that are in the locations identified in the coverage zone file, starting with those locations identified as "best" and "second-best" locations for the client's IP address, and continuing on to all locations identified in the coverage zone file for that IP address, if necessary.

For information on specifying a coverage zone file for your CDN and setting other dynamic and static routing parameters, see the "Modifying Routing Properties" section on page 4-25.

Importing and Pre-Positioning Content

In order to be able to serve pre-positioned content and live, streamed media, Cisco Internet CDN Software Version 2.1 uses an XML-based manifest file to identify live content versus static or pre-positioned video-on-demand content on the origin servers of the content provider. This is in contrast to earlier versions of the software, in which content was cached on Content Engines based on hosted domain records received from the Content Distribution Manager.

The manifest file serves as a roadmap for all content that will be imported to a content provider's hosted domain and stored on the Content Engines hosting the hosted domain.

For instructions on creating manifest files, see the "Creating a Manifest File for Importing Media" section on page 2-3. For instructions on importing the content named in the manifest file, see the "Creating a Hosted Domain for a Content Provider" section on page 2-49 or "Working with Hosted Domains" section on page 3-34.

Supported Content Types

Cisco Internet CDN Software supports any standard static content type. In addition, the CDN supports live streaming and video-on-demand delivery of the following file formats:

- Audio Visual Interleaved (AVI)
- Graphics Interchange Format (GIF)
- Hypertext Markup Language (HTML, HTM)
- Joint Photographic Experts Group (JPG)
- Microsoft PowerPoint (PPT)
- Microsoft Windows Media Player (ASF and ASX)
- Microsoft Windows Media Audio (WMA)
- Microsoft Windows Media Video (WMV)
- Microsoft Word (DOC)
- Motion Picture Experts Group (MPEG, MPG)
- MPEG Audio Layer 3 (MP3)

- Portable Document Format (PDF)
- QuickTime (QT)
- QuickTime Movie (MOV)
- RealAudio (RA)
- RealMedia (RM)
- RealPix (RP)
- RealText (RT)
- RealVideo (RV)
- RealNetworks synchronized container format (SMIL)

CDN Users

Cisco Internet CDN Software has three types of users:

- CDN administrators
- CDN operations-level users
- CDN guests

Table 1-2 describes user access privileges for the various Cisco Internet CDN Software features.

Table 1-2 User Access Privileges to CDN Features

Internet CDN Software Feature	Admin	Operations	Guest
Hosted domains	Edit	Edit	View
Content providers	Edit	Edit	View
Virtual CDNs	Edit	Edit	View
Content Engines	Edit	View	View
Content Routers	Edit	View	View
Clusters	Edit	View	View
Supernodes	Edit	View	View

Table 1-2 User Access Privileges to CDN Features (continued)

Internet CDN Software Feature	Admin	Operations	Guest
Regions	Edit	View	View
Locations	Edit	View	View
System passwords	Edit	Hidden	Hidden
Remote logging	Edit	View	View
Software update	Edit	Hidden	Hidden
System logs	View	View	View
Content Engine statistics	View	View	View
DNS properties	Edit	View	View
QuickTime configuration	Edit	View	View
RealServer configuration	Edit	View	View
SNMP configuration	Edit	View	View
System configuration	Edit	Hidden	Hidden
Windows Media Server configuration	Edit	View	View
Content Services Switch	Edit	View	View
Simple peek	Edit	Hidden	Hidden
Login password administration	Edit	Edit	Edit

CDN Administrators

CDN administrators use Cisco Internet CDN Software to create CDNs. For example, administrators add new hosted domains, oversee content import, and remove Content Engines from the network.

Administrators interact with CDN devices using the web browser-based graphical user interface to the Content Distribution Manager. The Content Distribution Manager provides web pages that make it easy to perform administrative functions, and uses Hypertext Transfer Protocol Secure (HTTPS) to protect communications between itself and CDN devices.

For example, a CDN administrator controls:

- Access—By adding, removing, and modifying user login accounts
- Content—By adding and removing content providers, adding and removing hosted domains, and assigning hosted domains to Content Engines
- Membership—By adding and removing Content Engines and Content Routers
- Members—By upgrading software and rebooting Content Engines and Content Routers
- Configuration—By changing system parameters, such as the frequency of various kinds of communication among the members of the system

When an administrator uses the web-based user interface to enter new information, the Content Distribution Manager validates the new information, adds it to the policy database, propagates changes to the Content Engines and Content Routers, and examines the system state.

See Table 1-2 for an overview of administrator account access privileges for each feature on the Cisco Internet CDN Software graphical user interface.

CDN Operations-Level Users

CDN operations-level users can create, modify, and delete hosted domains, virtual CDNs, and content providers, but cannot modify other system components, update CDN software, modify system configuration, or change device passwords.

Operations-level users interact with CDN devices using the web browser-based graphical user interface to the Content Distribution Manager. The Content Distribution Manager provides write-level access to only those web pages that contain features for creating and modifying hosted domains, virtual CDNs, and content providers. In addition, operations-level users have access to the Login Password Administration page, from which they can change their own login password. See the "Changing the Login Account Password" section on page 1-27 for information on using the login password administration feature.

Other information available to administrator-level accounts can be viewed but not edited. Certain administrative features are hidden from operations-level users.

See Table 1-2 for an overview of operations account access privileges for each feature on the Cisco Internet CDN Software graphical user interface.

CDN Guests

CDN guest-level users can view CDN device configuration, including configuration settings for hosted domains, virtual CDNs, and so on, but they cannot modify the CDN or any of its components in any way.

Guest-level users interact with CDN devices using the web browser-based graphical user interface to the Content Distribution Manager. The Content Distribution Manager provides read-only access to those web pages that contain information on hosted domains, virtual CDNs, and content providers. In addition, guest-level users have access to the Login Password Administration page from which they can change their own login password. See the "Changing the Login Account Password" section on page 1-27 for information on using the login password administration feature. Other features available to administrator-level accounts are hidden from guest-level users.

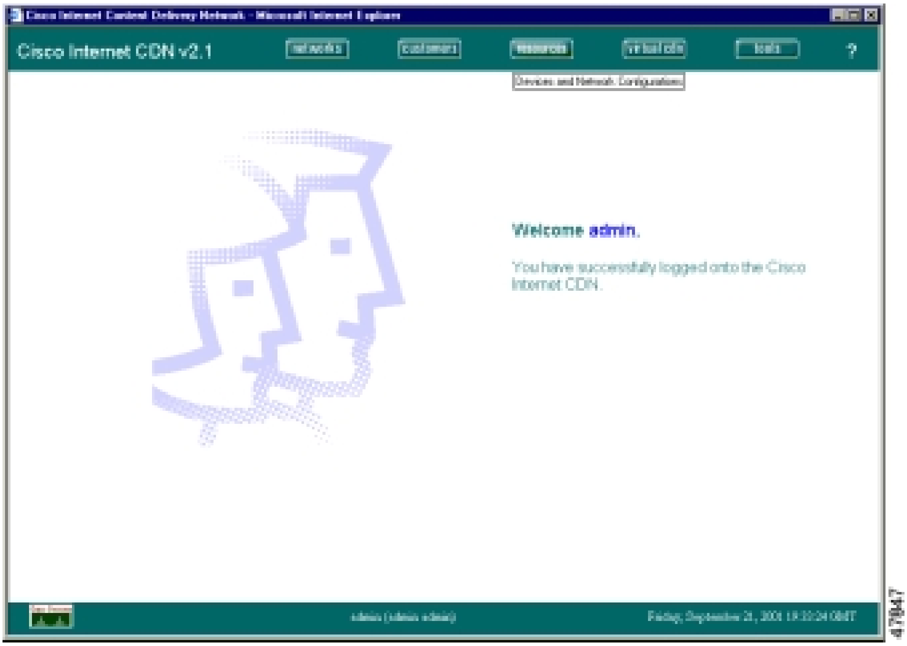
See Table 1-2 for an overview of guest account access privileges for each feature on the Cisco Internet CDN Software graphical user interface.

About the Cisco Internet CDN Software User Interface

A CDN is a constantly changing system. Content Engines and Content Routers are added and removed. Content providers come and go. New hosted domains are defined, old ones are removed, and assignments of Content Engines to hosted domains and virtual CDNs change; the Cisco CDN software may need updating and devices may need to be rebooted.

Changes to your CDN are managed using a web browser-based management interface that is part of the Content Distribution Manager. (See Figure 1-3.)

Figure 1-3 Internet CDN Software User Interface


Cisco Internet Content Delivery Network - Microsoft Internet Explorer
Cisco Internet CDN v2.1
networks
customers
resources
virtual cdn
tools
?
Devices and Network Configuration
admin (admin admin)
Friday, September 21, 2001 18:33:24 GMT
47047

Welcome admin.

You have successfully logged onto the Cisco Internet CDN.

The Content Distribution Manager is a central location from which much of the work of creating and managing CDNs and hosted content can be controlled. All modifications made through the Content Distribution Manager are added to the Oracle policy database and then propagated to the Content Routers, Content Engines, and Content Services Switches that make up your CDN.

Table 1-3 describes the five primary groups of features associated with the Content Distribution Manager user interface:

Table 1-3 Content Distribution Manager User Interface Features

Content Distribution Manager Feature	Description
Networks	Lets you view, modify, and create new regions and locations. These geographical designations are used to group your CDN devices.
Customers	Lets you view, modify, and create new content provider accounts. Content providers are the organizations that will be hosting content on your CDN using hosted domains. You track contact and billing information for each content provider.
Resources	Manages and configures your CDN devices such as Content Engines, Content Routers, hosted domains, and so on.
Virtual CDN	Lets you view, modify, and create new virtual CDNs. Virtual CDNs provide you with a way to flexibly group Content Engines, apart from (or in addition to) their geographic region and location. For example, you could group CDN devices according to their hardware type (Content Engine 590 ICDN-K9 models and Content Engine 7300 ICDN-K9 models).
Tools	Performs a variety of configuration and system monitoring activities. You can view device performance, configure playservers, and update your Cisco Internet CDN Software.
Help (?)	Provides help on the current page.

Content Distribution Manager Icons

The Content Distribution Manager uses status icons for required fields, password field validation, and access to device configuration features. The icons you may see on the Content Distribution Manager user interface are shown in Table 1-4.

Table 1-4 Content Distribution Manager User Interface Icons

Status Icon	Description
*	Required field. The designated field must be filled in before you click **Save**.
📝	Edit. Click this icon to access the Modify [item] page, displaying information and configuration options for the selected CDN component.
⚠	Error. Data was not entered, or invalid data was entered in the field. Place the cursor over the symbol message to view error text.
✔	Valid password. The password value you entered was accepted by the system. Your new password values take effect immediately.
⚙	System tools. Click this icon to access the System Tools dialog for the selected device. The System Tools dialog contains advanced configuration options for CDN devices.
Save	Saves changes you have made to the current CDN component and returns you to the View [item] page. For example, after making changes to a Content Engine location and region, click **Save** to commit your changes and return to the View Content Engines page.
Cancel	Returns you to the View [item] page without committing any configuration changes.

When problems arise with data entered into the Content Distribution Manager user interface, error messages are displayed for each problem field, on popup windows and in the footer area of the Content Distribution Manager user interface. These error messages help identify the source of problems and speed problem resolution.

To resolve the errors, hold the mouse cursor over each field-level error indicator. Error text will appear in a "tool tip" above the mouse cursor. Make any necessary adjustments to the format of the data you are entering and click the **Save** button. See the "User Interface Errors" section on page A-1 for more information on resolving errors on the CDN software graphical user interface.

Logging On to the Content Distribution Manager User Interface

All functions related to managing your CDNs are done using the web browser-based management interface that is installed on the Content Distribution Manager.

To access the Content Distribution Manager user interface from your workstation, follow these steps:

Step 1 In your web browser, enter the URL or IP address for the Content Distribution Manager. For example, enter the URL:

https://*Name_of_Content_Distribution_Manager*

Alternatively, enter the IP address:

https://*IP_address_of_Content_Distribution_Manager*

If you are prompted to accept the server certificate, click **Yes**.

A request for a username and password appears.

Step 2 Enter your username and password.

```
User name: admin
Password: <password>
```

Note The default username is **admin** and the default password is **default**. If the defaults have been changed by another Content Distribution Manager administrator, you need to get the new username and password.

Step 3 Click **OK**.

Logging On Following Session Timeout

The Content Distribution Manager web interface is equipped with a timeout feature that terminates idle sessions after a set amount of time. See the "Modifying the System Timeout Value" section on page 4-56 for instructions on changing the length of time that must pass before your session times out.

When a session has timed out, you immediately lose access to the Content Distribution Manager web interface, which is replaced with a message informing you that "this session has expired.

To log back on to the Content Distribution Manager:

Step 1 Close all web browser windows that were used to access the Content Distribution Manager by clicking the **Close** button to close the active window, or click the **File** menu and choose **Close** or **Exit**.

Note Often when you log on to the Content Distribution Manager, the web interface is loaded into a separate instance of the web browser from the one used to point to the Content Distribution Manager URL. Make sure that both instances of the browser are terminated before attempting to log back on to the Content Distribution Manager.

Step 2 Open a new instance of your preferred web browser and point it to the URL of your Content Distribution Manager. You are prompted to log on to the Content Distribution Manager web interface.

Changing the Login Account Password

Regardless of your level of access (administrator, operations, or guest), you can update the login password of the account you are currently using. You should periodically change your login password to reduce the likelihood that unauthorized users will be able to use your login and password to access CDN data.

To change your login account password:

Step 1 From the Cisco Internet CDN Software user interface, click **tools**.

The View Content Engine Statistics page appears.

Step 2 From the drop-down list, choose the **Login Password Administration** option.

The Login Password Administration page appears, listing the name of the current login account.

Step 3 In the Old Password field, enter your current login password. You must be able to provide the current password before updating the login password.

Step 4 In the New Password field, enter your new password. Passwords should be eight characters long.

Step 5 In the Re-type New Password field, reenter your new password to verify the value that you entered. The value entered here must match the value that you entered in the New Password field, or you will not be allowed to update the login password.

Step 6 Click **Save**. The account’s login password is updated and you are returned to the Login Password Administration page.

Exiting the Content Distribution Manager User Interface

When you have finished managing your CDNs, you exit the user interface.

To exit the Content Distribution Manager user interface, follow these steps:

Step 1 Save any changes you made, or cancel the changes.

Step 2 From the **File** menu, choose **Close**, or click the browser **Close** button.

Creating Content Delivery Networks

A Content Delivery Network (CDN) is a coordinated system made up of three types of machines: a Content Distribution Manager, a Content Engine, and a Content Router. Optionally a fourth element, the Content Services Switch, may be implemented and used to group Content Engines into supernodes, providing next-click failover for cached content.

The first step in setting up a CDN is to unpack and properly configure your hardware devices and CDN database by following the instructions in the hardware documents that shipped with the devices, as well as the *Cisco Internet CDN Software Configuration Guide.*

Once the hardware devices and database that make up your CDN are properly installed and configured, you are ready to use the information contained in this chapter to organize those devices into a CDN that is capable of serving pre-positioned or live media to end users.

This chapter contains the following sections:

- Before Setting Up CDNs, page 2-2
- Setting Up a CDN, page 2-3
- Creating User Accounts, page 2-65

Before Setting Up CDNs

To set up a CDN, you need to define:

- Your content in the form of URLs that point to pre-positioned content and live streamed content on one or more origin servers
- Your customers (the content providers that will be using the Internet CDN product to help deliver media to end users)
- Regional groupings for your Content Engines, Content Engine clusters, and Content Routers
- Locations (smaller, local groupings within regions that organize Content Engines and Content Routers)
- Supernodes and Content Engine clusters (only if using a Content Services Switch)
- Hosted domains (the content which is cached on one or more Content Engines or clusters and which is delivered by content providers to end users)
- Virtual CDNs (user-defined groupings of Content Engines and clusters)

The following sections describe how to define and configure these various elements.

The order in which topics are presented in this document is designed to minimize possible conflicts or confusion. Although the Content Distribution Manager does not require you to follow a specific order when setting up your CDN, certain tasks need to be performed before others. For example, because a location must have an associated region, information on defining regions is presented before information for defining locations. Because Content Engines and Content Routers must be placed in locations, you define these devices after you define locations.

Setting Up a CDN

In each Cisco Internet CDN, content is imported to hosted domains from web-based origin servers associated with a particular third-level domain name, for example:

```
http://www.cisco.com
```

Each hosted domain is associated with a specific content provider and corresponds to a particular collection of live and pre-positioned video-on-demand content being distributed on the CDN. Content providers may have one or more hosted domains on a CDN at a time.

After they are created, hosted domains are associated with one or more Content Engines that cache the pre-positioned content that has been copied (or *replicated*) from the origin server. This content is then used to serve user requests.

These sections detail the steps that must be taken to set up your Cisco Internet CDN.

Creating a Manifest File for Importing Media

Although each hosted domain is mapped to a single origin server when it is created, the Cisco Internet CDN actually allows content to be pulled from multiple servers and placed on a hosted domain. In order to be able to map content from more than one location and to filter and configure media that is placed on a hosted domain, an Extensible Markup Language (XML)-based reference file called the *manifest file* is used.

About the Manifest File

The manifest file, which is linked to the hosted domain using the Content Distribution Manager user interface, allows you to define a series of servers from which content can be fetched, as well as a list of content items on each server to be fetched.

Written in XML, a finished manifest file contains a series of URLs pointing to live and pre-positioned content from the various origin servers.

Each hosted domain is associated with a single manifest file.

Because XML files, like HTML files, are simple text-format files that use special tags to designate how content is to be handled and represented on the web, it is possible to create manifest files using any ASCII text editor. A variety of third-party XML authoring tools also exist, and may speed the process of generating manifest files.

This section explains the structure of the XML-based manifest file. In the manifest file syntax examples that follow, note the capitalization and data formats used. In order for your finished manifest file to work, your XML tags and tag attributes must use the format outlined in this document. Errors in capitalization on a tag or tag attribute, or incorrectly formatted data will result in errors.

After you are comfortable with its structure and the various methods for generating a manifest file, see the "Creating a Hosted Domain for a Content Provider" section on page 2-49 for instructions on creating a hosted domain and pointing it to a manifest file that names content you wish to bring in to your CDN.

Manifest File Structure and Syntax

The Cisco Internet CDN manifest file is an XML-based file that provides powerful features for representing and manipulating CDN data, while remaining comprehensible and easy for CDN administrators to edit manually using any text editor. Example 2-1 provides type definitions for the various elements of an Internet CDN manifest file. Details on each manifest file element follow.

Example 2-1 Manifest Document Type Definitions (DTDs)

```
<!-- CdnManifest DTD-->
<!ENTITY % playServerTable SYSTEM "PlayServerTable.dtd">
%playServerTable;
<!ELEMENT CdnManifest playServerTable?, options?, server*,(item | item-group)*)>
<!ELEMENT options EMPTY>
<!ATTLIST options
clearlog (true | false) "false"
noRedirectToOrigin (true | false) "false"
timeZone CDATA #IMPLIED
manifest-id #IMPLIED
>
<!ELEMENT host EMPTY>
<!ATTLIST host
name CDATA #REQUIRED
proto (http) "http"
port CDATA #IMPLIED
user CDATA #IMPLIED
password CDATA #IMPLIED
>
<!ELEMENT server (host+)>
<!ATTLIST server
name CDATA #REQUIRED
>
<!ELEMENT contains EMPTY>
<!ATTLIST contains
cdn-url CDATA #REQUIRED
>

<!ELEMENT item (contains*)>
<!ATTLIST item
cdn-url CDATA #IMPLIED
src CDATA #REQUIRED
server CDATA #IMPLIED
playserver (real | http | qtss | wmt) #IMPLIED
type (prepos | live) #IMPLIED
ttl CDATA #IMPLIED
serve CDATA #IMPLIED
prefetch CDATA #IMPLIED
expires CDATA #IMPLIED
alternateUrl CDATA #IMPLIED
noRedirectToOrigin (true | false) #IMPLIED
>
<!ELEMENT item-group (item | item-group)*>
<!ATTLIST item-group
server CDATA #IMPLIED
playserver (real | http | qtss | wmt) #IMPLIED
```

```
type (prepos | live) #IMPLIED
ttl CDATA #IMPLIED
alternateUrl CDATA #IMPLIED
cdnPrefix CDATA #IMPLIED
srcPrefix CDATA #IMPLIED
noRedirectToOrigin (true | false) "false"
>
```

<CdnManifest> </CdnManifest>

The <CdnManifest> tag marks the beginning and end of the manifest file content. At a minimum, each <CdnManifest> tag set must contain at least one item that will be fetched and stored on the hosted domain, and may optionally reference a list of host servers from which content will be fetched. (See Example 2-2.)

Any number of servers, hosts, and items can be defined, up to a limit of 10,000 items in the manifest file.

Example 2-2 CdnManifest Tag

```
<CdnManifest>
<playServerTable> ... </playServerTable>
<options ...>
<server ...>
    <host.../>
</server>
<item> ... </item>
</CdnManifest>
```

<playServerTable> </playServerTable>

Playserver tables provide a way for you to set default mappings for a variety of media types on your hosted domains. Mappings can be set for both MIME content types (the preferred mapping) and file extensions. Playserver tables allow you to override default mappings on the Content Engine for content types on a particular hosted domain.

Using the manifest file, you can map groups of content items as well as individual pieces of content to an installed playserver. Playserver mappings can be made at the following locations (listed in order of precedence):

- Content item URL—Playserver mappings appear right after the hosted domain name in place of the default cdn-media tag.
- In the manifest file as an attribute of the <item> or <item-group> tags—Playserver mappings placed here are identified using the playserver attribute and only apply to the named item or group of items.
- In the manifest file as a PlayServerTable—Mappings here are grouped within the <playServerTable> and <playServer> tags and are applied to all content served from the hosted domain using the manifest file.
- In the system-level playserver map configured during CDN startup.

<playServerTable> tags are enclosed within the <CdnManifest> tags and name at least one playserver, for example, RealServer, to which certain MIME types and file extensions are mapped.

Example 2-3 shows a PlayServerTable as it might appear in a manifest file. The following table would provide content mappings for RealServer for the hosted domain using the manifest file in which the table appears:

Example 2-3 PlayServerTable Tag

```
<playServerTable>
<playServer name=”real”>
<contentType name=”application/x-pn-realaudio”/>
<contentType name=”application/vnd.rn-rmadriver”/>
<extension name=”ra”/>
<extension name=”smi”/>
</playServer>
</playServerTable>
```

<playServer></playServer>

The <playServer> tag names a media server type on the Content Engine that will be responsible for playing the content types and files with extensions that are mapped to it using the <content-type> tags. The <playServer> tag is enclosed within <playServerTable> tags.

Note Do not confuse the <playServer> tag with the playserver setting in an <item> or <item-group>, which specifies a server type to be used for an individual piece of content or group of related content items. Although both playserver settings accomplish the same task, <item>-level playserver settings take precedence over the content type and file extension mappings specified by the <playServer> tags in the <playServerTable> area.

name (required)

Each <playServer> tag names the type of server to which content will be mapped using the *name* attribute. Content Engines support four types of playservers:

- real (RealMedia RealServer)
- http (web server)
- qtss (Apple QuickTime)
- wmt (Microsoft Windows Media)

<contentType>

The <contentType> tag names a MIME content type that is being mapped to a playserver.

The <contentType> tag must be enclosed within a <playServer> tag set. When both <contentType> and <extension> tags are present in a PlayServerTable for a particular media type, the <contentType> mapping takes precedence.

name (required)

Each <contentType> tag names a type of media that will be mapped to the playserver using the *name* attribute. See Table 2-1 for a list of supported media types.

Table 2-1 Supported Media File Formats Grouped by Manifest File Content Type

Extension	Supported Formats	Notes
http	• Audio Visual Interleaved (AVI) • Graphics Interchange Format (GIF) • Hypertext Markup Language (HTML, HTM) • Joint Photographic Experts Group (JPG) • Microsoft PowerPoint (PPT) • Microsoft Word (DOC) • Motion Picture Experts Group (MPEG, MPG) • MPEG Audio Layer 3 (MP3) • Portable Document Format (PDF) • QuickTime Movie (MOV) • ASX	The content item will be handled by an HTTP server; this tag is used for content that cannot be streamed by any of the servers listed in the previous section, for example, Adobe PDF, PostScript (PS), and MPG files.
media	• AVI • GIF • HTML, HTM • JPG • PPT • DOC • MPEG, MPG) • MP3 • PDF	This is the default value used by the Cisco Internet CDN Software. Use the media tag when no playserver is specified to handle a content item; the linked item may be a pre-positioned or a live content item.
qtss	• QuickTime (QT) • MOV	The content item will be handled by the Apple QuickTime Darwin Streaming Server.

Table 2-1 Supported Media File Formats Grouped by Manifest File Content Type (continued)

Extension	Supported Formats	Notes
real	• RealAudio (RA) • RealMedia (RM) • RealPix (RP) • RealText (RT) • Synchronized Container Format (SMIL)	The content item will be handled by RealServer.
wmt	• ASF (includes WMA and WMV) • ASX	The content item will be handled by Windows Media Services.

<extension>

The <extension> tag names a file extension that is being mapped to a playserver.

The <extension> tag comes after the <playServer> tag. When both <contentType> and <extension> tags are present in a playServerTable for a particular media type, the <contentType> mapping takes precedence.

name (required)

The *name* attribute provides the file extension for a mapped content type. When files with the named extension are requested, the mapped playserver will be used to serve them.

<options/>

The <options/> tag (see Example 2-4) is a manifest designation that allows you to specify global settings for the hosted domain using the predefined attributes described in the paragraphs that follow.

The <options> tag is enclosed within the <CdnManifest> tags and specifies at least one global setting for the hosted domain. When omitted, default values or <item>-level equivalents are used.

If parameters are defined in both the manifest file <options> tag and the <item> tag for a particular piece of content, the <item>-level designation takes precedence.

Example 2-4 Options Tag

```
<options timeZone="EST" noRedirectToOrigin="false" />
```

manifest-id

This user-defined attribute specifies a unique, numeric identifier for the manifest file that is used to distinguish it from other manifest files on your CDN. Providing a unique identifier for each manifest makes the job of distinguishing one manifest file from another simpler.

noRedirectToOrigin (optional)

When set to *false*, this attribute allows the CDN to redirect requests for a content item to the origin server if it has not been pre-positioned yet.

When set to *true*, this attribute prevents the CDN from redirecting content to the origin server if it has not been pre-positioned on the hosted domain cache.

timeZone (optional)

This attribute specifies the time zone that is used by all content items and item groups on the hosted domain. When not specified, the default time zone is Greenwich Mean Time (GMT). Accepted values for this attribute include any standard time zone ID or abbreviation supported by the Java language, for example:

```
EST
```

which is the abbreviation for Eastern Standard Time.

See Appendix C, "CDN Supported Time Zones," for a list of supported time zone abbreviations that can be used in the manifest file.

<server></server>

The <server> tags (see Example 2-5) define a host or set of hosts from which content is to be retrieved.

The <server> tags are contained within <CdnManifest> tags and contain one or more <host> tags, which identify hosts (server locations) from which content will be retrieved.

Within each <server> tag set, be sure to list hosts in order of importance.

Example 2-5 Server Tag

```
<server name=“origin-server”>
<host name=”www.cisco.com” .../>
</server>
```

name (required)

Each <server> tag set provides a name that individual content items and item groups use to point to the list of hosts. This name is specified using the *name* attribute.

<host />

The <host/> tag (see Example 2-6) defines a web or live server from which content is to be retrieved for hosting on the hosted domain. Multiple host servers can be defined within a single <server> tag set.

The <host> tag must be enclosed within <server> tags. Multiple <host> tags may appear within the same <server> tag set, and should be listed according to their importance, with the most important host listed first.

Example 2-6 Host Tag

```
<host name=”www.cisco.com”
proto=“http”
port=“80” />
```

For each <host> tag, there are a variety of required and optional attributes, which are described below.

name (required)

The *name* attribute identifies the DNS name or IP address of the host. This attribute may also point to a particular directory on the host.

password (optional)

The *password* attribute identifies the password for the user account required to access the host server. Defining a user account and password is optional, and is dependent on the protocol being used.

port (required)

The *port* attribute identifies the TCP port through which traffic to and from the host will pass. The port used is dependent on the protocol used to communicate with the host.

proto (required)

The *proto* attribute identifies the communication protocol that is used to fetch content from the host. The only supported protocol for the Cisco Internet CDN Software is HTTP.

user (optional)

The *user* attribute identifies the secure login used to access the host. Defining a user account and password is optional, and is dependent on the protocol being used.

<item /> and <item></item>

The <item> tag names a single piece of content on the hosted domain, for example, a graphic (see Example 2-7), MPEG video, or RealAudio sound file. Content items may be listed individually, or grouped using the <item-group> tag.

The <item> tag must be enclosed within <CdnManifest> tags and may also be enclosed within <item-group> tags.

Example 2-7 Item Tag

```
<item cdn-url= “logo.jpg”
server=”origin-web-server”
src= “images/ciscologo256_colors.jpg”
type=“prepos”
playserver=“http”
ttl=300/>
```

For each <item> tag, there are a variety of required and optional attributes, which are described below.

alternateUrl (optional)

The *alternateUrl* attribute names a location that will be displayed in the place of the content item if the src (source) location is invalid. For example, the alternateUrl tag might point to an HTML-format help page.

cdn-url (optional)

The *cdn-url* attribute identifies the public location for the content item on the hosted domain. The *cdn-url* attribute can use wildcard (*) values in the manifest file only when the content item is live (streamed) content. The published content URL must of course point to the live content item on the live server.

The value supplied for the *cdn-url* attribute becomes one part of the published request URL that end users see and link to. If no *cdn-url* value is supplied, the *cdn-url* is set to the *src* attribute.

contains (optional)

The <*contains.../*> tag (see Example 2-8) identifies other pieces of content that are embedded within the content item currently being described. For example, a SMIL-format file may contain links to JPEG and RealAudio files that are crucial components of the finished SMIL presentation. Using the <contains.../> tag to name each component file ensures that these items are ready to be served when the SMIL file is requested.

Requests for an item with links to other pieces of content are only accepted after the CDN determines that all dependent content items are present in the cache.

Example 2-8 Item Tag with Contained Elements

```
<item cdn-url="house.rp"
  src="house/house.rp">
    <contains cdn-url="image08.jpg"/>
    <contains cdn-url="image09.jpg"/>
    <contains cdn-url="image11.jpg"/>
    <contains cdn-url="image12.jpg"/>
    <contains cdn-url="image13.jpg"/>
</item>
```

expires (optional)

The *expires* attribute designates a time in yyyy-mm-dd hh:mm:ss format after which the content item will no longer be served from the CDN. If no time zone is specified using the timeZone tag, the default time zone of Greenwich Mean Time (GMT) is used to determine the point after which the content item will no longer be available.

At some point after the expiration date and time have been reached, the expired content is removed from the cache.

If the *expires* attribute designates a time in the future, the content item will continue to be served from the CDN.

noRedirectToOrigin (optional)

When set to *false*, the *noRedirectToOrigin* attribute allows the CDN to redirect requests for a content item to the origin server if the content item is not yet pre-positioned at the location specified by the *src* attribute tag.

When set to *true*, this attribute prevents the CDN from redirecting content to the origin server if it cannot be found in the hosted domain cache.

playserver (optional)

The *playserver* attribute names the server that will be used to play this media item. When specified, this value overrides any content mapping in the <playServerTable> area. See the "<playServer></playServer>" section on page 2-8 for supported playserver designations.

RealServer and Windows Media Services are the only supported platforms for delivering live content. Thus, when the type is *live*, the playserver must be either *real* or *wmt*.

prefetch (optional)

The *prefetch* attribute designates a time in yyyy-mm-dd hh:mm:ss format after which a content item should be retrieved from the origin server and repositioned on the Content Engine.

If no time zone is specified using the timeZone tag, the default time zone of Greenwich Mean Time (GMT) is used to determine the point at which the content will be retrieved from the origin server.

If the *prefetch* attribute designates a time in the future, the content item is not updated.

serve (optional)

The *serve* attribute specifies the date and time after which grouped content items can be requested from the Content Engine in yyyy-mm-dd hh:mm:ss format. The default time zone is GMT unless otherwise specified using the <options> tag.

server (optional)

The *server* attribute identifies the server from which the content item will be fetched. The name specified must match the server name in the <server> tag. If omitted, the origin server of the hosted domain is assumed to be the server.

src (required)

The *src* attribute names the relative URL on the origin server from which content will be fetched. When no *cdn-url* value is specified, the *src* attribute is used in the published content URL.

ttl (optional)

The *ttl* attribute identifies the period, in minutes, for which the content item should be controlled for changes before release. The default value is 30 minutes.

type (optional)

The *type* attribute indicates how the content should be handled. Two options are supported:

- prepos—Content should be pre-positioned on the hosted domain. This is the default value, which is applied if no type is specified.
- live—Content is a live broadcast and cannot be pre-positioned.

<item-group></item-group>

The <item-group> tag (see Example 2-9) names a collection of content items with shared attributes on the hosted domain, for example, a group of graphics on the same host with the same Time To Live (TTL) value. If an attribute is specified in both the <item-group> tag and separately for a grouped content item, the <item>-level attribute takes precedence over the group attribute.

The <item-group> tag must be enclosed within <CdnManifest> tags and contain two or more <item> tags identifying content items that share the attributes named by the <item-group> tag.

Example 2-9 Item-Group Tag

```
<item-group server="origin-web-server" type="prepos" ttl="300">
    <item cdn-url="wild.ram" src="wildlife.ram" />
    <item cdn-url="gg.mpeg" src="GoldenGate.mpeg" />
    <item cdn-url="jbg.mp3" src="JohnnyBeGood.mp3" />
    <item cdn-url="paul.asx" src="fin371k.asx" />
</item-group>
```

For each <item-group> tag, there are a variety of required and optional attributes, which are described in the paragraphs that follow.

alternateUrl (optional)

The *alternateUrl* attribute names a location that will be displayed in the place of the content item if the src (source) location is invalid. For example, the alternateUrl tag might point to an HTML-format help page.

cdnPrefix (optional)

The *cdnPrefix* attribute names a directory or partial path that is placed in the published request URL immediately before the value named by the item’s *cdn-url* attribute.

noRedirectToOrigin (optional)

When set to *false*, the *noRedirectToOrigin* attribute allows the CDN to redirect requests to serve grouped content items to the origin server if they cannot be found at the location specified by the *src* attribute.

When set to *true*, this attribute prevents the CDN from redirecting requests for grouped content items to the origin server if they cannot be found in the hosted domain cache.

playserver (optional)

The *playserver* attribute names the server that will be used to play the grouped content items. When specified for grouped content items, this value overrides any content mapping in the <playServerTable> area. See the “<playServer></playServer>” section on page 2-8 for supported playserver designations.

RealServer and Windows Media Services are the only supported platforms for delivering live content. When the type is *live*, the playserver must be either *real* or *wmt*.

serve (optional)

The *serve* attribute specifies the date and time after which the content item can be requested from the Content Engine in yyyy-mm-dd hh:mm:ss format. The default time zone is GMT unless otherwise specified using the <options> tag.

server (optional)

The *server* attribute identifies the server from which the grouped content items will be fetched. The name specified must match the server name in the <server> tag. If omitted, the origin server from the hosted domain is assumed to be the server.

srcPrefix (optional)

The *srcPrefix* attribute names a directory or partial path that is used to build a directory structure for the items in the content item group. The value specified by the *srcPrefix* attribute is placed in the published request URL immediately before the item's *src* attribute.

ttl (optional)

The *ttl* attribute identifies the period, in minutes, for which the grouped content item should be controlled for changes before release. The default value is 30 minutes.

type (optional)

The *type* attribute indicates how each grouped content item should be handled. Two options are supported:

- prepos—Content should be pre-positioned on the hosted domain. This is the default value, which is applied in the event that no type is specified.
- live—Content is a live broadcast and cannot be pre-positioned.

Sample Manifest File

Example 2-10 shows a functional manifest file. Use this example as a model when creating or troubleshooting your own manifest files.

Example 2-10 Manifest File Containing Pre-positioned and Live Content

```
<?xml version="1.0"?>
<!DOCTYPE CdnManifest SYSTEM "CdnManifest.dtd">
<CdnManifest>
<options timeZone="EST" />
<server name="origin-web-server">
  <host name="http://www.cisco.com/media/"
        proto="http" />
</server>
<item-group
      server="origin-web-server"
      type="prepos"
      ttl="300">
 <item cdn-url="wild.ram" src="wildlife.rm" />
  <item cdn-url="gg.mpeg" src="GoldenGate.mpeg" />
  <item cdn-url="jbg.mp3" src="JohnnyBeGood.mp3" />
  <item cdn-url="paul.avi" src="fin371k.avi" />
</item-group>
<item cdn-url="house.rm"
  src="house/house.rm"/>
<item cdn-url="house.rt"
  src="house/house.rt"/>
<item cdn-url="house.smi"
  src="house/house.smi">
    <contains cdn-url="house.rm"/>
    <contains cdn-url="house.rt"/>
  </item>
<!--item-group server="live-streamer" type="live">
    <item cdn-url="/voices.rm" src="encoder/test.rm"/-->
<!--/item-group-->
</CdnManifest>
```

Publishing URLs That Link to CDN Content

Having reviewed the syntax and structure of the manifest file, and created a manifest file for your hosted domain, you are ready to create URLs that point end users to your CDN content.

All URLs pointing to CDN content use the following structure:

http://*hosted_domain_name*/*cdn-url*

Optionally, CDN URLs can contain a playserver designation as follows:

http://*hosted_domain_name*/*playserver*/*cdn-url*

When no playserver is designated, cdn-media is used as the default playserver designation.

The elements of these URLs are described in Table 2-2. Be aware that all URL information is case sensitive—ignoring case sensitivity in your published Web pages will result in the CDN being unable to retrieve the requested content.

Table 2-2 Components of a CDN URL

URL Component	Description
hosted_domain_name	Fourth-level domain name assigned to your hosted domain or the alias assigned to that hosted domain. See the "Creating a Hosted Domain for a Content Provider" section on page 2-49 for more information on naming hosted domains.

Table 2-2 Components of a CDN URL (continued)

playserver	Optional. The server designated to handle the content item to which you are linking. If no playserver is specified, cdn-media is used as the default playserver designation. Playservers can be specified in a number of locations, including the manifest file. Playserver designations in the URL of a content item override a content mapping in the manifest file. See Table 2-1 for a list of media formats, organized by extension. The following playserver definitions are supported in CDN URLs: • *cdn-media* • *cdn-real* • *cdn-qtss* • *cdn-http* • *cdn-wmt*
cdn-url	Relative location of the content item on the CDN device. This value is supplied by the *cdn-url* or *src* attribute in the <item> tag in the manifest file for each piece of content. Wildcard characters are accepted in the *cdn-url attribute* only when you link to live content. Actual content URLs must of course point to the actual content item.

Adding Content Providers

Content providers are your customers. Content providers deploy content on a CDN.

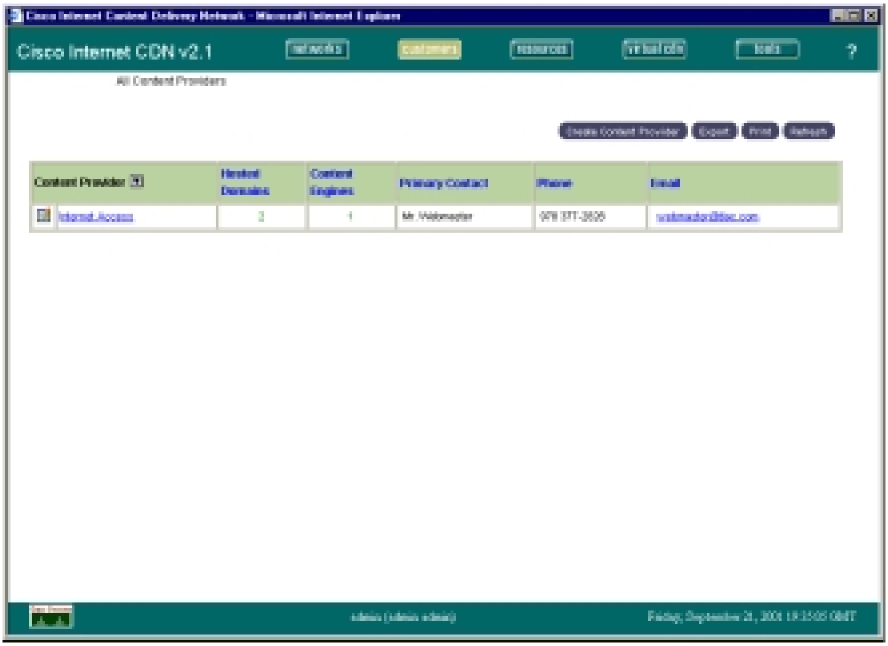
Note Before you add a content provider, you need to have up-to-date customer contact information available so that you can enter the correct information when you add the content provider.

To add a content provider, follow these steps:

Step 1 From the Cisco Internet CDN Software user interface, click **customers**.

The View Content Providers page appears. (See Figure 2-1.)

Figure 2-1 View Content Providers

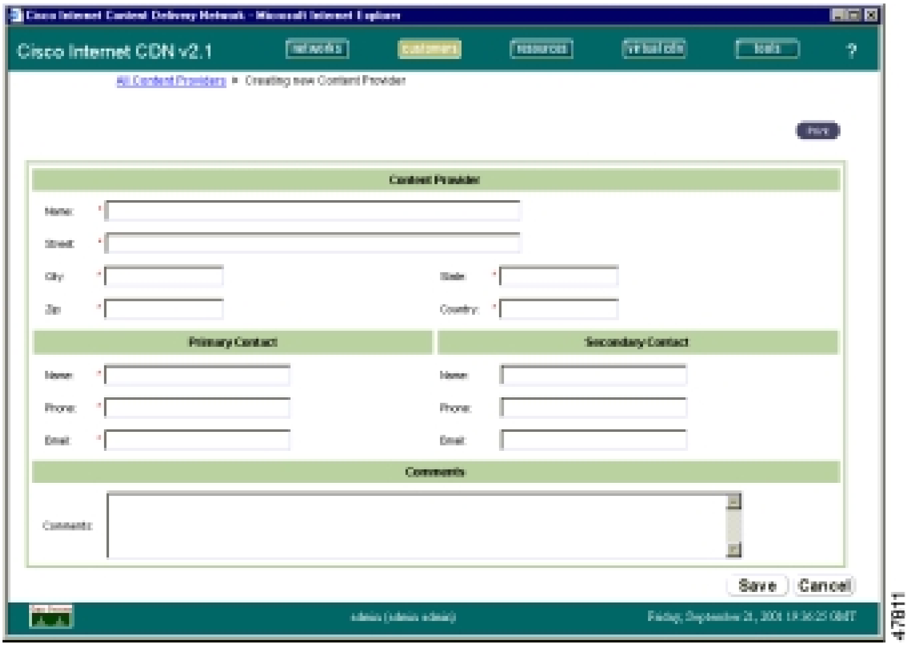


Content Provider	Hosted Domains	Content Engines	Primary Contact	Phone	Email
Internet Access	2	1	Mr. Webmaster	978 377-2026	webmaster@foo.com

Step 2 Click **Create Content Provider**.

The Create a New Content Provider page appears. (See Figure 2-2.)

Figure 2-2 Create a New Content Provider



Step 3 Under the Content Provider heading, enter the company name for the content provider in the Name field.

Note The company name must be distinct from that of other content provider company names.

Step 4 Enter the postal address for the content provider in these fields: Street, City, State, Zip (postal code), and Country.

Step 5 Under the Primary Contact heading, enter the name of the primary technical contact for the content provider in the Name field.

Note The primary technical contact is usually the person responsible for the origin server that provides content to the delivery network.

Step 6 Use the fields provided to enter the phone number and e-mail address for the primary contact for this customer.

Step 7 Repeat Step 5 and Step 6 for the secondary contact person for the content provider.

Note For a secondary contact, enter the name, telephone number, and e-mail address of a finance or accounting contact. (This step is optional.)

Step 8 Click **Save** to create a new content provider.

Adding Regions and Locations

A region is a geographical area. For example, Northeastern USA could be a region, or each time zone in the United States could correspond to a region. The three default regions are Eastern USA, Central USA, and Western USA.

Note There must be a minimum of three regions. Although you can delete the default regions, you must always maintain at least three regions on the Content Distribution Manager.

A location is a physical place, for example San Jose, California, or a point of presence (POP). Each location has a region associated with it, which means that locations are grouped together in regions.

Content Routers and Content Engines have regions and locations associated with them. Content Routers use location and region information to make decisions about where to direct DNS requests.

Content Engines use regions and locations for grouping. You set up regions and locations based on the particular needs of your content providers.

Note You can define up to 20 regions and 192 locations.

When you create a region, you must specify whether the region is *desirable*. A desirable region is one to which you can route any end user request (regardless of the geographic origin of the request) because of the existence of robust network connectivity. By default, a region *is not* desirable.

Most regions in the United States are desirable because network connectivity in the United States is generally very good. Network connectivity in other parts of the world may not be as robust, so if an end user request is received from Asia, you might not want to route the request to Africa, for example. However, routing the Asian request to anywhere in the United States would be acceptable.

Adding a Region

Since a location has a region associated with it, it is convenient to add regions before you add locations.

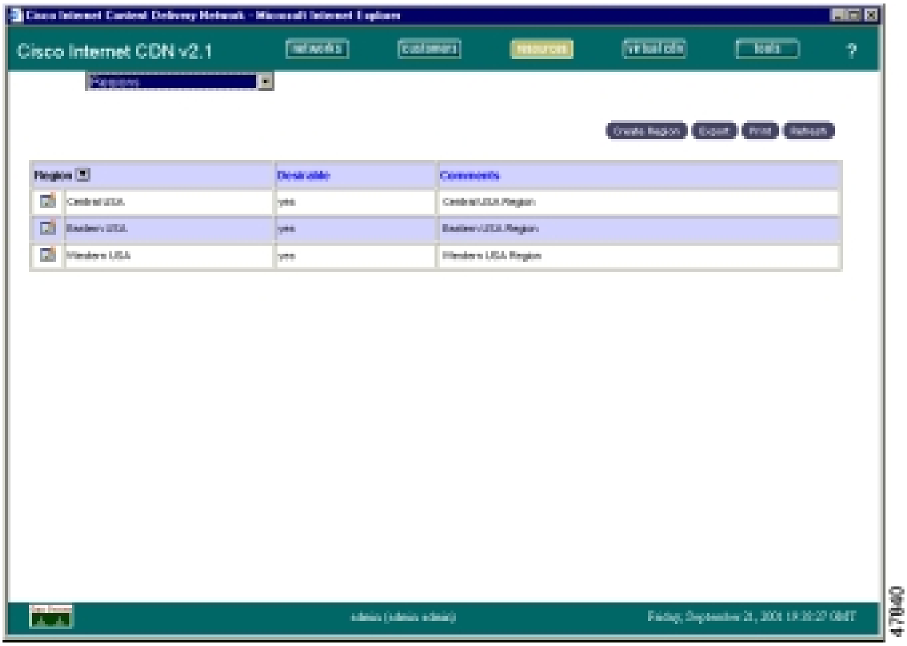
To add a region, follow these steps:

Step 1 From the Cisco Internet CDN Software user interface, click **resources**.

Step 2 From the dropdown list, choose **Regions**. The View Regions page appears. (See Figure 2-3.)

Note Alternatively, click **networks**.

Figure 2-3 View Regions



Region	Desirable	Comments
Central USA	yes	Central USA Region
Eastern USA	yes	Eastern USA Region
Western USA	yes	Western USA Region

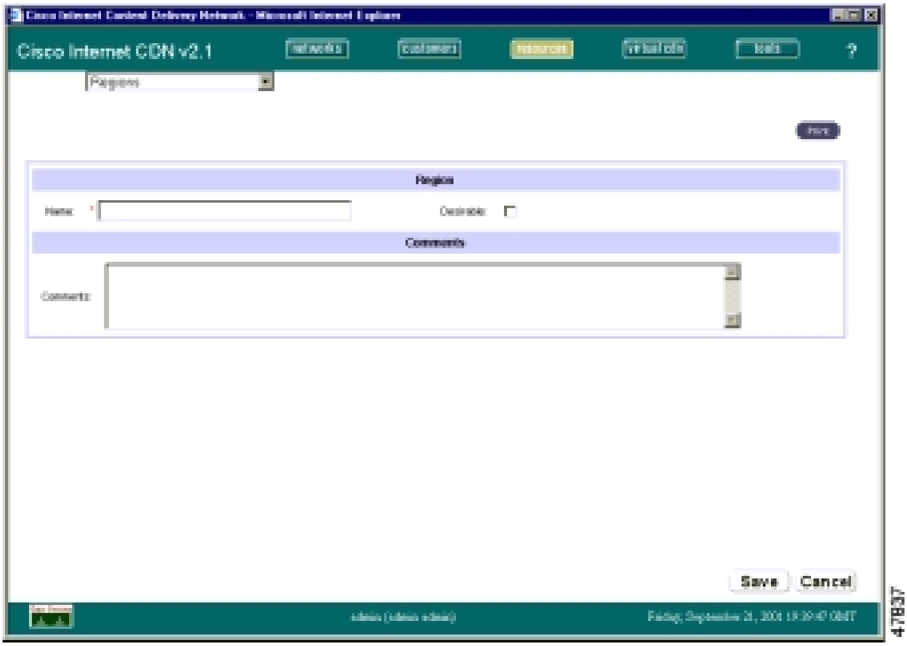
admin (admin admin)

Friday, September 21, 2001 18:30:27 GMT

Step 3 Click **Create Region**.

The Create a Region page appears. (See Figure 2-4.)

Figure 2-4 Create a Region



Step 4 Under the Region heading, enter a region name in the Name field.

Note The region name must be distinct from those of all other regions.

Step 5 Under the Comments heading, enter a description that is useful to you. (Comments do not appear to end users.) This step is optional.

Note If you click **Cancel** at any time, all values return to their previous settings, and the View Regions page reappears.

Step 6 If the region is a desirable region, check the **Desirable** check box.

Step 7 Click **Save** to create the new region.

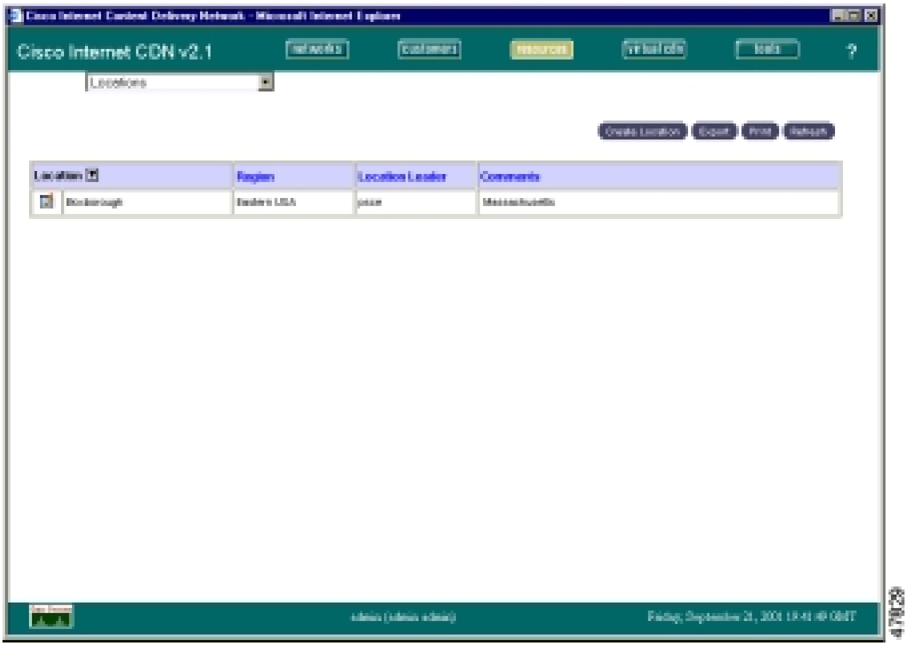
Adding a Location

To add a location, follow these steps:

Step 1 From the Cisco Internet CDN Software user interface, click **resources**.

Step 2 From the drop-down list, choose **Locations**. The View Locations page appears. (See Figure 2-5.)

Figure 2-5 View Locations

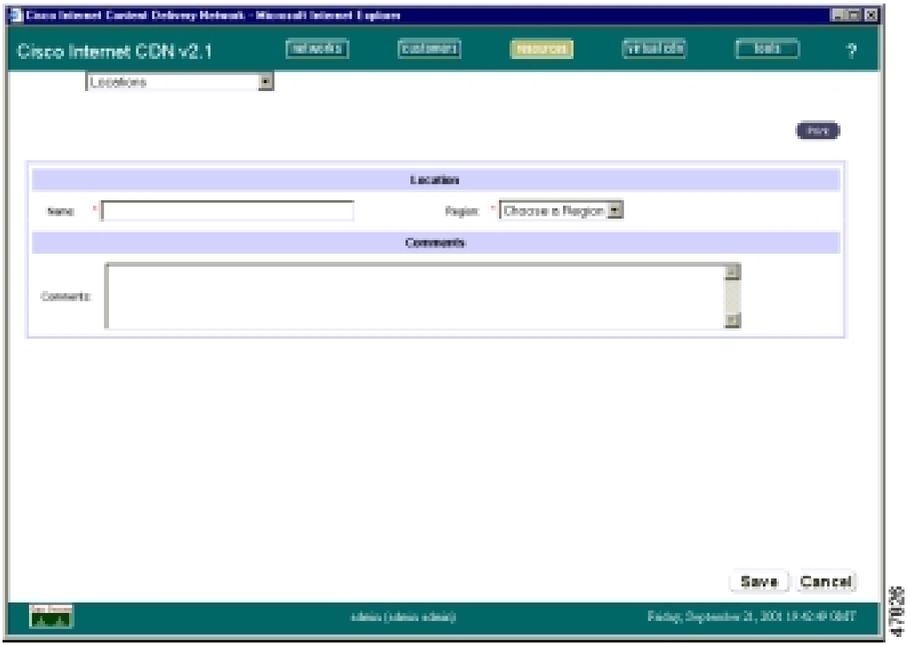


Location	Region	Location Leader	Comments
Boxborough	Eastern USA	[illegible]	Massachusetts

Step 3 Click the **Create Location** button.

The Create a Location page appears. (See Figure 2-6.)

Figure 2-6 Create a Location



Step 4 Under the Location heading, enter a name for the location in the Name field.

Note The location name must be distinct from those of all other locations.

Step 5 Next, choose a region from the **Region** drop-down list.

You must specify a region that is associated with the location. If you have not yet added the region you want, click **Cancel** and see the instructions for the "Adding a Region" section on page 2-25 before attempting to create a location.

Step 6 Under the Comments heading, enter a description that is useful to you in the field provided. (Comments do not appear for end users.) This step is optional.

Step 7 Click **Save** to create your new location.

Activating the Warm Standby Content Distribution Manager

After configuring your warm standby Content Distribution Manager by following the procedure in the “Configuring the Content Distribution Manager” section in Chapter 3 of the *Cisco Internet CDN Software Configuration Guide*, you must activate the device from the graphical user interface of the primary Content Distribution Manager.

If you do not activate your warm standby Content Distribution Manager, it will not act as a failover device if the primary Content Distribution Manager goes offline unexpectedly.

To activate the warm standby Content Distribution Manager:

Step 1 From the Cisco Internet CDN Software user interface, click **resources**.

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

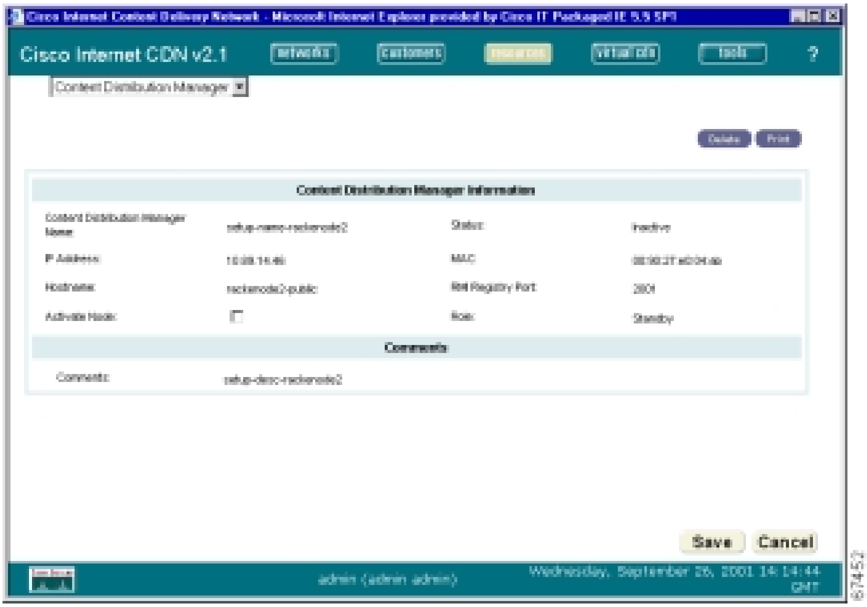
The View Content Distribution Managers page appears.

Step 3 Click the icon next to the name of the warm standby Content Distribution Manager. This is the device with the role of *N/A* and the status of *inactive*. The other Content Distribution Manager listed is your primary device.

Note There cannot be two primary Content Distribution Managers.

The Modify a Content Distribution Manager page appears. (See Figure 2-7.)

Figure 2-7 Modify a Content Distribution Manager


Cisco Internet Content Delivery Network - Microsoft Internet Explorer provided by Cisco IT Packaged IE 5.5 SP1
Cisco Internet CDN v2.1
networks
customers
resources
virtual cdn
tools
?
Content Distribution Manager
Delete
Print
Save
Cancel
admin (admin admin)
Wednesday, September 26, 2001 14:14:44 GMT
67452

Content Distribution Manager Information

Content Distribution Manager Name:	setup-name-racknode2	Status:	Inactive
IP Address:	10.28.14.46	MAC:	00:90:27:a0:04:ab
Hostname:	racknode2-public	RMI Registry Port:	2001
Activate Node:	□	Role:	Standby

Comments

Comments: setup-desc-racknode2

Step 4 Under the General Configuration heading, check the **Activate Node** check box.

Step 5 Click **Save** to update the Content Distribution Manager record and activate the warm standby Content Distribution Manager.

You are returned to the View Content Distribution Managers page.

The warm standby Content Distribution Manager status changes briefly to *standby* while the device is being activated before changing to *online*, indicating that the device is ready to act as a failover device.

If the Content Distribution Manager does not return to the online state, verify that the device is running before contacting Cisco Technical Support.

Activating and Defining Content Routers and Content Engines

Using the Content Distribution Manager, you can edit the device properties of the Content Engines and Content Routers that you have configured. Properties that can be edited appear in Table 2-3.

Table 2-3 Content Engine and Content Router Properties

Device Property	Description	Notes
Status	Indicates whether the device has been activated	Status is online or offline. Devices cannot be deactivated after they have been activated.
Name	Provides the name of the device	Content Engine names cannot contain spaces if the named Content Engine will be a member of a cluster.
Version	Version of Cisco Internet CDN Software currently installed on the selected device	
Region	Describes the general geographic location of the physical device	
Location	Describes the specific physical location of the physical device	
Root Password	Password for the administrative-level root account for the selected device	Allows administrators to overwrite the root account password and gain direct, command-line access to the device.

Table 2-3 Content Engine and Content Router Properties (continued)

Device Property	Description	Notes
HTTP Password	Password for the web-based graphical user interface for the selected device	Allows administrators to secure access to configuration information for selected devices from the Content Distribution Manager.
Storage Allocation	Amount of space (in gigabytes) reserved on the selected device to cache pre-positioned media	Applies only to Content Engines.
Description	Optional description of the selected device for easy recognition in the Content Distribution Manager interface	

Activating and Defining a Content Router

A Content Router is a device that selects suitable Content Engines within a CDN to serve a given end user request.

Note There can be up to eight Content Routers in a CDN.

Before you can activate and define a Content Router, it must be registered with the Content Distribution Manager. Registration happens in the last step of the Content Router setup routine, but Content Routers can be reregistered with the Content Distribution Manager at any time.

In addition, your DNS server must have entries that provide a mapping to the Content Routers before content routing can take place. For information about configuring your Content Routers and registering them with the Content Distribution Manager, or for questions regarding DNS configuration, refer to the *Cisco Internet CDN Software Configuration Guide*.

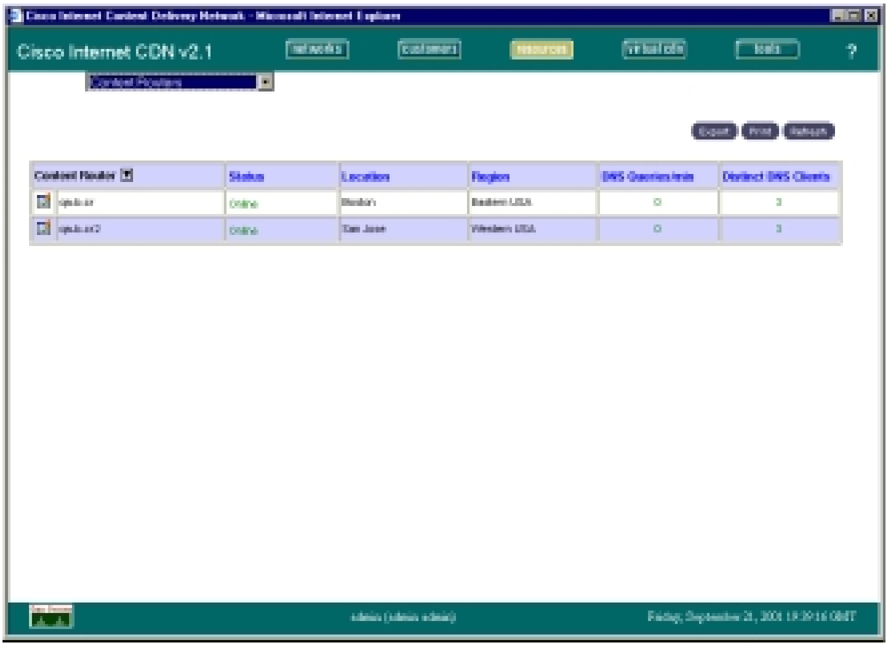
To activate and define a Content Router, follow these steps:

Step 1 From the Cisco Internet CDN Software user interface, click **resources**.

Step 2 From the drop-down list, choose **Content Routers**.

The View Content Routers page appears. (See Figure 2-8.)

Figure 2-8 View Content Routers

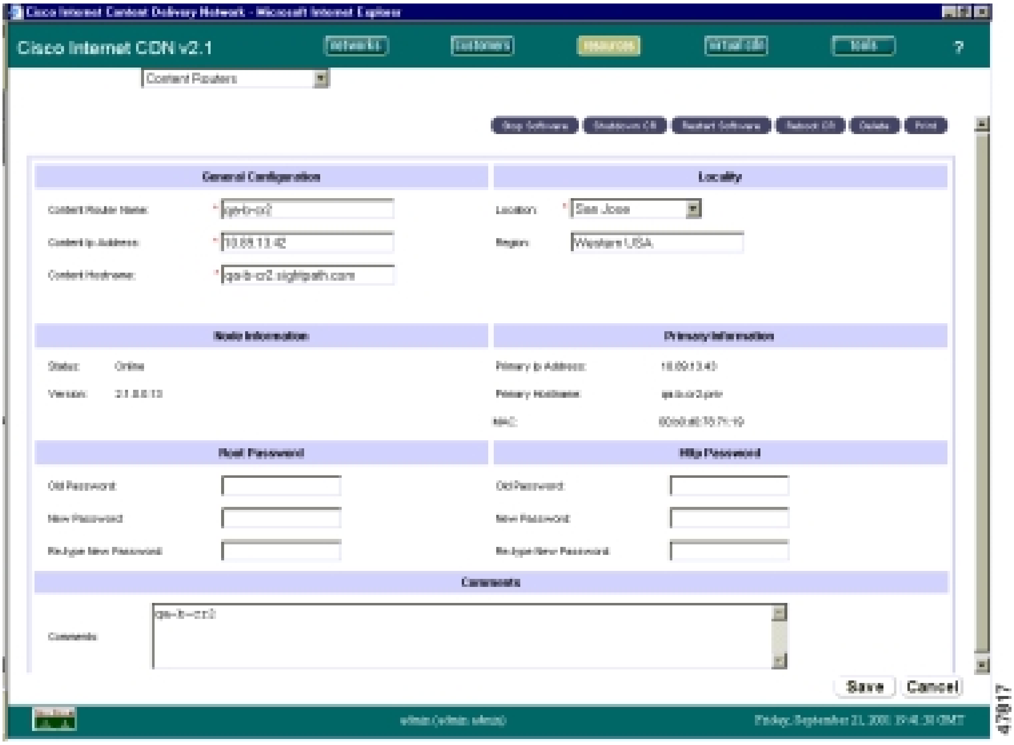


Content Router	Status	Location	Region	DNS Queries/min	Distinct DNS Clients
[illegible]	Online	Boston	Eastern USA	0	3
[illegible]	Online	San Jose	Western USA	0	3

Step 3 Click the icon next to the name of the Content Router that you want to activate and define.

The Modify a Content Router page appears. (See Figure 2-9.) From this page you activate, define, and manage a Content Router.

Figure 2-9 Modify a Content Router



General Configuration

Content Router Name: * qa-b-cr2

Content Ip Address: * 10.69.13.42

Content Hostname: * qa-b-cr2.sightpath.com

Locality

Location: * San Jose

Region: Western USA

Node Information

Status: Online

Version: 2.1.0.0.13

Primary Information

Primary Ip Address: 10.69.13.43

Primary Hostname: qa-b-cr2.prir

MAC: 00:d0:b7:75:71:19

Root Password

Old Password:

New Password:

Re-type New Password:

Http Password

Old Password:

New Password:

Re-type New Password:

Comments

Comments: qa-b-cr2

admin (admin, admin)

Friday, September 21, 2001 15:41:38 GMT

Step 4 Under the General Configuration heading, enter a new name in the Content Router Name field if you want to change the name of the Content Router.

Note The Content Router was named when it was configured. If you change the name, you must choose a unique name. No two Content Routers can have the same name.

Step 5 Under the General Configuration heading, check the **Activate Node** check box (not shown in Figure 2-9).

This activates the Content Router. The next time you display the Modify a Content Router page, the Activate Node check box will have disappeared and you will see that the Content Router is active.

Note You cannot deactivate a Content Router once it has been activated. However, you can delete it, stop it, or shut it down. For information, see the "Deleting a Content Router" section on page 3-23.

Step 6 From the pull-down Location list, choose a location in which the selected Content Router will be grouped.

If the desired location has not already been created, see the "Adding a Location" section on page 2-28 for instructions on how to add a location.

Note A region is associated with a location, so the region appears automatically when the location is selected or defined. You cannot define a region here. For information on defining a region, see the "Adding a Region" section on page 2-25.

Step 7 Click **Save** to activate the selected Content Router.

Step 8 Change the default root and HTTP passwords for the Content Router from their default values once the device has been activated. See the "Modifying Content Router Passwords" section on page 3-22 for instructions.

Activating and Defining a Content Engine

A Content Engine is a device that stores content from content providers and serves it to an end user.

Note There can be up to 2000 Content Engines in a CDN.

Before you can activate and define a Content Engine, it must be registered with the Content Distribution Manager. Registration happens in the last step of the Content Engine setup routine, but Content Engines can be registered again with the Content Distribution Manager at any time. For information about configuring a Content Engine, refer to the *Cisco Internet CDN Software Configuration Guide*.

If the Content Engine you are activating will be a member of a supernode, review the recommended supernode configuration procedure in the "Supernode Configuration Priorities" section on page 2-40 before proceeding.

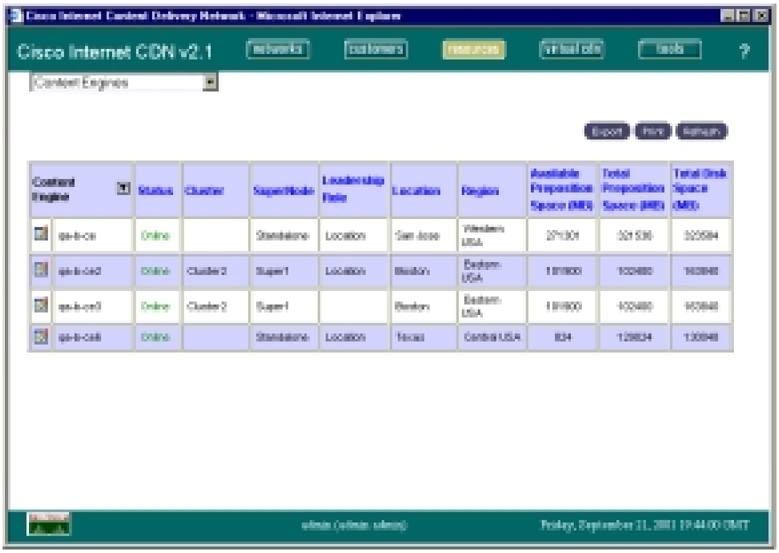
To activate and define a Content Engine, follow these steps:

Step 1 From the Cisco Internet CDN Software user interface, click **resources**.

Step 2 From the drop-down list, choose **Content Engines**.

The View Content Engines page appears. (See Figure 2-10.)

Figure 2-10 View Content Engines

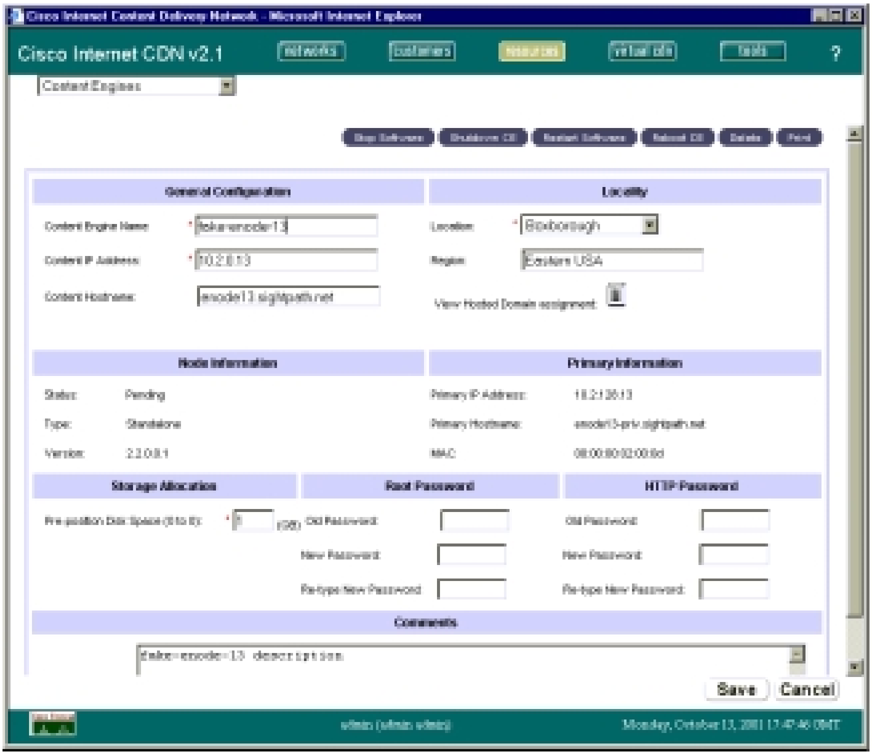


Content Engine	Status	Cluster	SuperNode	Leadership Role	Location	Region	Available Preposition Space (MB)	Total Preposition Space (MB)	Total Disk Space (MB)
qa-b-ce	Online		Standalone	Location	San Jose	Western USA	271301	321536	322584
qa-b-ce2	Online	Cluster2	Super1	Location	Boston	Eastern USA	181800	102480	163840
qa-b-ce3	Online	Cluster2	Super1		Boston	Eastern USA	181800	102480	163840
qa-b-ce4	Online		Standalone	Location	Texas	Central USA	834	129834	130048

Step 3 Click the icon next to the name of the Content Engine that you want to activate and define.

The Modify a Content Engine page appears. (See Figure 2-11.) From this page, you activate, define, and manage the Content Engine. A Content Engine that has been activated is available for assignment to a CDN.

Figure 2-11 Modify a Content Engine



General Configuration

Content Engine Name: * fake-encode-13

Content IP Address: * 10.2.0.13

Content Hostname: encode13.sightpath.net

Locality

Location: * Boxborough

Region: Eastern USA

View Hosted Domain assignment:

Node Information

Status: Pending

Type: Standalone

Version: 2.2.0.8.1

Primary Information

Primary IP Address: 10.2.130.13

Primary Hostname: encode13-priv.sightpath.net

MAC: 08:00:80:02:00:0d

Storage Allocation

Pre-position Disk Space (0 to 8): * 1 (GB)

Root Password

Old Password:

New Password:

Re-type New Password:

HTTP Password

Old Password:

New Password:

Re-type New Password:

Comments

fake-encode-13 description

admin (admin admin)

Monday, October 13, 2001 17:47:46 GMT

Step 4 Under the General Configuration heading, enter a new name in the Content Engine Name field if you want to change the name of the Content Engine.

The Content Engine was named when it was configured. If you change the name, you must choose a unique name. No two Content Engines can have the same name.

Note Content Engine names cannot contain spaces if the named Content Engine will be a member of a cluster.

Step 5 Under the General Configuration heading, check the **Activate Node** check box (not shown in Figure 2-11).

Note You cannot deactivate a Content Engine once it has been activated. However, you can delete it, stop it, or shut it down. For information, see the "Deleting a Content Engine" section on page 3-16.

Step 6 From the Location drop-down list, choose a location in which to place the selected Content Engine.

If the desired location has not already been created, see the "Adding a Location" section on page 2-28 for instructions on how to add a location before continuing. Then choose it from the location list.

Note A region is associated with a location, so the region appears automatically when the location is selected or defined. You cannot define a region here. For information on defining a region, see the "Adding a Region" section on page 2-25.

Step 7 Under the Storage Allocation heading, set the amount of disk space on the selected Content Engine that will be reserved for pre-positioning video-on-demand media for content providers by entering the amount of space (in gigabytes) in the Pre-position Disk Space field.

Note Remember to leave enough room on your Content Engines to accommodate all your static cache content when setting pre-positioning disk space.

Step 8 Click **Save** to update the Content Engine record and activate the selected Content Engine.

Step 9 Change the default root and HTTP passwords for the Content Engine from their default values once the device has been activated. See the "Modifying Content Engine Passwords" section on page 3-13 for instructions.

Adding Supernodes and Content Engine Clusters

Supernodes consist of two or more Content Engines grouped (or "clustered") behind a Content Services Switch. Supernodes provide data redundancy and next-click failover for CDN content, as well as load balancing between Content Engines for improved response time.

When creating a supernode on the CDN, you point the Content Distribution Manager to a Content Services Switch that has already been configured. To properly configure the supernode, you must have the following Content Services Switch configuration information at hand:

- IP address of the switch, referred to as the *CSS configuration address*. This address is used by the Content Distribution Manager to communicate directly with the switch.
- Content Services Switch password. This password is used by the Content Distribution Manager to gain secure access to the switch.

Supernode Configuration Priorities

Because supernodes are complex entities involving the configuration of two separate hardware devices in addition to software components, it is important to configure your hardware devices and software in the proper order, to avoid confusion or errors caused by trying to configure a supernode before one of its components has been properly prepared.

The following tasks must be completed when you configure a new supernode on your CDN. Tasks are listed in the order in which you should complete them. References to related sections in the Cisco Internet CDN software and hardware documentation are provided.

1. Install and configure your Content Services Switch either manually or using the merlot-css-setup script as described in the "Configuring the Content Services Switch" section of Chapter 3 in the *Cisco Internet CDN Software Configuration Guide*.
2. Install and configure your Content Distribution Manager, Content Router, and Content Engines as described in Chapter 3, "Configuring CDN Devices," in the *Cisco Internet CDN Software Configuration Guide*.

3. Register (but do not *activate*) all Content Engines that will belong to the supernode using the procedure described in the "Activating and Defining a Content Engine" section on page 2-36.
4. Create the supernode using the procedure outlined in the next section.
5. Create the clusters that will belong to the supernode using the procedure outlined in the "Creating a Cluster" section on page 2-44.
6. Activate the Content Engines that belong to the supernode and then reserve the necessary disk space on each of the Content Engines using the procedure in the "Modifying Content Engines" section on page 3-11.
7. If you have not already done so, add content providers and hosted domains using the procedures in the "Adding Content Providers" section on page 2-22 and the "Creating a Hosted Domain for a Content Provider" section on page 2-49.

Creating a Supernode

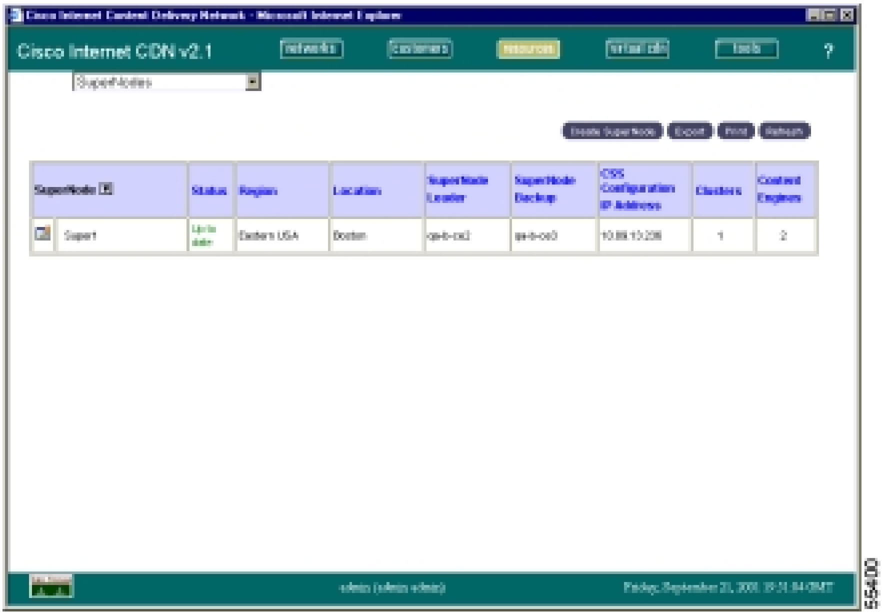
Before attempting to create a supernode, review the recommended supernode configuration procedure in the "Supernode Configuration Priorities" section on page 2-40 before proceeding.

To create a new supernode:

Step 1 From the Cisco Internet CDN Software user interface, click **resources**.

Step 2 From the drop-down list, choose **SuperNodes**. The View Supernodes page appears. (See Figure 2-12.)

Figure 2-12 View Supernodes



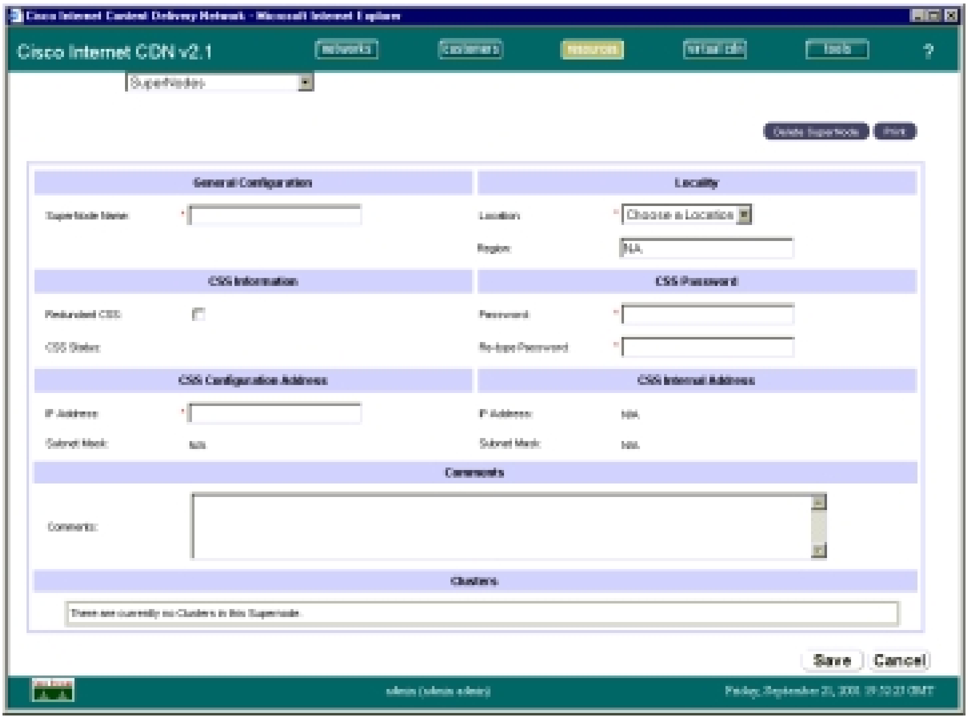
SuperNode		Status	Region	Location	SuperNode Leader	SuperNode Backup	CSS Configuration IP Address	Clusters	Content Engines
	Super1	Up to date	Eastern USA	Boston	qa-b-ce2	qa-b-ce3	10.88.13.236	1	2

admin (admin admin)

Friday, September 21, 2001 19:31:04 GMT

Step 3 Click **Create SuperNode**. Fields for configuring the supernode appear on the Create a Supernode page. (See Figure 2-13.)

Figure 2-13 Create a Supernode



General Configuration

SuperNode Name: *

Locality

Location: * Choose a Location

Region: NA

CSS Information

Redundant CSS: □

CSS Status:

CSS Password

Password: *

Re-type Password: *

CSS Configuration Address

IP Address: *

Subnet Mask: N/A

CSS Internal Address

IP Address: N/A

Subnet Mask: N/A

Comments

Comments:

Clusters

There are currently no Clusters in this Supernode.

Step 4 Under the General Configuration Heading, in the SuperNode Name field, enter the name of the new supernode.

Step 5 From the Location drop-down list, choose a location in which the supernode (and its clusters) will be grouped. Once you choose a location, the region is supplied automatically.

If you have not already created a location, see the "Adding a Location" section on page 2-28 before continuing.

Step 6 Under the CSS Information heading, check the **Redundant CSS** check box if the Content Services Switch you are identifying is acting as a redundant switch.

Step 7 Under the CSS Password heading, in the Password field, enter the root account password required to log in to your Content Services Switch.

Step 8 Confirm the Content Services Switch root account password by reentering it in the Re-type Password field.

Note Do not attempt to supply a new root account password for the Content Services Switch using the password fields provided on the Modify a Supernode page. Entering a password other than the actual root account password in these fields may cause your Content Services Switch to become unstable.

Step 9 Under the CSS Configuration Address heading, enter the IP address of the Content Services Switch in the IP Address field. You should have recorded the IP address of the Content Services Switch during its initial configuration.

Step 10 If you wish, in the Comments field, enter a text description that will accompany the Content Services Switch. (Comments do not appear to end users.)

Step 11 Click **Save** to create the new supernode. The Content Distribution Manager uses the addresses you supplied to contact the Content Services Switch. You are returned to the View Supernodes page. The supernode status appears as *configuring* until the new supernode configuration information has been propagated.

Once the supernode status changes from *configuring* to *up to date*, you can proceed and create your Content Engine clusters. See the next section, "Creating a Cluster."

Creating a Cluster

Content Engines are designated for membership in a cluster during initial configuration, when they are associated with a Content Services Switch on the network. The actual Content Engine groupings, however, are created using the Content Distribution Manager user interface.

Note There can be up to 1000 clusters on a CDN.

Content Engines in a cluster act cooperatively to serve the same set of content for the hosted domain. Each Content Engine must be allocated a uniform amount of disk space for pre-positioning video-on-demand content. Because of this, we recommend that you put Content Engines with the same amount of available disk space in the same cluster so that resources are not wasted on any of your Content Engines.

Before attempting to create a cluster, you must first have done the following:

- Created the supernode to which the cluster will belong
- Obtained the static IP address from your DNS server that will serve as the virtual IP address, which is used to communicate with the Content Engines in the cluster
- Optionally obtained a host name from the DNS server that will serve as the virtual host name and be used to communicate with the Content Engines in the cluster

Before attempting to create a cluster, review the recommended supernode configuration procedure in the "Supernode Configuration Priorities" section on page 2-40 before proceeding.

To create a cluster:

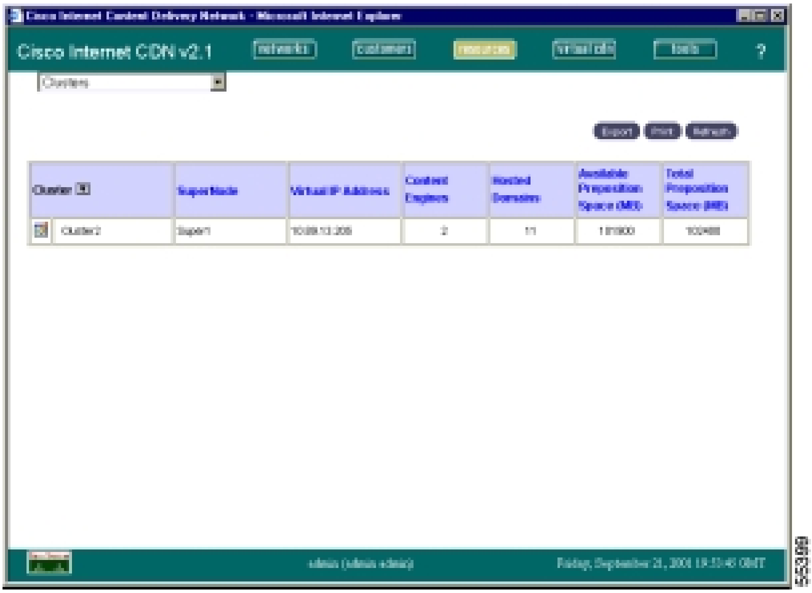
Step 1 From the Cisco Internet CDN Software user interface, click **resources**.

Step 2 From the drop-down list, choose **SuperNodes**.

The View Supernodes page appears. (See Figure 2-12.)

Step 3 Click the edit icon next to the supernode in which you wish to create a new cluster. Fields for modifying the supernode properties appear on the View Clusters page. (See Figure 2-14.)

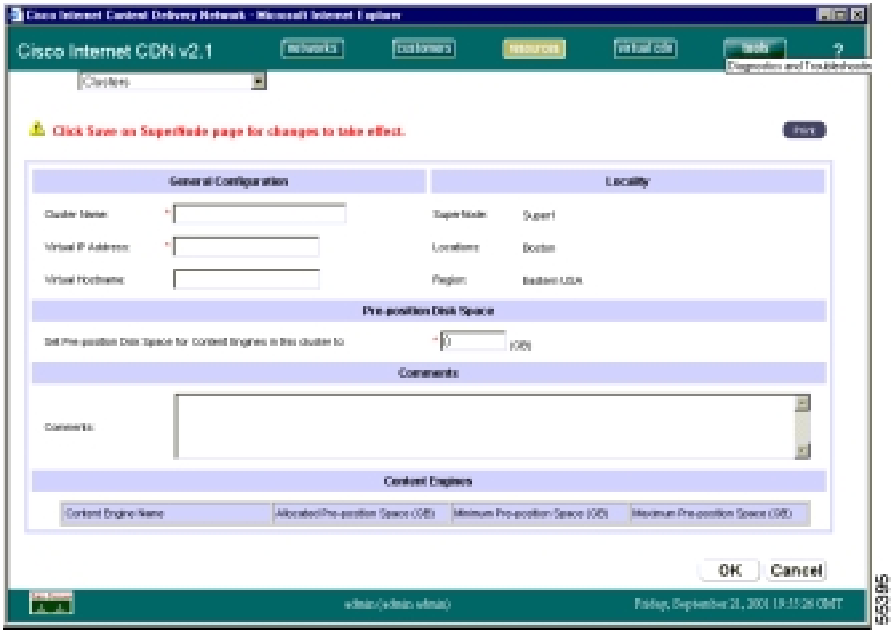
Figure 2-14 View Clusters



Cluster	SuperNode	Virtual IP Address	Content Engines	Hosted Domains	Available Preposition Space (MB)	Total Preposition Space (MB)
Cluster2	Super1	10.89.13.205	2	11	[illegible]	102400

Step 4 Click **Create Cluster** (not shown in Figure 2-14**)**. Fields for configuring the new cluster appear on the Create a Cluster page. (See Figure 2-15.)

Figure 2-15 Create a Cluster


Cisco Internet Content Delivery Network - Microsoft Internet Explorer
Cisco Internet CDN v2.1
networks
customers
resources
virtual cdn
tools
?
Diagnostics and Troubleshooting
Clusters
Help
OK
Cancel
admin (admin admin)
Friday, September 21, 2001 19:15:28 GMT
55395

Click Save on SuperNode page for changes to take effect.

General Configuration

Cluster Name: *

Virtual IP Address: *

Virtual Hostname:

Locality

SuperNode: Super1

Location: Boston

Region: Eastern USA

Pre-position Disk Space

Set Pre-position Disk Space for Content Engines in this cluster to: * 0 (GB)

Comments

Comments:

Content Engines

Content Engine Name	Allocated Pre-position Space (GB)	Minimum Pre-position Space (GB)	Maximum Pre-position Space (GB)

Step 5 Under the General Configuration heading, enter the name of the new cluster in the Cluster Name field.

Note You may wish to use a name that makes it easy to distinguish this group of Content Engines from others behind the same supernode.

Step 6 In the Virtual IP Address field, enter the static IP address for the cluster. This is the public IP address that end users link to when requesting content from the hosted domain. This address must be supplied by your DNS server.

Step 7 In the Virtual Hostname field, enter a DNS host name for the cluster. This host name is used in place of the Content IP address to represent the cluster to CDN users. This address must be supplied by your DNS server.

Note If your virtual IP address can be resolved back to a DNS address, the virtual host name value is optional.

Step 8 Under the Pre-position Disk Space heading, enter the amount of pre-positioned disk space (in gigabytes) that will be allocated on each Content Engine assigned to this cluster. Pre-positioned disk space is hard disk space on each Content Engine that is reserved for storing video-on-demand and other content for user requests.

Note Disk space allocations for pre-positioning content on Content Engines through the cluster take precedence over and, if necessary, overwrite other pre-positioned disk space allocations for devices.

Step 9 If you wish, in the Comments field, enter a text description to accompany the cluster. This step is optional. (Comments do not appear to end users.)

Step 10 Under the Content Engines heading, choose the name of the Content Engine you wish to add to this cluster. Content Engines cannot belong to more than one cluster, and Content Engines that have already been added to a cluster are not listed.

Note Content Engines that are members of clusters cannot have names that contain spaces.

Step 11 Click **OK** to create the new cluster.

The Content Distribution Manager uses the addresses you supplied to group the selected Content Engines into a new cluster.

Creating a Hosted Domain for a Content Provider

A hosted domain is a group of related content that is being hosted on a CDN and distributed on behalf of a content provider.

A given content provider can define multiple hosted domains containing different sets of content on the CDN.

Each hosted domain has the following characteristics:

- It is associated with a content provider.
- It stores the address of the content provider origin server from which the hosted content originates and from which the Content Engines retrieve their content for caching.
- It is assigned a unique, fourth-level domain called the hosted domain name, which is used in URLs pointing to CDN content.
- Its name corresponds to a real, delegated domain that has already been configured on your DNS server.
- It is associated with one or more Content Engines that store pre-positioned video-on-demand content for the content provider.

The content provider modifies its web page to point to content stored on the CDN, replacing URLs on its web page with the appropriate CDN URL. See the "Publishing URLs That Link to CDN Content" section on page 2-19.

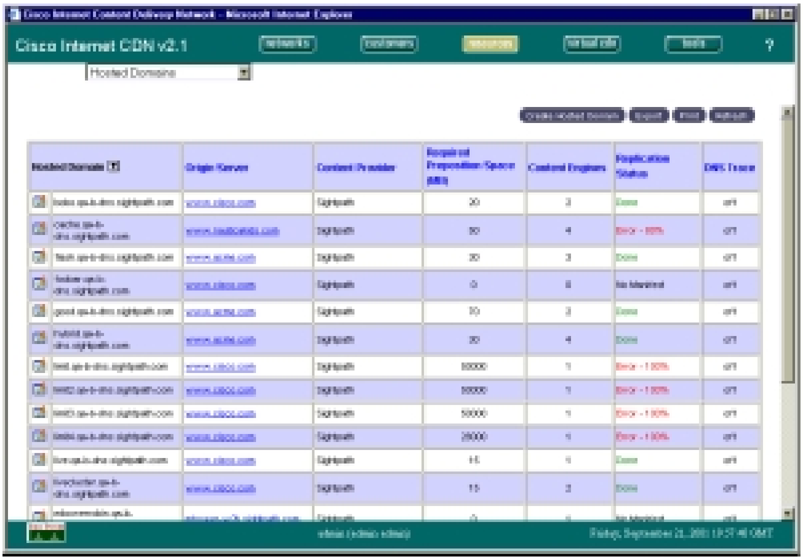
To create a hosted domain, follow these steps:

Step 1 From the Cisco Internet CDN Software user interface, click **resources**.

Step 2 From the drop-down list, choose **Hosted Domains**.

The View Hosted Domains page appears. (See Figure 2-16.)

Figure 2-16 View Hosted Domains

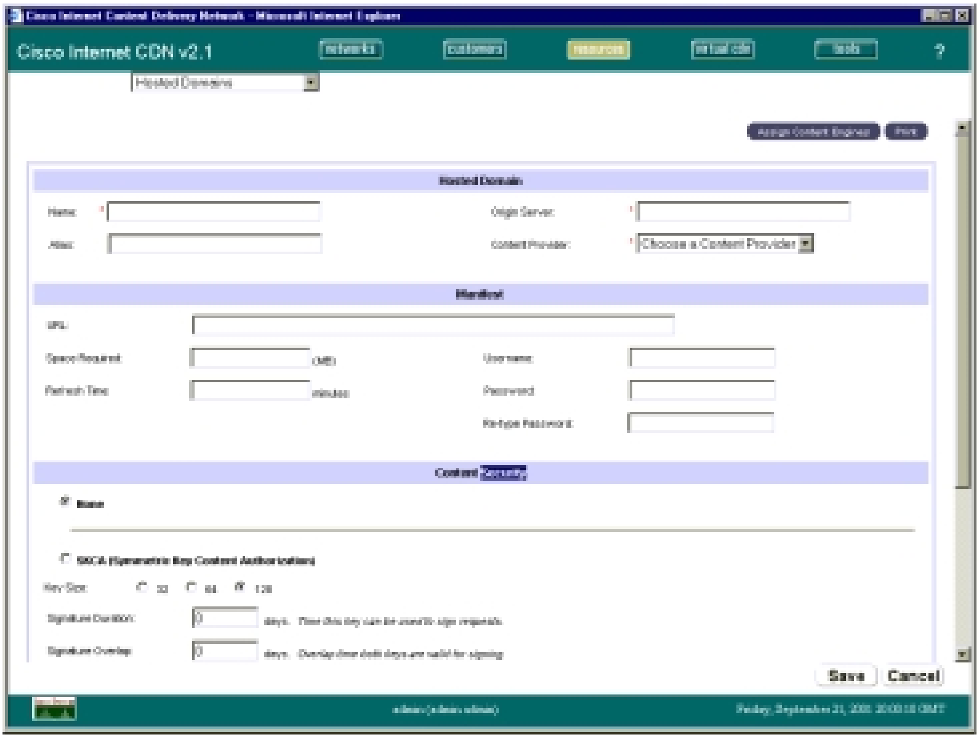


Hosted Domain	Origin Server	Content Provider	Required Prepositioned Space (MB)	Content Engines	Replication Status	DNS Trace
[illegible].qa-li-dns.sightpath.com	www.cisco.com	Sightpath	20	2	Done	off
cache.qa-li-dns.sightpath.com	www.[illegible].com	Sightpath	50	4	Error - 80%	off
flash.qa-li-dns.sightpath.com	www.acme.com	Sightpath	20	3	Done	off
[illegible].qa-li-dns.sightpath.com	www.cisco.com	Sightpath	0	0	No Manifest	off
good.qa-li-dns.sightpath.com	www.acme.com	Sightpath	70	2	Done	off
hybrid.qa-li-dns.sightpath.com	www.acme.com	Sightpath	20	4	Done	off
[illegible].qa-li-dns.sightpath.com	www.cisco.com	Sightpath	10000	1	Error - 100%	off
[illegible].qa-li-dns.sightpath.com	www.cisco.com	Sightpath	10000	1	Error - 100%	off
[illegible].qa-li-dns.sightpath.com	www.cisco.com	Sightpath	50000	1	Error - 100%	off
[illegible].qa-li-dns.sightpath.com	www.cisco.com	Sightpath	25000	1	Error - 100%	off
live.qa-li-dns.sightpath.com	www.cisco.com	Sightpath	15	1	Done	off
[illegible].qa-li-dns.sightpath.com	www.cisco.com	Sightpath	15	2	Done	off
[illegible].qa-li-	[illegible].sightpath.com	Sightpath	0	0	No Manifest	off

Step 3 Click **Create Hosted Domain**.

The Create a Hosted Domain page appears. (See Figure 2-17.)

Figure 2-17 Create a Hosted Domain



Hosted Domain

Name: *
Alias:
Origin Server: *
Content Provider: * Choose a Content Provider

Manifest

URL:
Space Required: (MB)
Refresh Time: minutes
Username:
Password:
Retype Password:

Content Security

● None

○ SKCA (Symmetric Key Content Authorization)

Key Size: ○ 32 ○ 64 ● 128
Signature Duration: 0 days.
Signature Overlap: 0 days.

Step 4 Under the Hosted Domain heading, enter a valid CDN hosted domain name in the Name field, using the following guidelines:

- The hosted domain name must be a valid, fourth-level delegated domain name, for example:

  `www.cdn.cisco.com`

- The hosted domain name *does not* contain underscore (_) characters.
- The first part of the domain name (*www* in the example above) is open, and can be defined by you when you create the hosted domain name.

- The remaining subdomain (the three segments after the first dot) must correspond to a delegated domain created on your DNS server to provide a functional mapping for the Content Routers.
- The CDN must be given the right to act as the authoritative DNS server for the subdomain you specify.

Step 5 In the Origin Server field, enter the name or IP address of the origin website of the content provider’s content, for example:

```
www.cisco.com
```

Your Origin Server field *cannot* contain a path to a subdirectory on the server. The following example is *not* a valid origin server address:

```
www.cisco.com/support
```

Step 6 From the Content Provider drop-down list, choose the content provider whose content will be stored on this hosted domain.

If you have not added any content providers to the CDN yet, see the “Adding Content Providers” section on page 2-22 for instructions on doing so before continuing.

Step 7 In the Alias field, enter an optional alias for the hosted domain. For example, if your hosted domain name is:

```
www.cdn.cisco.com
```

but you want to use a third-level as opposed to a fourth-level domain name on all your published links, you can use the Alias field to map a third-level domain name to your host domain name such as:

```
www.cisco-cdn.com
```

Note You must provide a CNAME mapping between the delegated domain and your alias on the DNS server before aliasing will work. Entering your alias on the Create a Hosted Domain page is not sufficient to enable hosted domain aliasing.

Step 8 Under the Manifest heading, identify the manifest file that will be used by this hosted domain to coordinate the delivery of live and video-on-demand content. See the "Creating a Manifest File for Importing Media" section on page 2-3 for more information on creating manifest files.

a. In the URL field, enter the Internet address of the manifest file for this hosted domain. For example:

```
http://www.cisco.com/manifest/manifest.xml
```

b. In the Space Required field, enter the amount of disk space (in megabytes) that needs to be reserved on the Content Engines to cache the content named in the manifest file.

c. In the Refresh Time field, enter the frequency (in minutes) with which Content Engines assigned to the hosted domain should check for updates to the manifest file. Once Content Engines detect a change in the manifest file, the file is retrieved ("fetched") and read. New content is then served in accordance with the updated manifest file instructions. Old content (media files cached, but no longer pointed to by the manifest) is purged from the Content Engines.

d. If you wish, set up a username and password required to retrieve the manifest file. This step is optional. Enter a username in the Username field, and then enter and verify the password in the Password and Re-type Password fields provided.

Step 9 If you wish, enter notes about the Hosted Domain or instructions for other users in the Comments field. This step is optional. Comments are for internal use only and are not accessible to end users.

Step 10 Click **Save** to create the new hosted domain.

Before you can begin serving content from the new hosted domain, you must first assign Content Engines to it. See the next section, "Assigning Content Engines to Hosted Domains."

Assigning Content Engines to Hosted Domains

Once you have created a hosted domain using the Content Distribution Manager, you need to assign it to one or more Content Engines from which its content will be served.

Content Engines may be grouped together into supernodes, or act as standalone nodes. Within a given supernode, there may be one or more groupings of Content Engines, referred to as clusters. Nodes and supernodes are in turn grouped by region and location. Alternatively, clusters and nodes can be viewed according to the virtual CDN to which they belong.

To assign Content Engines to your hosted domain:

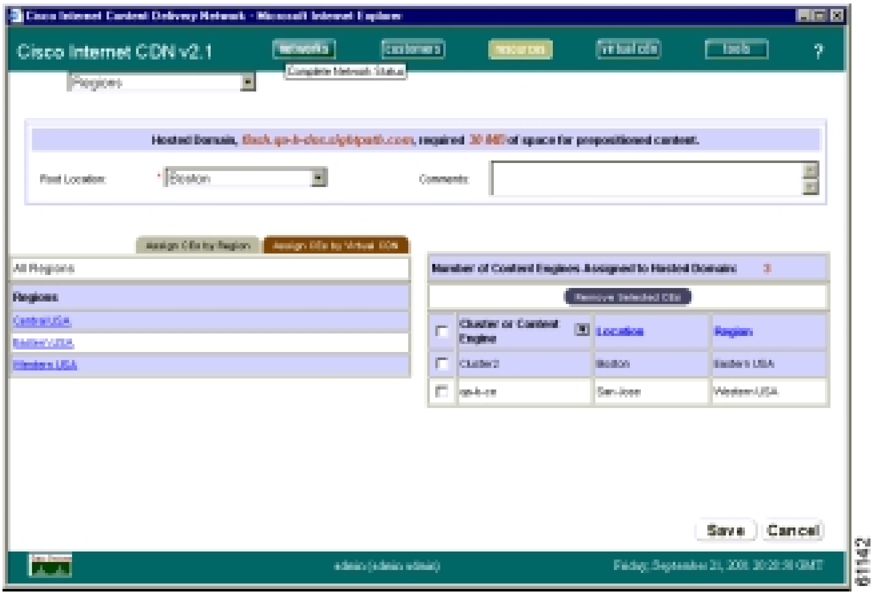
Step 1 From the Cisco Internet CDN Software user interface, click **resources**.

Step 2 From the drop-down list, choose **Hosted Domains**. The View Hosted Domains page appears (see Figure 2-16), listing the hosted domains on your CDN.

Step 3 Follow the instructions for modifying an existing hosted domain in the "Modifying Hosted Domains" section on page 3-36 to open your hosted domain for editing.

Step 4 Click the **Assign Content Engines** button. The browser refreshes to display the Assign Content Engines to Hosted Domains page. (See Figure 2-18.) A list of Content Engines to which the hosted domain is assigned appears.

Figure 2-18 Assign Content Engines to Hosted Domains



Hosted Domain, [illegible], required 30 MB of space for prepositioned content.

Root Location: * Boston

Comments:

All Regions

Regions
Central USA
Eastern USA
Western USA

Number of Content Engines Assigned to Hosted Domain: 2

□	Cluster or Content Engine	Location	Region
□	Cluster2	Boston	Eastern USA
□	qa-k-ce	San Jose	Western USA

admin (admin admin)

Friday, September 21, 2001 20:20:38 GMT

Step 5 Click the **Assign CEs by Region** or **Assign CEs by Virtual CDN** tab.

Note Virtual CDNs are groupings of Content Engines that are independent of the Content Engines’ geographical location. Virtual CDNs can be created to respond to the particular needs of a CDN.

Step 6 Choose the region or virtual CDN containing the Content Engines that you wish to assign to the hosted domain. A list of locations in the region or clusters in the virtual CDN appears.

If you are assigning Content Engines by regions, click the name of the location in your region containing the Content Engines you wish to assign; otherwise, go to Step 7.

Step 7 Check the check box adjacent to the name of the cluster or Content Engine with which you wish to associate the hosted domain.

Step 8 Click the **Add Selected CEs** button. The list of clusters or Content Engines to which the hosted domain is assigned refreshes, listing the newly added Content Engine or cluster.

Step 9 From the Root Location drop-down menu, choose a root location for the hosted domain.

The *root location* is the location within the CDN content distribution hierarchy from which content is replicated. Content replication is handled by the lead Content Engine in the root location to lead Content Engines in nonroot locations. Once it is replicated to the lead Content Engine in each location, content is then distributed to all nonlead Content Engines in the location.

Step 10 Click **Save**.

Activating Windows Media Services for a Hosted Domain

If you will be serving Windows Media content from a hosted domain using a Windows Media Server, you must first activate Windows Media Services on each hosted domain that will be serving the Windows Media content.

Make sure that all Content Engines on your hosted domain are running Version 2.1 or later of the Cisco Internet CDN Software before enabling Windows Media Services on the hosted domain. Although it is possible for a hosted domain to contain Content Engines that are running different versions of the Cisco Internet CDN Software, Content Engines that using versions of the CDN software earlier than Version 2.1 are not able to serve Windows Media content.

Note Before activating Windows Media Services, you must first have purchased licenses for Windows Media Services for each of the Content Engines in each of the hosted domains that will be serving content using a Windows Media Server.

To activate Windows Media Services on a hosted domain:

Step 1 Enable Windows Media Services on your CDN. See the "Modifying Windows Media Services Configuration" section on page 4-13 for details.

Step 2 From the Cisco Internet CDN Software user interface, click **resources**.

From the drop-down list, choose **Hosted Domains**. The View Hosted Domains page appears (see Figure 2-16), listing the hosted domains on your CDN.

Step 3 Click the edit icon next to the name of the hosted domain you wish to edit. The Create a Hosted Domain page appears. (See Figure 2-17.)

Step 4 Check the **Enable WMT on all Content Engines assigned to this Hosted Domain** check box. Each Content Engine on the hosted domain will restart with the Windows Media Server enabled.

Step 5 Click **Save**. You are returned to the View Hosted Domains page.

Step 6 Repeat Step 3 through Step 5 for each hosted domain on which you wish to enable Windows Media Services.

Configuring Content Security for Hosted Domains

The Cisco Internet CDN offers content providers the option of securing CDN content using Symmetric Key Content Authorization (SKCA).

Using this form of content security, content providers "sign" all user requests with a unique "symmetric key"—essentially a powerful algorithm that is used to encrypt string values. Each hosted domain on which content security is enabled has its own set of symmetric keys. The content provider has access to all symmetric keys. In this case, the input string from which the encrypted "signature" is derived from a combination of authentication information from the original user request. The resulting encrypted string, or Message Authentication Code (MAC), is appended to the request along with the (unencrypted) authentication variables. The entire request string is then forwarded from the content provider to the Content Engine.

Once the Content Engine receives the secure request, it first determines which symmetric key was used to sign the request. Once the symmetric key is located, the Content Engine inserts the unencrypted authentication variables into the symmetric key. If the value that is produced matches the MAC on the incoming request, the Content Engine attempts to serve the request to the user, checking first to make sure that the requested URL has not expired.

If the value that is produced does not match the MAC on the incoming request, the Content Engine rejects the request and redirects the requesting client to an error message page.

For instructions on viewing a hosted domain’s symmetric keys, see the “Viewing Symmetric Keys” section on page 4-10.

To configure content security for a hosted domain:

Step 1 From the Cisco Internet CDN Software user interface, click **resources**.

Step 2 From the drop-down list, choose **Hosted Domains**. The View Hosted Domains page appears (see Figure 2-16), listing the hosted domains on your CDN.

Step 3 Click the icon next to the name of the hosted domain on which you want to enable content security.

The Modify a Hosted Domain page appears. (See Figure 3-7.)

Step 4 Click the **SKCA (Symmetric Key Content Authorization)** button to enable content security on the hosted domain.

Step 5 Use the fields provided to configure content authentication as follows:

- **Key size**—Select a key size by clicking the appropriate button: 32, 64, or 128 bit. The size selected determines the number of bits in the key.
- **Signature Duration**—Enter a value representing the number of days a key can be used to sign user request URLs. Once a key has expired, it can no longer be used to sign user requests.
- **Signature Overlap**—Enter a value representing the number of days during which two keys are valid for signing and verifying user requests.

Step 6 In the Error URL field, enter the address of the web page that you wish to display whenever content cannot be served.

This error page will display the invalid request URL and an error code, both of which are generated by the Content Engine.

For an explanation of the content authentication errors, see Appendix A, “Error and Event Messages.”

Step 7 In the Key Access Password field, enter a value that will serve as a secure password that must be entered by any CDN user wishing to view the symmetric key for the hosted domain.

Step 8 Reenter the password value in the Retype Key Access Password field to verify that the value you entered is correct.

Step 9 Click **Save**. The hosted domain is updated with the new symmetric key information.

If you need to update the symmetric key password, see the "Changing the Symmetric Key Password" section on page 4-11.

Replicating Content from the Origin Server to a Hosted Domain

Once you have created your hosted domain, assigned Content Engines to it, and linked your hosted domain to a manifest file that identifies the content to be hosted, you are ready to copy content from your origin server to the hosted domain. This process is referred to as "fetching" content from the origin server and "replicating" or "pre-positioning" it on the Content Engines that belong to your hosted domain.

Note By its very nature, live content is not fetched from the origin server or the live streaming server. Instead, manifest file entries prepare Content Engines to properly handle and direct live content requests.

To fetch content from your origin server and replicate it to your Content Engines:

Step 1 From the Cisco Internet CDN Software user interface, click **resources**.

Step 2 From the drop-down list, choose **Hosted Domains**. The View Hosted Domains page (see Figure 2-16) appears.

Step 3 Follow the instructions for modifying an existing hosted domain in the "Modifying Hosted Domains" section on page 3-36 to open your hosted domain for editing.

Step 4 Verify that the URL field points to the correct manifest file (with an XML extension) for the hosted domain.

Step 5 Click **Fetch Manifest**. You are prompted to confirm your decision to begin copying the content named by the manifest file to the Content Engines assigned to the hosted domain.

Step 6 Click **OK**. You are returned to the View Hosted Domains page. (See Figure 2-16.)

Step 7 You can view the status of media replication from the origin server to your Content Engines at any time. See the "Viewing the Status of Content Replication to a Hosted Domain" section on page 3-43 for instructions.

Setting the Responsible Person Address for the CDN

Using the Routing Properties feature of the Cisco Internet CDN Software, you can set the responsible person (RP) contact information for the hosted domains on your CDN. The RP address is used to report problems to your domain administrator.

To configure the responsible person address:

Step 1 From the Cisco Internet CDN Software user interface, click **tools**.

Step 2 From the drop-down list, choose **Routing Properties**. Fields displaying the coverage zones and CDN-specific configuration settings used by your DNS server appear.

Step 3 In the Email Address field, enter the full e-mail address for the RP account to which messages regarding the CDN domain can be sent.

Step 4 Click **Save** to save changes to the RP e-mail account.

Creating a Virtual CDN

A virtual CDN is a logical grouping of Content Engines and clusters that provides an alternative to region and location groupings when you view, manage, and assign Content Engines.

Once assigned to a hosted domain, Content Engines or clusters distribute the content from content providers.

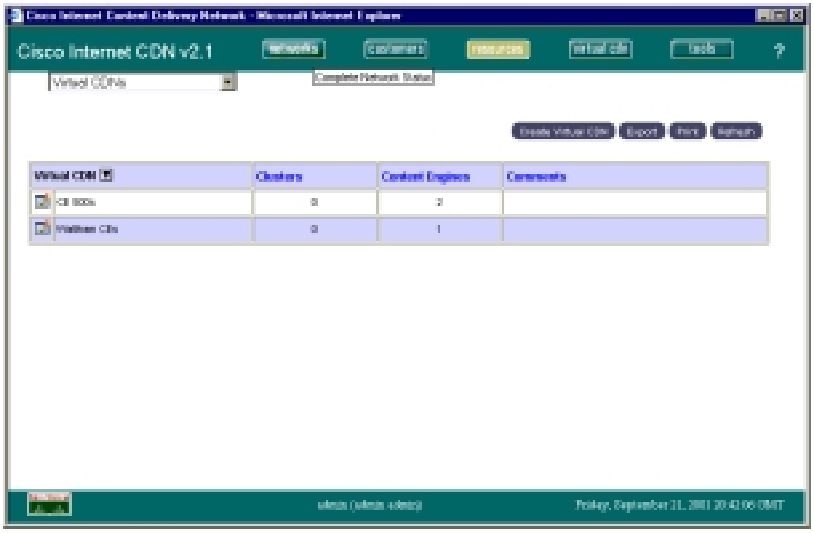
To create a virtual CDN, follow these steps:

Step 1 From the Cisco Internet CDN Software user interface, click **virtual cdn**.

The View Virtual CDNs page appears. (See Figure 2-19.)

Tips Alternatively, you can access the View Virtual CDNs page by clicking **resources** and then choosing **Virtual CDNs** from the drop-down list.

Figure 2-19 View Virtual CDNs

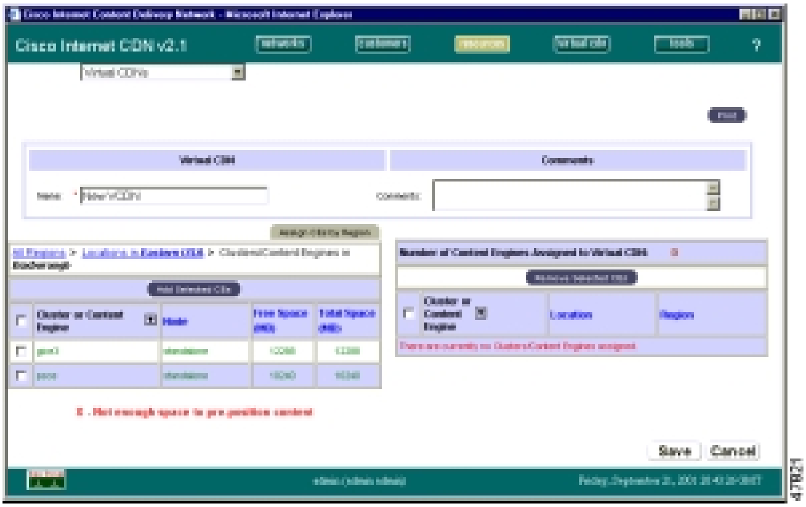


Virtual CDN	Clusters	Content Engines	Comments
CE 500s	0	2	
Waltham CEs	0	1	

Step 2 Click the **Create Virtual CDN** button.

The Create a Virtual CDN page appears. (See Figure 2-20.)

Figure 2-20 Create a Virtual CDN



Step 3 Under the Virtual CDN heading, in the Name field, enter a name for the virtual CDN.

Step 4 In the Comments field, enter a description for the virtual CDN that is useful to you. (This step is optional.) Although it is not required, you may want to assign your Content Engines and Content Engine clusters to the virtual CDN that you are creating at this time.

Step 5 Click the **Assign CEs by Region** tab. The page refreshes, displaying a list of defined regions.

Step 6 Click the name of the region containing the first Content Engines that you wish to assign. A table displaying the locations defined for the region appears.

Step 7 Click the name of the location containing the first Content Engines that you wish to assign. A table listing the Content Engines and Content Engine clusters in the location appears.

Step 8 Check the check box next to each Content Engine or cluster that you wish to add to the virtual CDN, or check the check box in the column header to choose all devices in the list.

Step 9 Click the **Add Selected CEs** button to add the Content Engines or clusters to the virtual CDN. The list of assigned Content Engines refreshes to include the newly added Content Engine.

Step 10 Repeat Step 6 through Step 9 for each Content Engine or cluster that you wish to add to the newly created virtual CDN.

Step 11 Click **Save** to create your new virtual CDN.

For instructions on modifying the list of assigned Content Engines and clusters after you have created your virtual CDN, see the next section, "Assigning Content Engines to Virtual Content Delivery Networks."

Assigning Content Engines to Virtual Content Delivery Networks

A Content Engine or Content Engine cluster can be assigned to one or more virtual CDNs at any time. To assign a Content Engine to a virtual CDN:

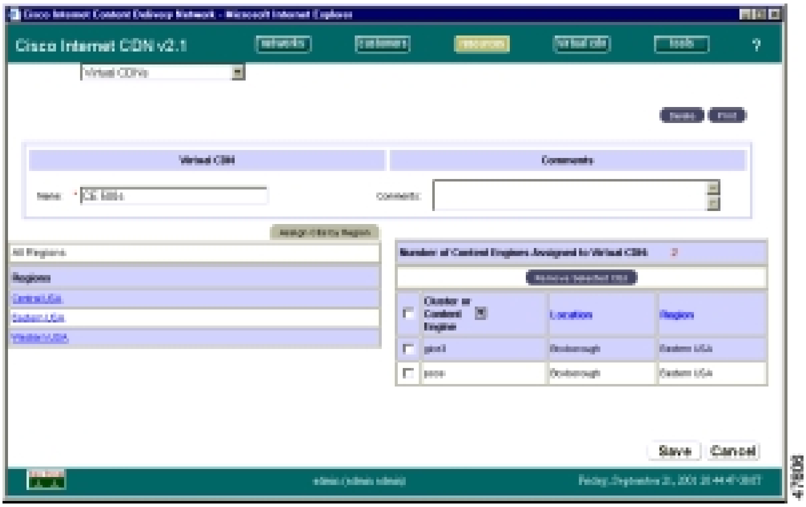
Step 1 From the Cisco Internet CDN Software user interface, click **virtual CDN**. The View Virtual CDNs page appears. (See Figure 2-19.)

Step 2 Click the icon next to the name of the virtual CDN to which you want to assign a Content Engine.

The Modify a Virtual CDN page appears. (See Figure 2-21.)

Step 3 Click the **Assign CEs by Region** tab. The page refreshes, displaying a list of defined regions.

Figure 2-21 Modify a Virtual CDN



Step 4 Choose the name of the region containing the first Content Engines that you wish to assign. A table displaying the locations defined for the region appears.

Step 5 Choose the name of the location containing the first Content Engines that you wish to assign. A table listing the Content Engines and clusters in the location appears.

Step 6 Check the check box next to each Content Engine or cluster that you wish to add to the virtual CDN, or click the check box in the column header to choose all devices in the list.

Step 7 Click the **Add Selected CEs** button to add the Content Engines or clusters to the virtual CDN.

Step 8 Repeat Step 4 through Step 7 for each Content Engine or cluster that you wish to add to the virtual CDN.

Step 9 Click **Save** to update the virtual CDN with the new Content Engines or clusters.

Creating User Accounts

You can use the user administration feature of the Content Distribution Manager to create login accounts to access the Cisco Internet CDN Software user interface. Accounts can be created for administrator, operations, and guest-level login accounts.

Note All user names must be unique. There cannot be duplicate user names on the CDN, even if the users have different permission levels.

For detailed information on the purpose of each type of account, see the "CDN Users" section on page 1-18.

To create a new user account:

Step 1 From the Cisco Internet CDN Software user interface, click **tools**.

The View Content Engine Statistics page appears.

Step 2 From the drop-down list, choose **User Administration**.

The View User Accounts page appears, listing existing user accounts.

Step 3 Click the **Create User** button. The User Account Configuration page appears.

Step 4 Under the User Account heading, configure the user account with the following required information:

a. Enter the user login name into the Username field, for example:

```
jchambers
```

b. In the Password field, enter the password to be used for the user account.

c. Reenter the password in the Re-type Password field.

d. From the Role drop-down list, choose a user role for the account, for example:

```
operations
```

Step 5 Under the Personal Information heading, enter contact information for the individual associated with this user account as follows:

a. In the First Name and Last Name fields, enter the name of the contact associated with this user account. These fields are required.

b. Optionally, in the Job Title field, enter the title of the contact.

c. Optionally, in the Department field, enter the department associated with the contact.

d. Optionally, in the Phone field, enter the phone number of the contact.

e. Optionally, in the Email field enter the e-mail address of the contact.

Step 6 Optionally, in the Comments field, enter any comments associated with this contact.

Step 7 Click **Save**. The account is added to the list of user accounts.

Working with Cisco Internet CDN Software

This chapter provides information about modifying CDNs and using the system tools for changing system passwords, setting up remote logging, and updating Cisco Internet CDN Software on your Cisco CDN devices.

This chapter contains the following sections:

Working with Regions and Locations

By default, Content Engines and Content Routers are grouped by geographical region and location. Because physical proximity bears a direct relationship to response time when serving user requests, it is useful to be able to group your Content Routers and the Content Engines that will be serving content according to their physical location.

However, you may also need to group your CDN according to other criteria. Using the virtual CDN feature, you can group Content Engines in whatever manner suits your organization—by hardware type or any other criteria that seem appropriate. Refer to the "Creating a Virtual CDN" section on page 2-60 for more information on setting up virtual Content Delivery Networks or the "Working with Virtual Content Delivery Networks" section on page 3-7 for help modifying or removing virtual Content Delivery Networks.

Working with regions and locations entails:

- Modifying Regions
- Deleting Regions
- Modifying Locations
- Deleting Locations

Modifying Regions

To modify a region, follow these steps:

Step 1 From the Cisco Internet CDN Software user interface, click **resources**.

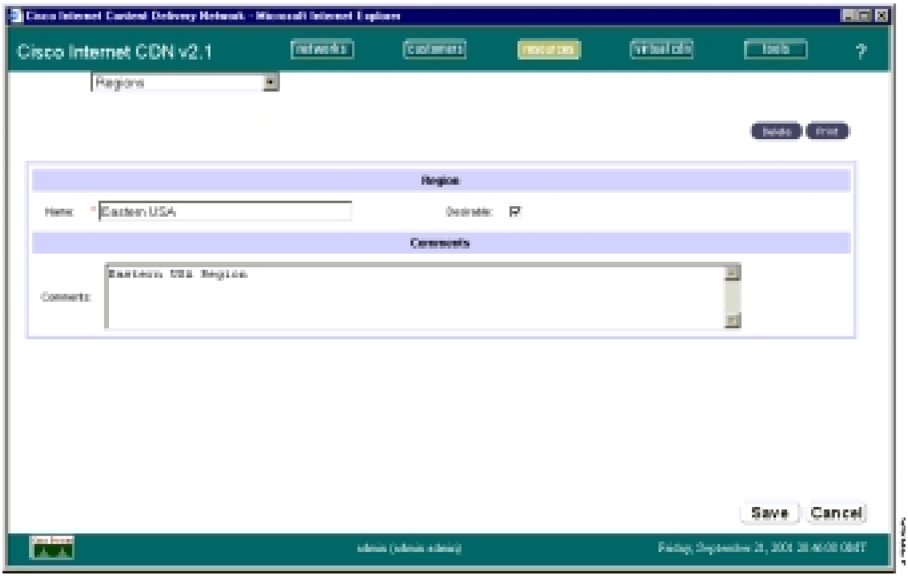
Step 2 From the drop-down list, choose **Regions**.

The View Regions page appears. (See Figure 2-3.)

Step 3 Click the edit icon next to the name of the region that you want to modify.

The Modify a Region page appears. (See Figure 3-1.)

Figure 3-1 Modify a Region



Name: * Eastern USA

Desirable: ☑

Comments: Eastern USA Region

Step 4 Enter a new name or description as needed in the Name field.

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

Step 5 If needed, check or uncheck the **Desirable** check box to change the desirability of a region.

A desirable region is one to which you can route any end user request (regardless of the geographic origin of the request) because of the existence of robust network connectivity.

Most regions in the United States are desirable regions because network connectivity in the United States is generally very good. Network connectivity in other parts of the world may not be as robust, so if an end user request is received from Asia, you might not want to route the request to Africa, for example. However, routing the Asian request to anywhere in the United States would be acceptable.

Step 6 Click **Save**.

Deleting Regions

To delete a region, follow these steps:

Step 1 From the Cisco Internet CDN Software user interface, click **resources**.

Step 2 From the drop-down list, choose **Regions**.

The View Regions page appears. (See Figure 2-3.)

Step 3 Click the edit icon next to the region that you want to delete.

Note A region can be deleted only if it does not have assigned locations. You can reassign a location from one region to another region if necessary. See the "Modifying Locations" section on page 3-5.

Step 4 Click **Delete**. You are prompted to confirm your decision to delete the region.

Step 5 Click **OK**.

Modifying Locations

To modify a location, follow these steps:

Step 1 From the Cisco Internet CDN Software user interface, click **resources**.

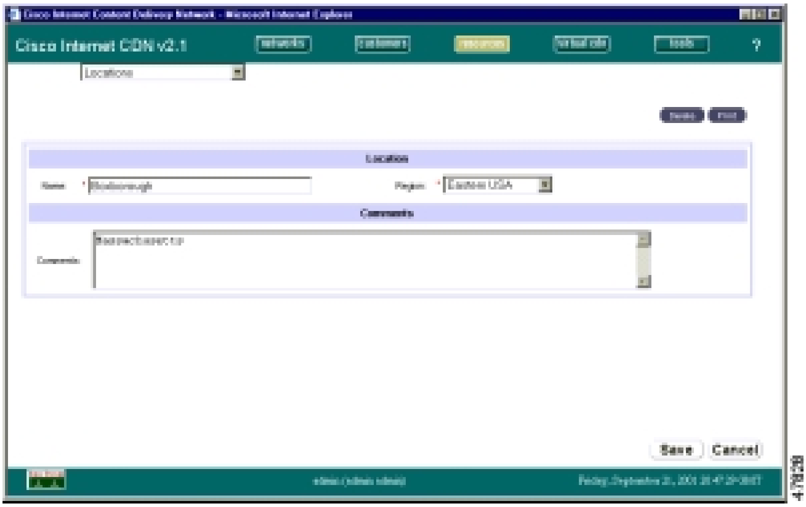
Step 2 From the drop-down list, choose **Locations**.

The View Locations page appears. (See Figure 2-5.)

Step 3 Click the edit icon next to the name of the location that you want to modify.

The Modify a Location page appears. (See Figure 3-2.)

Figure 3-2 Modify a Location



Name: * Boxborough
Region: * Eastern USA

Step 4 Enter a new name or description as needed.

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

Step 5 If needed, change the location to a different region by choosing a region from the **Region** drop-down list.

You must specify a region that is associated with the location.

Step 6 Click **Save**.

Deleting Locations

You can delete locations as needed, as long as they are not the root locations of activated Content Engines or Content Routers.

Note If a location has a Content Engine or Content Router assigned to it, you can first assign the Content Engine or Content Router to another location and then delete the original location.

To delete a location, follow these steps:

Step 1 From the Cisco Internet CDN Software user interface, click **resources**.

Step 2 From the drop-down list, choose **Locations**.

The View Locations page appears. (See Figure 2-5.)

Step 3 Click the edit icon next to the location that you want to delete.

The Modify a Location page appears. (See Figure 3-2.)

Step 4 Click **Delete**. You are asked to confirm your decision to delete the location.

Step 5 Click **OK**.

Working with Virtual Content Delivery Networks

Using the virtual CDN feature of the Content Distribution Manager, you can modify information about a virtual Content Delivery Network (CDN) or remove a virtual CDN from the system.

You work with Virtual Content Delivery Networks by:

- Modifying a Virtual Content Delivery Network
- Deleting a Virtual Content Delivery Network

Modifying a Virtual Content Delivery Network

To modify a virtual Content Delivery Network:

Step 1 From the Cisco Internet CDN Software user interface, click **virtual cdn**. The View Virtual CDNs page appears.) (See Figure 2-19.)

Step 2 Click the edit icon next to the name of the virtual CDN that you wish to edit. The browser window refreshes, displaying the Modify a Virtual CDN page. (See Figure 2-21.)

Step 3 Modify the virtual CDN name by entering a new value in the Name field.

The name must be unique and should be a name that is useful in distinguishing the virtual CDN from others on your system.

Step 4 Optionally, enter any notes about the virtual CDN in the Comments field.

Step 5 If you want to modify the list of Content Engines or clusters assigned to the virtual CDN, see the next section, "Adding and Removing Content Engines from a Virtual CDN."

Step 6 Click **Save** to save your modifications to the virtual CDN. The browser window refreshes, listing the updated virtual CDNs.

Adding and Removing Content Engines from a Virtual CDN

To add or remove Content Engines or clusters from a virtual CDN:

Step 1 From the Cisco Internet CDN Software user interface, click **virtual cdn**. The View Virtual CDNs page appears.) (See Figure 2-19.)

Step 2 Click the edit icon next to the name of the virtual CDN that you wish to edit. The browser window refreshes, displaying the Modify a Virtual CDN page. (See Figure 2-21.)

Step 3 Click the **Assign CEs by Region** tab.

Step 4 Choose the region in which the Content Engines reside. A list of locations in the region or clusters in the virtual CDN appears.

Step 5 Choose the name of the location for the Content Engines. A list of the Content Engines and clusters in that location appears.

Note As you move down from regions to locations, your path is saved in the header area just above the **Add Selected CEs** button. Click the **All Regions** or location link to back up and change your location.

Step 6 Check the check box adjacent to the name of the cluster or Content Engine that you wish to associate with, or remove from, the virtual CDN.

Note To choose all Content Engines, choose the topmost check box next to the Cluster or Content Engine heading.

Step 7 Click **Add Selected CEs,** and then click **Save**.

The list of clusters or Content Engines to which the hosted domain is assigned refreshes, listing the newly added Content Engine or cluster.

Step 8 To remove Content Engines, check the box next to the name of the Content Engine that you wish to remove from this list and click **Remove Selected CEs**.

Step 9 Click **Save**. The browser window refreshes, listing the updated virtual CDNs. The list of Content Engines shows the updated count for the virtual CDN.

Deleting a Virtual Content Delivery Network

To delete a virtual CDN:

Step 1 From the Cisco Internet CDN Software user interface, click **virtual cdn**. The View Virtual CDNs page appears.) (See Figure 2-19.)

Step 2 Click the edit icon next to the name of the virtual CDN that you wish to edit. The browser window refreshes, displaying the Modify a Virtual CDN page. (See Figure 2-21.)

Step 3 Click **Delete**. You are prompted to confirm your decision to delete the virtual CDN.

Step 4 Click **OK**. The browser window refreshes with an updated list of virtual CDNs.

Working with Content Distribution Managers

You work with Content Distribution Managers by deleting a warm standby Content Distribution Manager.

Deleting a Warm Standby Content Distribution Manager

You can delete a warm standby Content Distribution Manager from the CDN at any point after you have registered the device and before the device has come online as the primary Content Distribution Manager. Once the device has been called into use as the primary Content Distribution Manager, however, you cannot delete it using the Content Distribution Manager user interface.

Delete a warm standby Content Distribution Manager when the device is experiencing unresolvable problems or when its network address or configuration has changed and you need to add the device back to the CDN using its new address and configuration information.

When deleting a warm standby Content Distribution Manager from the CDN, you are effectively removing that device and the content it contains from the routing scheme that the CDN software uses to fill user requests. Should your primary Content Distribution Manager fail during the time that the warm standby is deleted, there will be no failover for the Content Distribution Manager.

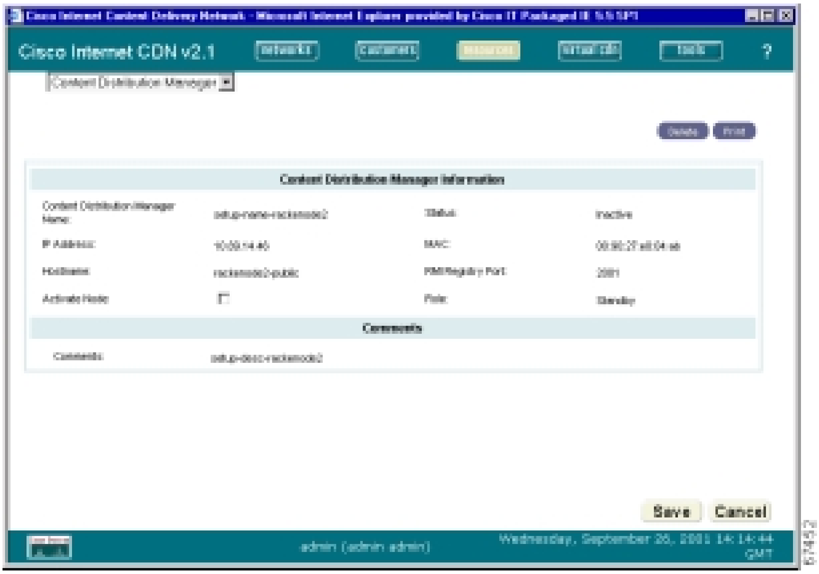
To delete a warm standby Content Distribution Manager:

Step 1 From the Cisco Internet CDN Software user interface, click **resources**.

Step 2 From the drop-down list, choose **Content Distribution Manager**. The browser refreshes, listing the Content Distribution Managers on your CDN. The warm standby Content Distribution Manager is identified as *Standby.*

Step 3 Click the edit icon next to the name of the warm standby Content Distribution Manager that you wish to delete. The browser window refreshes, displaying the Modify a Content Distribution Manager page. (See Figure 3-3.)

Figure 3-3 Modify a Content Distribution Manager


Cisco Internet Content Delivery Network - Microsoft Internet Explorer provided by Cisco IT Packaged IE 5.5 SP1
Cisco Internet CDN v2.1
networks
customers
resources
virtual cdn
tools
?
Content Distribution Manager
Delete
Print
Save
Cancel
57452

Content Distribution Manager Information

Content Distribution Manager Name:	setup-name-racknode2	Status:	Inactive
IP Address:	10.09.14.46	MAC:	00:90:27:a8:04:ab
Hostname:	racknode2-public	RMI Registry Port:	2001
Activate Node:	□	Role:	Standby

Comments

Comments: setup-desc-racknode2

admin (admin admin)

Wednesday, September 26, 2001 14:14:44 GMT

Step 4 Click **Delete**. You are prompted to confirm your decision.

Step 5 Click **OK** to execute your request. You are returned to the View Content Distribution Managers page, which lists the remaining Content Distribution Manager on your CDN.

Step 6 To complete the process of deleting the warm standby Content Distribution Manager offline, shut down the device by logging directly in to the Content Distribution Manager you deleted and accessing the command-line interface (CLI) using the admin account and password:

a. At the prompt, enter **enable** to enable the administrative mode, for example:

```
device_name> enable
```

The prompt changes to a pound sign (#) to indicate that you are in administrative mode.

b. Enter **shutdown** to stop the Cisco Internet CDN Software and shut down the device.

Working with Content Engines

You work with Content Engines by:

- Modifying Content Engines
- Modifying Content Engine Passwords
- Stopping, Shutting Down, Restarting, and Rebooting a Content Engine
- Deleting a Content Engine
- Viewing Content Engine Statistics

Modifying Content Engines

Use the resources feature of the Content Distribution Manager to make changes to the name of a Content Engine from the Content Distribution Manager user interface.

You can modify a Content Engine by changing the following items:

- Name
- Location
- Root and HTTP passwords
- Description
- Content IP address
- Content host name
- Pre-positioned disk space

Note Changing the location of pre-positioned disk space will cause the Content Engine to restart.

To modify a Content Engine, follow these steps:

Step 1 From the Cisco Internet CDN Software user interface, click **resources.**

Step 2 From the drop-down list, choose **Content Engines**. The View Content Engines page (see Figure 2-10) appears, listing the Content Engines on your CDN.

Step 3 Click the edit icon next to the name of the Content Engine that you wish to edit. The browser window refreshes, displaying the Modify a Content Engine page. (See Figure 2-11.) Fields for editing the selected Content Engine appear.

Step 4 If you choose to, enter the new name of the Content Engine in the Content Engine Name field. Otherwise, proceed to the next step.

Step 5 If you choose to, modify the description used to identify the Content Engine by entering a new description in the Comments field. Otherwise, proceed to the next step.

Step 6 Enter the new Content Engine IP address in the Content IP Address field. This is the static content IP address from your DNS server that will be used to communicate with the Content Engine.

Step 7 If you choose to, enter the new host name in the Content Hostname field. Otherwise, proceed to the next step.

This is the DNS address that can be used to reach the Content Engine. Otherwise, proceed to the next step.

Step 8 If you choose to, click the Location drop-down list, and choose a new CDN location for the Content Engine. Otherwise, proceed to the next step.

Depending on the location you choose, the Region field will change to reflect the region containing that location.

Step 9 If you choose to, change the pre-positioned disk space. Otherwise, proceed to the next step.

Enter a value (in gigabytes, up to 24 gigabytes) representing the disk space allocated to pre-positioning content on the Content Engine. Changing the pre-positioned disk space causes the Content Engine to restart.

Step 10 Click **Save**. You are returned to the View Content Engines page (see Figure 2-10), which lists Content Engines on your CDN.

Modifying Content Engine Passwords

Both Content Engines and Content Routers maintain two sets of passwords:

- Root password—This password controls access to the CDN device console using direct login or remote login using the Telnet or SSH command interfaces.
- HTTP password—This password controls access to device configuration features accessible from the Content Distribution Manager.

To modify the root or HTTP password:

Step 1 From the Cisco Internet CDN Software user interface, click **resources**.

Step 2 From the drop-down list, choose **Content Engines**. The View Content Engines page appears (see Figure 2-10), listing the Content Engines on your CDN.

Step 3 Click the edit icon next to the name of the Content Engine that you wish to edit. The browser window refreshes, displaying the Modify a Content Engine page. (See Figure 2-11.)

Step 4 Locate the fields for modifying the current password. Fields for modifying the root password and HTTP password are grouped in columns under the appropriate heading.

Step 5 Enter the current password (that you wish to change) in the Old Password field.

If you have forgotten the current password for this device, you can enter the current system password in its place and then proceed with changing the password to a new value. See the "Changing System Passwords" section on page 4-4 for more information on maintaining your system passwords.

Step 6 Move your cursor to the New Password field, and enter the password you wish to begin using.

Note Passwords should be eight characters long.

Step 7 Move your cursor to the Re-type New Password field and reenter the new password to confirm your decision.

Step 8 Click **Save**. The password is updated for the selected Content Engine.

The Modify a Content Engine page refreshes. If the password was successfully changed, a green circle with a check mark is displayed on the user interface next to the affected password field. See the "Exiting the Content Distribution Manager User Interface" section on page 1-28 for details.

Stopping, Shutting Down, Restarting, and Rebooting a Content Engine

Using the resources feature of the Content Distribution Manager, you can stop, restart, reboot, or shut down a Content Engine remotely, with the following consequences:

- **Reboot CE**—This option causes the device to perform a controlled shutdown of all CDN servers and then restarts the operating system on the device.
- **Restart Software**—This option halts and then restarts the CDN servers on the device.
- **Shutdown CE**—This option causes the device to perform a controlled shutdown of all CDN servers, requiring a manual reboot of the device. Clicking **Shutdown CE** is equivalent to issuing a **node exit** command, or a control exit command in Linux.

Once a device has been shut down, you will not be able to access it remotely using Telnet or SSH, nor will you be able to issue commands using the command-line interface. To bring a device back online, gain physical access to the device and cycle the power off and then on again.

- **Stop Software**—This option is equivalent to issuing a **node stop** command from the command-line interface; clicking **Stop** halts the CDN servers on the device, bringing the device offline.

  To bring a device back online that has been stopped from the Content Distribution Manager, it is necessary to remotely access the device using SSH or Telnet (if Telnet has been enabled on the device). After logging on to the device using the admin account and secure password, use commands issued through the Cisco Internet CDN Software command-line interface (CLI) to restart the CDN processes on the device. For example:

  ```
  cdn-device> enable
  cdn-device# node start
  cdn-device# exit
  cdn-device> exit
  ```

Refer to the *Cisco Internet CDN Software Command Reference* for more information on the node command, or using the CDN command-line interface.

To stop, restart, reboot, or shut down a Content Engine:

Step 1 From the Cisco Internet CDN Software user interface, click **resources**.

Step 2 From the drop-down list, choose **Content Engines**. The View Content Engines page appears (see Figure 2-10), listing the Content Engines on your CDN. The online status of the device is listed under the heading Node status.

Step 3 Click the edit icon next to the name of the Content Engine that you wish to stop, shut down, reboot, or restart. The browser window refreshes, displaying the Modify a Content Engine page. (See Figure 2-11.)

Step 4 Click the appropriate button to stop, shut down, restart, or reboot the Content Engine. You are prompted to confirm your decision.

- If you are shutting down the Content Engine, you are asked to confirm your decision. Click **OK** to confirm.
- If you are stopping, restarting, or rebooting the Content Engine, click the **Yes Continue** button to execute your request.

You are returned to the View Content Engines page, which lists the Content Engines on your CDN.

Deleting a Content Engine

Delete a Content Engine when the device is experiencing unresolvable problems or when its network address or configuration has changed and you need to add the device back to the CDN using its new address and configuration information.

When deleting a Content Engine from the CDN, you are effectively removing that device and the content it contains from the routing scheme that the CDN software uses to fill user requests. Although the CDN software is designed to route requests around Content Engines that are busy, offline, or missing, removing a Content Engine may affect the speed with which the CDN can serve user requests.

Note You cannot delete a Content Engine if it is the last node assigned to a location that is designated as the root location for a hosted domain. If you receive an error referencing the root location for a hosted domain, add more Content Engines to that location, or change the root location for the hosted domain before attempting to delete the Content Engine again.

To delete a Content Engine:

Step 1 From the Cisco Internet CDN Software user interface, click **resources**.

Step 2 From the drop-down list, choose **Content Engines**. The View Content Engines page appears (see Figure 2-10), listing the Content Engines on your CDN. The online status of the device is listed under the heading Node status.

Step 3 Click the edit icon next to the name of the Content Engine that you wish to delete. The browser window refreshes, displaying the Modify a Content Engine page. (See Figure 2-11.)

Step 4 Click **Delete**. You are prompted to confirm your decision.

Step 5 Click **OK** to execute your request. You are returned to the View Content Engines page (see Figure 2-10), which lists the remaining Content Engines on your CDN.

Step 6 You now need to log in directly to the Content Engine you deleted and access the command-line interface (CLI) using the admin account and password.

Step 7 At the prompt, enter **enable** to enable the administrative mode. For example:

```
device_name> enable
```

The prompt changes to a pound sign (#) to indicate that you are in administrative mode.

Step 8 Enter **shutdown** to stop the Cisco Internet CDN Software and shut down the device.

Viewing Content Engine Statistics

It is often useful to be able to get a picture of the performance of Content Engines across your network. You can do this using the Content Engine Statistics feature, available from the Tools area of the Content Distribution Manager user interface.

The Content Engines Statistics feature enables you to view, at a glance, which Content Engines are online, as well as assess their available resources, the volume of traffic being routed to them, and their performance in serving requests. The information displayed using the Content Engine Statistics tool is based on a snapshot of your CDN taken on the quarter hour. The statistics displayed represent the state of your Content Engines for the previous quarter hour.

Using the tabs provided, you view statistics for all Content Engines on your CDN, or look at the overall performance of the Content Engines in your hosted domains and virtual CDNs.

See Table 3-1 for information on the meaning of each Content Engine statistic presented in the table.

Table 3-1 Content Engine Statistics

Content Engine Property	Description
Content Engine/Hosted Domains/Virtual CDNs	Name of the device or device grouping (hosted domain, virtual CDN).
Content Engines	*Hosted domains and virtual CDNs only.* Number of Content Engines belonging to the hosted domain or virtual CDN.
Status	*Content Engines only.* Online status of the Content Engine—online, offline, or configuring.
Location	*Content Engines only.* CDN location with which the Content Engine is associated.
Region	*Content Engines only.* CDN region with which the Content Engine is associated.
Cache Hits/min	Average number of content items per minute successfully served from the cache of the Content Engine or from all the Content Engines in the hosted domain or virtual CDN during the preceding quarter hour.
Cache Misses/min	Average number of content items per minute that could not be served from the cache of the Content Engine or from all the Content Engines in the hosted domain or virtual CDN during the preceding quarter hour. These requests were served from the origin server instead.
Cache Kb/min	Rate in kilobits per minute at which content was served from the Content Engine cache, or the average rate at which content was served from the cache for all devices on the hosted domain or virtual CDN during the preceding quarter hour.
Cache Disk Size (MB)	Total disk space on the Content Engine or the sum total for all Content Engines in the hosted domain or virtual CDN, in megabytes.

Table 3-1 Content Engine Statistics (continued)

Content Engine Property	Description
Cache Memory Size (KB)	Total memory on the Content Engine or the sum total for all Content Engines in the hosted domain or virtual CDN, in kilobytes.
DNS Queries/min	Average number of DNS queries received per minute by the Content Engine, or by the hosted domain or virtual CDN during the preceding quarter hour.

To view Content Engine statistics for your CDN:

Step 1 From the Cisco Internet CDN Software user interface, click **tools**.

Step 2 From the drop-down list, choose **Content Engine Statistics**. The browser refreshes, displaying the Content Engine Statistics page.

Step 3 Click the tab corresponding to the way you would like to view your Content Engine statistics.

- To view the statistics for each Content Engine on your CDN, click the **Content Engines** tab.
- To view the overall performance of the Content Engines in your hosted domains, click the **Hosted Domains** tab.
- To view the overall performance of the Content Engines in your virtual CDNs, click the **virtual CDNs** tab.

The Content Engine Statistics tool displays the information you requested.

Step 4 See the "Printing and Exporting CDN Data" section on page 3-47 for information on reporting on your Content Engine statistics.

Viewing Hosted Domain Assignments

You can use the Modify a Content Engine page to view which hosted domains a particular Content Engine is assigned to. You can view hosted domain assignments for a bird's eye view of how a given Content Engine is deployed across your CDN—which hosted domains it belongs to, the root location and amount of pre-positioned disk space required in each hosted domain, and the number of Content Engines also assigned to each hosted domain.

To view hosted domain assignments for a Content Engine:

Step 1 From the Cisco Internet CDN Software user interface, click **resources**.

Step 2 From the drop-down list, choose **Content Engines**. The View Content Engines page appears (see Figure 2-10), listing the Content Engines on your CDN. The online status of the device is listed under the heading Node status.

Step 3 Click the edit icon next to the name of the Content Engine for which you wish to view hosted domain assignments. The browser window refreshes, displaying the Modify a Content Engine page. (See Figure 2-11.)

Step 4 Under the heading Locality, click the note pad icon. A listing of the Content Engine's hosted domain assignments appears in a separate window.

Working with Content Routers

You work with Content Routers by:

- Modifying Content Routers
- Modifying Content Router Passwords
- Stopping, Shutting Down, Restarting, and Rebooting a Content Router
- Deleting a Content Router

Modifying Content Routers

You use the resources feature of the Content Distribution Manager to make changes to a Content Router.

You can modify the following Content Router properties:

- Name
- Location

- Root and HTTP passwords
- Description
- Content IP address
- Content host name

Note Changing the location will cause the Content Router to restart.

To modify a Content Router, follow these steps:

Step 1 From the Cisco Internet CDN Software user interface, click **resources.**

Step 2 From the drop-down list, choose **Content Routers**. The View Content Routers page appears (see Figure 2-8), listing the Content Routers on your CDN.

Step 3 Click the edit icon next to the name of the Content Router that you wish to edit. The browser window refreshes, displaying the Modify a Content Router page. (See Figure 2-9.) Fields for editing the selected Content Router appear.

Step 4 If you wish to, enter the new name of the Content Router in the Content Router Name field. Otherwise, proceed to the next step.

Step 5 If you wish to, modify the description used to identify the Content Router by entering a new description in the Comments field. Otherwise, proceed to the next step.

Step 6 Enter the new Content Router IP address in the Content IP Address field. This is the static content IP address from your DNS server that will be used to communicate with the Content Router.

Step 7 If you wish to, enter the new host name in the Content Hostname field. Otherwise, proceed to the next step.

This is the DNS address that can be used to reach the Content Router.

Step 8 If you wish to, click the Location drop-down list and choose a new CDN location for the Content Router. Otherwise, proceed to the next step.

Depending on the location you choose, the Region field will change to reflect the region containing that location.

Step 9 Click **Save**. You will be returned to the View Content Routers page (see Figure 2-8), which lists Content Routers on your CDN.

Modifying Content Router Passwords

Both Content Routers and Content Engines maintain two sets of passwords:

- Root password—This password controls remote access to the CDN device console using direct login or remote login using the Telnet or SSH command interfaces.
- HTTP password—This password controls access to device configuration features accessible from the Content Distribution Manager.

To modify the root or HTTP password:

Step 1 From the Cisco Internet CDN Software user interface, click **resources**.

Step 2 From the drop-down list, choose **Content Routers**. The View Content Routers page appears (see Figure 2-8), listing the Content Routers on your CDN.

Step 3 Click the edit icon next to the name of the Content Router that you wish to edit. The Modify a Content Router page appears. (See Figure 2-9.)

Step 4 Locate the fields for modifying the current password. Fields for modifying the root password and HTTP password are grouped in columns under the appropriate heading.

Step 5 Enter the current password (that you wish to change) in the Old Password field.

If you have forgotten the current password for this device, you can enter the current system password in its place, and then proceed with changing the password to a new one. See the "Changing System Passwords" section on page 4-4 for more information on maintaining your system passwords.

Note Passwords should be eight characters long.

Step 6 Move your cursor to the New Password field, and enter the password that you wish to begin using.

Step 7 Move your cursor to the Re-type New Password field and enter the new password a second time to confirm your decision.

Step 8 Click **Save**. The password is updated for the selected Content Router.

The Modify a Content Router page refreshes. If the password was successfully changed, a green circle with a check mark is displayed on the user interface next to the affected password field. See the "Exiting the Content Distribution Manager User Interface" section on page 1-28 for details.

Stopping, Shutting Down, Restarting, and Rebooting a Content Router

As with Content Engines, you can use the resources feature of the Content Distribution Manager to stop, restart, reboot, or shut down a Content Router remotely.

See the instructions in the "Stopping, Shutting Down, Restarting, and Rebooting a Content Engine" section on page 3-14 for a more detailed discussion of the effect of stopping, shutting down, restarting, or rebooting a CDN device.

The instructions presented in that section also apply to Content Routers.

Deleting a Content Router

Delete a Content Router when the device is experiencing unresolvable problems or when its network address or configuration has changed and you need to add the device back to the CDN using its new address and configuration information.

When deleting a Content Router from the CDN, you are effectively removing that device from the routing scheme that the CDN software uses to fill user requests. Although the CDN software is designed to route requests around Content Routers that are busy, offline, or missing, removing a Content Router may affect the speed with which the CDN can serve user requests.

To delete a Content Router:

Step 1 From the Cisco Internet CDN Software user interface, click **resources**.

Step 2 From the drop-down list, choose **Content Routers**. The View Content Routers page appears (see Figure 2-8), listing the Content Routers on your CDN. The online status of the device is listed under the heading Node status.

Step 3 Click the edit icon next to the name of the Content Router that you wish to delete. The Modify a Content Router page appears (see Figure 2-9), displaying fields for editing the selected Content Router.

Step 4 Click **Delete**. You are prompted to confirm your decision.

Step 5 Click **Yes Continue** to execute your request. You are returned to the View Content Routers page (see Figure 2-8), which lists the remaining Content Routers on your CDN.

Step 6 You now need to log in directly to the Content Router you deleted and access the command-line interface using the admin account and password.

Step 7 At the prompt, enter **enable** to enable the administrative mode. For example:

```
device_name> enable
```

The prompt changes to a pound sign (#) to indicate that you are in administrative mode.

Step 8 Enter **shutdown** to stop the Cisco Internet CDN Software and shut down the device.

Working with Supernodes and Content Engine Clusters

Using the resources feature of the Content Distribution Manager, you can modify supernodes, as well as the Content Services Switch and Content Engine clusters assigned to them.

You can work with supernodes and clusters by:

- Modifying a Supernode
- Deleting a Supernode
- Modifying a Cluster
- Deleting a Cluster

Modifying a Supernode

It is possible to edit a supernode name and the location and region with which the supernode is associated on a CDN. In addition, you can modify the address of the Content Services Switch and the administrative password used to access the Content Services Switch. These changes can be made directly from the Content Distribution Manager user interface.

Modifying the Supernode Name, Location, and Region

To modify the supernode name, location, or region:

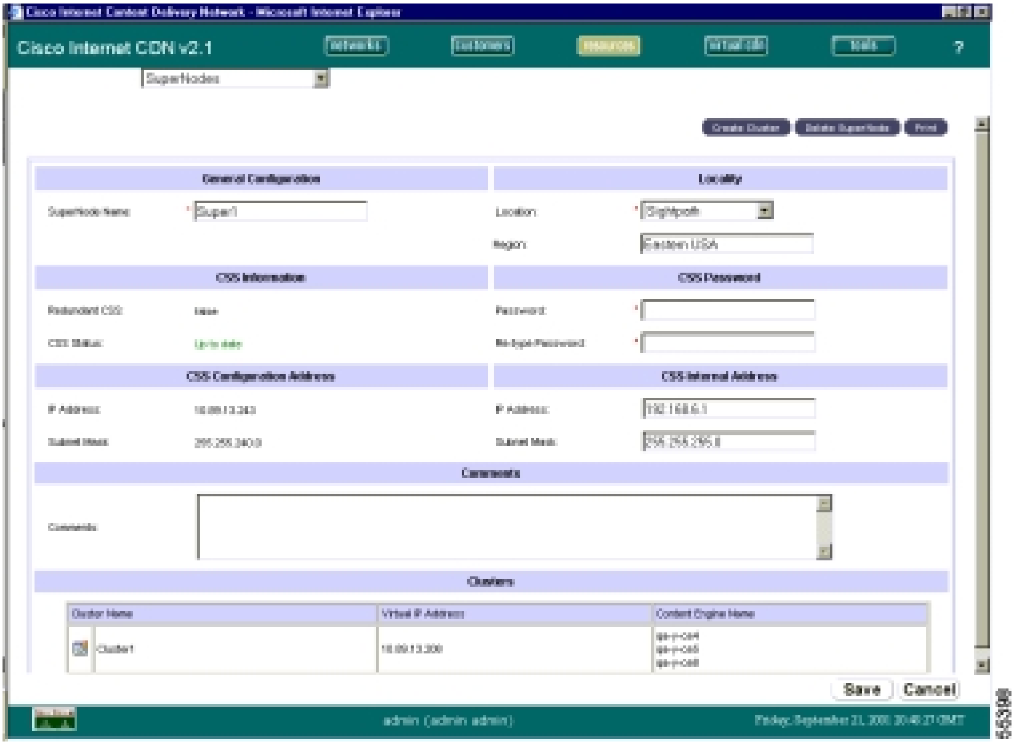
Step 1 From the Cisco Internet CDN Software user interface, click **resources**.

Step 2 From the drop-down list, choose **SuperNodes**. The View Supernodes page appears. (See Figure 2-12.)

Step 3 Click the icon next to the supernode you wish to edit. The Modify a Supernode page appears. (See Figure 3-4.)

- To edit the name of the supernode (this is the user-friendly name that identifies the supernode within the Content Distribution Manager user interface and elsewhere), enter a new name in the SuperNode Name field.
- To modify the location with which the supernode is associated, from the **Location** drop-down list, choose a new location. The region may change depending on what location you choose.
- To add a new cluster to the supernode or delete a cluster from the supernode, see the "Creating a Cluster" section on page 2-44.

Figure 3-4   Modify a Supernode



General Configuration

SuperNode Name: * Super1

Locality

Location: * Sightpath

Region: Eastern USA

CSS Information

Redundant CSS: false

CSS Status: Up to date

CSS Password

Password: *

Re-type Password: *

CSS Configuration Address

IP Address: 10.89.13.243

Subnet Mask: 255.255.240.0

CSS Internal Address

IP Address: 192.168.6.1

Subnet Mask: 255.255.255.0

Comments

Comments:

Clusters

Cluster Name	Virtual IP Address	Content Engine Name
Cluster1	10.89.13.200	[illegible] [illegible] [illegible]

Step 4 Click **Save** to update your changes to the supernode name and location. You are returned to the View Supernodes page. The status of the supernode that you just modified is *configuring* until your name and location changes have been integrated.

Step 5 Wait until the changes have been incorporated and the status returns to *online* before making additional changes to the supernode configuration.

.

Updating the Content Services Switch Password

If the password for the CLI for the Content Services Switch has changed, use the Content Distribution Manager user interface to update the CDN with the new password information.

To update the root password information for your Content Services Switch:

Step 1 From the Cisco Internet CDN Software user interface, click **resources**.

Step 2 From the drop-down list, choose **SuperNodes**.

The View Supernodes page appears (See Figure 2-12.) The IP address of the Content Services Switch associated with the supernode is provided in the column labeled CSS Configuration IP Address.

Step 3 Click the icon next to the supernode corresponding to the Content Services Switch with the CLI password that you wish to modify. The Modify a Supernode page appears. (See Figure 3-4.)

Step 4 Enter the new password information for the Content Services Switch CLI in the Password field.

Step 5 Verify the new password by entering it again in the Re-type Password field.

Step 6 Click **Save** to update the Content Services Switch CLI password. You are returned to the View Supernodes page.

The status of the supernode that you just modified is *configuring* until your password changes have been integrated.

Modifying the Content Services Switch Internal Address

The Content Services Switch maintains an internal subnet of content IP addresses referred to as the *internal subnet*. It is from this list of addresses that the Content Services Switch chooses Content Engines to serve content. Using the Modify Supernode page on the Content Distribution Manager user interface, you can change the Content Services Switch internal IP address and subnet mask.

Note Changing the internal IP address information for the Content Services Switch causes a temporary disruption in service from the Content Engines assigned to the supernode, because these devices will be assigned new content IP addresses.

To modify the Content Services Switch internal IP address:

Step 1 From the Cisco Internet CDN Software user interface, click **resources**.

Step 2 From the drop-down list, choose **SuperNodes**.

The View Supernodes page appears (See Figure 2-12.) The IP address of the Content Services Switch associated with the supernode is provided in the column labeled CSS Configuration IP Address. This is the actual network address of the device.

Step 3 Click the icon next to the supernode corresponding to the Content Services Switch you wish to modify. The Modify a Supernode page appears. (See Figure 3-4.)

Step 4 Under the heading CSS Internal Address, enter the IP address and subnet mask that will be used by the Content Services Switch to assign content address to the Content Engines grouped behind it.

Step 5 Click **Save** to update the Content Services Switch internal IP address information. You will be asked to confirm your decision to change the internal IP address information.

Step 6 Click **OK**. You are returned to the View Supernodes page.

The status of the supernode that you just modified is *configuring* until your internal IP address changes have been integrated.

Deleting a Supernode

Deleting a supernode from the CDN effectively removes all content served from the Content Engines in that supernode from the CDN. User requests for that content will be routed to other nodes or supernodes on the CDN, if they exist.

After you delete the supernode, the associated Content Engines continue to appear on the Content Distribution Manager user interface, listed with the other Content Engines on your CDN, but with an *inactive* status. To remove these Content Engines from the CDN, follow the instructions for deleting Content Engines in the "Deleting a Content Engine" section on page 3-16.

Note You cannot delete a supernode if any of its Content Engines are the last node assigned to a location that is designated as the root location for a hosted domain. If you receive an error referencing the root location for a hosted domain, add more Content Engines to that location, or change the root location for the hosted domain before attempting to delete the supernode again.

To delete a supernode:

Step 1 From the Cisco Internet CDN Software user interface, click **resources**.

Step 2 From the drop-down list, choose **SuperNodes**. The View Supernodes page appears. (See Figure 2-12.)

Step 3 Click the icon next to the supernode that you wish to delete. The Modify a Supernode page appears. (See Figure 3-4.)

Step 4 Click **Delete Supernode**. You are prompted to confirm your decision to remove the supernode from the CDN.

Step 5 Click **OK**. You are returned to the View Supernodes page.

Modifying a Cluster

Once they are created, the name or description of Content Engine clusters can be changed, as well as the virtual IP address or virtual host name designation. In addition, Content Engines can be removed from the cluster and associated with a different cluster behind the same Content Services Switch.

To modify a cluster:

Step 1 From the Cisco Internet CDN Software user interface, click **resources**.

Step 2 From the drop-down list, choose **Clusters**. The View Clusters page appears. (See Figure 2-14.)

Step 3 Click the icon next to the cluster you wish to edit. The Modify a Cluster page appears. (See Figure 3-5.)

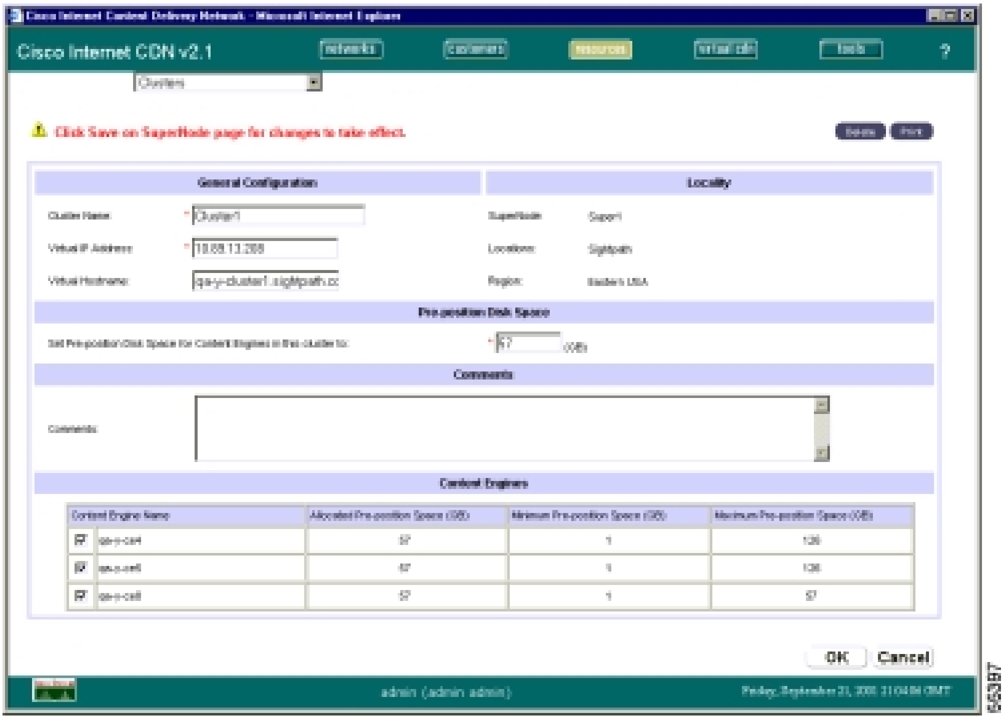
- To edit the cluster name (this is the user-friendly name that identifies the cluster within the Content Distribution Manager user interface and elsewhere), enter a new name in the Cluster Name field.
- To modify the virtual IP address or host name for the cluster, enter the new address information in the fields provided. Refer to the "CDN Device Network Addressing" section in Chapter 2 of the *Cisco Internet CDN Software Configuration Guide* for an explanation of the role of the cluster's virtual IP address.

  Note If the virtual IP address is resolvable back to the DNS server, no virtual host name is required.

- To modify the pre-positioned disk space available on each of the Content Engines in this cluster, enter a new number (representing the number of gigabytes of pre-positioned disk space) in the Pre-position Disk Space field provided. This is the amount of space that will be allocated on each Content Engine, and must be less than the amount of available disk space on each of the assigned Content Engines.

Note The amount of pre-positioned disk space assigned to Content Engines through the cluster will overwrite any other pre-positioned disk space designation for the device.

Figure 3-5 Modify a Cluster



Click Save on SuperNode page for changes to take effect.

General Configuration		Locality	
Cluster Name:	* Cluster1	SuperNode:	Super1
Virtual IP Address:	* 10.88.13.208	Location:	Sightpath
Virtual Hostname:	qa-y-cluster1.sightpath.cc	Region:	Eastern USA

Pre-position Disk Space

Set Pre-position Disk Space for Content Engines in this cluster to: * 57 (GB)

Comments

Comments:

Content Engines

	Content Engine Name	Allocated Pre-position Space (GB)	Minimum Pre-position Space (GB)	Maximum Pre-position Space (GB)
☑	qa-y-ce4	57	1	136
☑	qa-y-ce5	57	1	136
☑	qa-y-ce6	57	1	57

admin (admin admin)

Friday, September 21, 2001 [illegible] GMT

Step 4 Click **Save** to save your changes to the selected cluster.

Deleting a Cluster

When you delete a cluster, the Content Engines in that cluster remain on the CDN and can be reassigned to different clusters on the supernode. See the "Deleting a Content Engine" section on page 3-16 for instructions on deleting the Content Engines.

Note You cannot delete a cluster if any of its Content Engines are the last node assigned to a location that is designated as the root location for a hosted domain. If you receive an error referencing the root location for a hosted domain, add more Content Engines to that location, or change the root location for the hosted domain before attempting to delete the cluster again.

To delete a cluster:

Step 1 From the Cisco Internet CDN Software user interface, click **resources**.

Step 2 From the drop-down list, choose **SuperNodes**. The View Supernodes page appears. (See Figure 2-12.)

Step 3 Click the edit icon next to the name of the supernode containing the cluster you wish to delete. The Modify a Supernode page appears. (See Figure 3-4.)

Step 4 Click the icon next to the name of the cluster you wish to edit. The Modify a Cluster page appears. (See Figure 3-5.)

Step 5 Click the **Delete** button. You are prompted to confirm your decision to remove the cluster from the CDN.

Step 6 Click **OK**. You are returned to the View Supernodes page.

Working with Content Providers

You work with content providers by:

- Modifying Content Providers
- Deleting Content Providers

Modifying Content Providers

You can modify a content provider by changing the company name and address, the primary contact information, or the optional secondary contact information.

To modify a content provider, follow these steps:

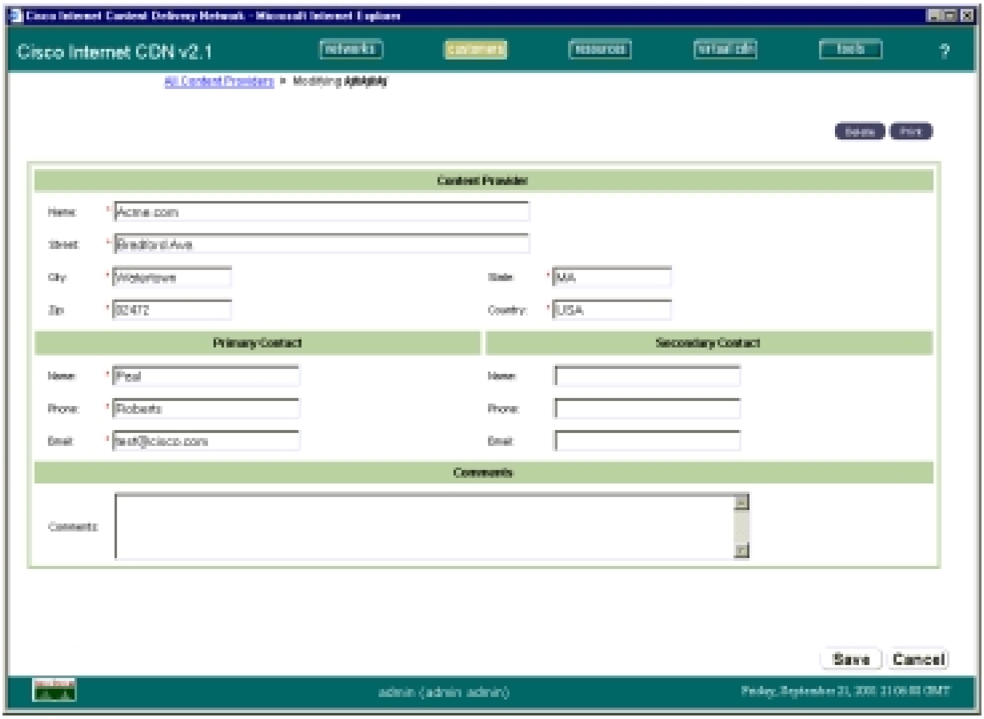
Step 1 From the Cisco Internet CDN Software user interface, click **customers**.

The View Content Providers page appears. (See Figure 2-1.)

Step 2 Click the edit icon next to the content provider name that you want to modify.

The Modify a Content Provider page appears. (See Figure 3-6.)

Figure 3-6 Modify a Content Provider


Cisco Internet Content Delivery Network - Microsoft Internet Explorer
Cisco Internet CDN v2.1
networks
customers
resources
virtual cdn
tools
?
All Content Providers » Modifying Apbbbbj
Delete
Print
Save
Cancel
admin (admin admin)
Friday, September 21, 2001 21:09:08 GMT
47813

Content Provider

Name:	* Acme.com		
Street:	* Bradford Ave		
City:	* Watertown	State:	* MA
Zip:	* 02472	Country:	* USA

Primary Contact		Secondary Contact	
Name:	* Paul	Name:	
Phone:	* Roberts	Phone:	
Email:	* test@cisco.com	Email:	

Comments

Comments:

Step 3 Enter any changes you want to make to the company name and address, the primary contact information, or the optional secondary contact information.

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

Step 4 Click **Save**.

Deleting Content Providers

You can delete content providers as needed.

Note When you delete a content provider, all hosted domains that have been added for the content provider are also deleted.

To delete a content provider, follow these steps:

Step 1 From the Cisco Internet CDN Software user interface, click **customers**.

The View Content Providers page appears. (See Figure 2-1.)

Step 2 Check the check box next to the content providers that you want to delete.

Step 3 Click **Delete**.

Working with Hosted Domains

Using the features of the Content Distribution Manager, you can modify or remove hosted domains that have been created. Keep in mind that modifying your hosted domain may affect the availability of content on the CDN.

You work with hosted domains by:

- Viewing Hosted Domains
- Modifying Hosted Domains
- Deleting Hosted Domains
- Updating Hosted Domain Content
- Purging Hosted Domains
- Viewing the Status of Content Replication to a Hosted Domain

Viewing Hosted Domains

You can view hosted domains across your CDN, or according to the content provider with which they are associated.

Viewing All Hosted Domains on Your CDN

To view hosted domains across your CDN:

Step 1 From the Cisco Internet CDN Software user interface, click **resources**.

Step 2 Choose **Hosted Domains** from the drop-down list.

The View Hosted Domains page appears. (See Figure 2-16.)

The content provider with which the hosted domains are associated is listed in the Content Provider column.

Viewing Hosted Domains Belonging to a Content Provider

To view hosted domains sorted by content provider:

Step 1 From the Cisco Internet CDN Software user interface, click **customers**.

The View Content Providers page (see Figure 2-1) appears, displaying a list of all content providers on your CDN.

Step 2 Click the content provider name. The screen refreshes, displaying a list of hosted domains associated with the selected content provider.

Modifying Hosted Domains

You can modify a hosted domain by changing the following items:

- Hosted domain name
- Hosted domain alias
- Origin server
- Content provider
- Manifest file (identifying hosted content)

To modify a hosted domain, follow these steps:

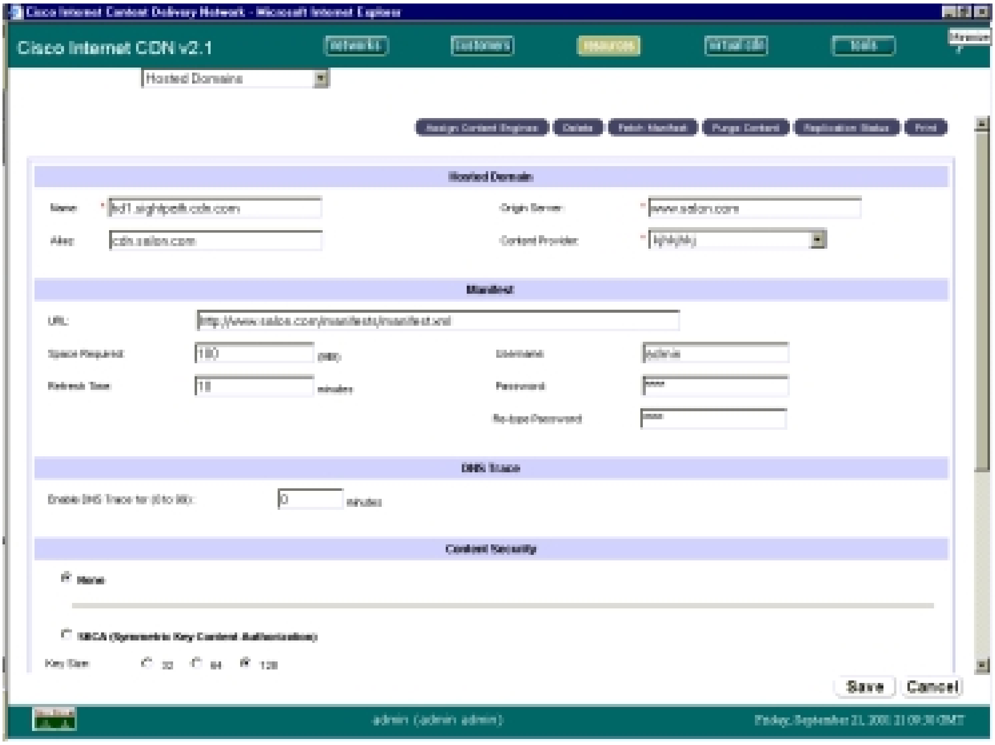
Step 1 From the Cisco Internet CDN Software user interface, click **resources**.

Step 2 Choose **Hosted Domains** from the drop-down list.

The View Hosted Domains page appears. (See Figure 2-16.)

Step 3 Click the icon adjacent to the name of the hosted domain that you want to change. The Modify a Hosted Domain page appears. (See Figure 3-7.)

Figure 3-7 Modify a Hosted Domain



Hosted Domain

Name: * kd1.sightpath.cdn.com
Origin Server: * www.salon.com
Alias: cdn.salon.com
Content Provider: * kjhkjhkj

Manifest

URL: http://www.salon.com/manifests/manifest.xml
Space Required: 100 (MB)
Username: admin
Refresh Time: 10 minutes
Password: ****
Re-type Password: ****

DNS Trace

Enable DNS Trace for (0 to 60): 0 minutes

Content Security

● None

○ SKCA (Symmetric Key Content Authorization)

Key Size ○ 32 ○ 64 ● 128

admin (admin admin)
Friday, September 21, 2001 21:09:30 GMT

Step 4 Use the fields provided under the Hosted Domain heading to modify the hosted domain name, origin server for the hosted domain content, or CDN content provider that the hosted domain is associated with. Refer to the following guidelines when necessary:

- Your origin server field *cannot* contain a path to a subdirectory on the server. For example:

  ```
  www.cisco.com
  ```

  is a valid origin server address, whereas the following address is not:

  ```
  www.cisco.com/support
  ```

- A valid CDN hosted domain name must use the following format:
  - The hosted domain name must be a valid, fourth-level domain name. For example:

    ```
    www.cdn.cisco.com
    ```

  - The first part of the domain name (*www* in the example above) is open, and can be defined by you when you create the hosted domain name.
  - The remaining subdomain (the three segments after the first dot) must correspond to entries on your DNS server to provide a functional mapping for the Content Routers.
  - The CDN must be given the right to act as the authoritative DNS server for the subdomain you specify.

Note The hosted domain name *cannot* contain underscore (_) characters.

Step 5 In the Alias field, enter an optional alias for the hosted domain. For example, if your hosted domain name is:

```
www.cdn.cisco.com
```

but you want to use a third-level instead of a fourth-level domain name on all your published links, you can use the Alias field to map a third-level domain name to your host domain name such as:

```
www.cisco-cdn.com
```

Note You must provide a CNAME mapping between the delegated domain and your alias on the DNS server before aliasing will work. Entering your alias on the hosted domains page is not sufficient to enable hosted domain aliasing.

Step 6 Use the fields provided under the Manifest heading to modify the location or information identifying the manifest file for the hosted domain. The manifest file provides information about live and video-on-demand (VOD) content served from the hosted domain. See the "Creating a Manifest File for Importing Media" section on page 2-3 for instructions on creating a manifest file for your hosted domain.

- The URL field contains the address of the manifest file for the hosted domain.
- The Space Required field identifies the amount of disk space reserved on your Content Engines for content identified in the manifest.
- The Refresh Time field identifies the frequency with which the Content Engines assigned to the hosted domain check for updates to the manifest file.
- The Username and Password fields allow you to enter any secure login information needed to access the manifest file at its remote location.

Step 7 Under the DNS Trace heading, enter the length of time (in minutes) that the DNS Trace feature will be enabled on the Content Engines assigned to the hosted domain. See the "Enabling and Disabling DNS Trace" section on page 4-70 for detailed information on using the DNS trace feature.

Step 8 If you wish to add comments regarding the hosted domain for the benefit of other Content Distribution Manager users, enter them in the Comments field provided.

Step 9 Click **Save** to save any changes you have made to the hosted domain configuration. The Content Distribution Manager updates the hosted domain information.

Adding and Removing Content Engines from a Hosted Domain

To add Content Engines to a hosted domain:

Step 1 From the Modify a Hosted Domain page (see Figure 3-7), click the **Assign Content Engines** button. Features for assigning Content Engines by region appear.

Step 2 Click the **Assign CEs by Region** or **Assign CEs by Virtual CDN** tab, depending on how you wish to locate the Content Engines you are adding.

Note Content Engines can be added to the hosted domain from more than one virtual CDN or region.

Step 3 Select the region or virtual CDN in which the Content Engines reside.

- If you are searching for Content Engines by region, a list of locations in the region appears. Click the location of the region in which the Content Engines are located.
- If you are searching for Content Engines by virtual CDN, a list of virtual CDNs appears.

Step 4 Click the name of the location or virtual CDN in which the Content Engines you wish to add are located. A list of the Content Engines and clusters in that location appears.

Note As you move down into virtual CDNs, or from regions to locations, your path is saved in the header area just above the **Add Selected CEs** button. Click the link at any point in the path to return to that point.

Step 5 Check the box adjacent to the name of the cluster or Content Engine that you wish to associate with the hosted domain.

Note To choose all Content Engines, you can choose the topmost check box (next to the Cluster or Content Engine heading).

Step 6 Click **Add Selected CEs** and then click **Save** to add the Content Engines to your hosted domain.

The list of clusters or Content Engines to which the hosted domain is assigned refreshes, listing the newly added Content Engine or cluster.

Step 7 To remove Content Engines, check the box next to the name of the Content Engines you wish to remove from this list and click **Remove Selected CEs**.

Step 8 If you wish to locate Content Engines in a different region or virtual CDN, repeat Step 2 through Step 6 for each Content Engine that you wish to add.

Step 9 To change the root location for the hosted domain, choose a new location from the Root Location drop-down list. The root location must contain a minimum of one node.

Step 10 Click **Save**. The browser window refreshes, listing the updated hosted domains. The list of Content Engines in the hosted domain shows the updated count.

Deleting Hosted Domains

To delete a hosted domain, follow these steps:

Step 1 From the Cisco Internet CDN Software user interface, click **resources**.

Step 2 From the drop-down list, choose **Hosted Domains**.

The View Hosted Domains page appears. (See Figure 2-16.)

Step 3 Click the icon adjacent to the name of the hosted domain that you want to delete.

The Modify a Hosted Domain page appears. (See Figure 3-7.)

Step 4 Click **Delete**. You are prompted to confirm your decision to delete the hosted domain.

Step 5 Click **OK** to confirm your decision. The hosted domain is removed from the CDN.

Updating Hosted Domain Content

At any point after you have replicated content to the Content Engines that are associated with your hosted domain, you can update that content using the fetch manifest feature. For example, if you modify your manifest file to point to new content or remove references to content that you want to make obsolete, you must fetch the manifest file to begin replication of any new hosted domain content, and to sever connections to content that you want to make obsolete.

Note Content that is removed from the manifest file is made unavailable as soon as that updated manifest file is fetched. Obsolete content is not immediately deleted from the hosted domain cache but is eventually removed to make room for new hosted domain content.

To fetch updated content from your origin server and replicate it to your Content Engines:

Step 1 From the Cisco Internet CDN Software user interface, click **resources**.

Step 2 From the drop-down list, choose **Hosted Domains**.

The View Hosted Domains page appears. (See Figure 2-16.)

Step 3 Follow the instructions for modifying an existing hosted domain in the "Modifying Hosted Domains" section on page 3-36 to open your hosted domain for editing.

Step 4 Verify that the URL field points to the correct manifest file for the hosted domain.

Step 5 Click **Fetch Manifest**. You are prompted to confirm your decision to begin copying the updated content named by the manifest file to the Content Engines assigned to the hosted domain.

Step 6 Click **OK**. You are returned to the View Hosted Domains page. (See Figure 2-16.)

Step 7 You can view the status of media replication from the origin server to your Content Engines at any time. See the "Viewing the Status of Content Replication to a Hosted Domain" section on page 3-43 for instructions.

Purging Hosted Domains

You can purge a hosted domain as needed. Purging a hosted domain deletes the content from all Content Engines that store the hosted domain content, making room for new content.

To purge a hosted domain, follow these steps:

Step 1 From the Cisco Internet CDN Software user interface, click **resources**.

Step 2 From the drop-down list, choose **Hosted Domains**.

The View Hosted Domains page appears. (See Figure 2-16.)

Step 3 Click the icon next to the hosted domain that you want to purge. The Modify a Hosted Domain page appears. (See Figure 3-7.)

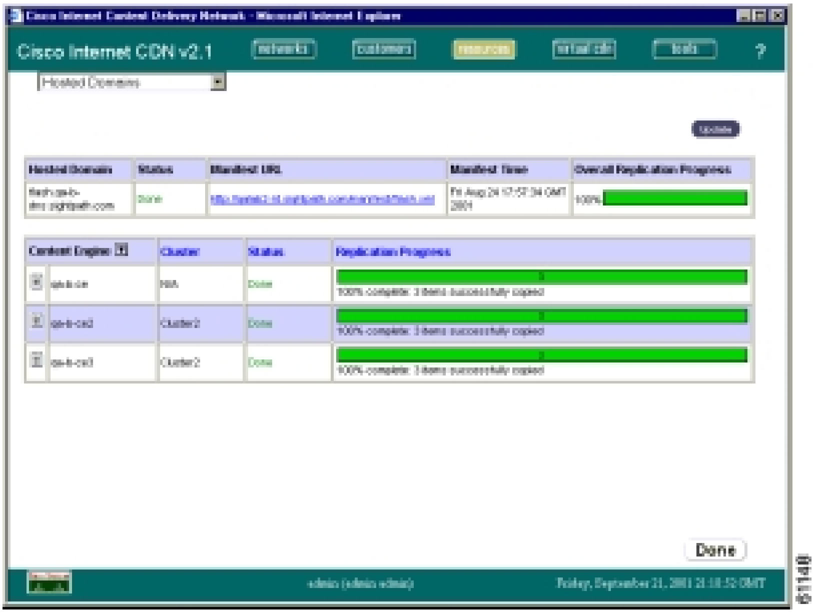
Step 4 Click **Purge Content**. You are prompted to confirm your decision to remove all cached content from the hosted domain.

Step 5 Click **OK** to confirm your decision.

Viewing the Status of Content Replication to a Hosted Domain

For any hosted domain, you can view the status of content replication to the Content Engines on that hosted domain.

Figure 3-8   View Content Replication Status



Hosted Domain	Status	Manifest URL	Manifest Time	Overall Replication Progress
flash.qa-b-dns.sightpath.com	Done	[illegible]	Fri Aug 24 17:57:34 GMT 2001	100%

Content Engine		Cluster	Status	Replication Progress
	qa-b-ce	N/A	Done	100% complete: 3 items successfully copied
	qa-b-ce2	Cluster2	Done	100% complete: 3 items successfully copied
	qa-b-ce3	Cluster2	Done	100% complete: 3 items successfully copied

admin (admin admin)   Friday, September 21, 2001 21:18:52 GMT

To view the replication status of your hosted domain:

Step 1 From the Cisco Internet CDN Software user interface, click **resources.**

Step 2 From the drop-down list, choose **Hosted Domains**.

The View Hosted Domains page appears. (See Figure 2-16.)

Step 3 Click the edit icon next to the name of the hosted domain you wish to edit. The browser window refreshes, displaying the Modify a Hosted Domain page. (See Figure 3-7.) Fields for editing the selected hosted domain appear.

Step 4 Click the **Replication Status** button. The View Content Replication Status page appears, which provides a graphic representation of the progress of content replication for each Content Engine.

Step 5 Click **Update** to refresh your screen and obtain current replication status information.

Note It may take a few moments for the replication status to be updated on the Replication Status display when a Content Engine encounters errors in a manifest file.

Viewing the Content Replication Log for a Content Engine

Content Engines log each piece of content that is replicated to or purged from them in a text-format log file. Replication log files take the name of the hosted domain to which they apply, and are maintained for each Content Engine in the hosted domain. For example:

```
hosted_domain_name.log
```

You can use the replication log to review the replication activity for a given device and determine which content items were and were not successfully copied from your origin server to the Content Engine. For example:

```
Thu May 10 19:04:45 GMT 2001 Filler [I]:
/www.cdn.cisco.com/SeaLion.mpeg#23 Imported.
Thu May 10 19:05:02 GMT 2001 Filler [I]:
/www.cdn.cisco.com/Madonna-Music.mpeg#19 Imported.
Thu May 10 19:05:06 GMT 2001 Filler [I]:
/www.cdn.cisco.com/Everclear-Wonderful.mpeg#22 Imported.
```

To view the content replication log for a Content Engine on your hosted domain:

Step 1 From the Cisco Internet CDN Software user interface, click **resources.**

Step 2 From the drop-down list, choose **Hosted Domains**.

The View Hosted Domains page appears. (See Figure 2-16.)

Step 3 Click the edit icon next to the name of the hosted domain you wish to edit. The browser window refreshes, displaying the Modify a Hosted Domain page. (See Figure 3-7.) Fields for editing the selected hosted domain appear.

Step 4 Click the **Replication Status** button. The View Content Replication Status page appears, which provides graphic representations of the progress of content replication for each Content Engine.

Step 5 Click the **Update** button to display the most current replication status information.

Step 6 Adjacent to the name of the Content Engine for which you wish to view the replication log, click the page icon. You are prompted to download the file from the Content Engine.

Step 7 Click the **Open File** or **Save to File** button and click **OK**. You can view the log file using any ASCII text editor.

Printing and Exporting CDN Data

Using the features of the Content Distribution Manager, you can output any tabular data on your CDN network in either printed or electronic format. This includes lists of customers, virtual CDNs, regions and locations, or any of the resources of your CDN, such as Content Engines, hosted domains, and so on.

Once output, your CDN data can be incorporated into presentations or, in electronic format, imported into spreadsheets or other third-party applications.

To print or export data from the Content Distribution Manager:

Step 1 From the Cisco Internet CDN Software user interface, locate the information you wish to print or export.

For example, if you wanted to print or export data on the regions defined for your CDN, you would click **networks** to display the list of all regions for the CDN. Alternatively, you could click **resources** and then choose **Regions** from the drop-down list to achieve the same result.

Step 2 With the data you would like to print or export displayed on the Content Distribution Manager, click the appropriate button above the displayed data:

- To print your CDN data using the default printer on your operating system, click **Print**.
- To export your CDN data to a comma-separated file that can be imported to a spreadsheet or other third-party application, click **Export**. You are prompted to save or open a file named exportcsv.jsp. This is your comma-separated file containing the data from the table.

Step 3 Click **Save** and choose a location on your workstation or network for the file.

Maintaining Cisco Internet CDN Software

This chapter contains information on maintaining and troubleshooting your Cisco Internet CDN Software. Additional configuration and troubleshooting information can be found in the hardware documentation that shipped with your CDN devices.

This chapter contains the following sections:

Adding and Removing SNMP Managers

The Cisco Internet CDN Software allows you to deploy one or more Simple Network Management Protocol (SNMP) managers for your CDN.

Note Registering a new SNMP manager with your CDN, as well as modifying or removing a registered SNMP manager, causes all your CDN nodes to restart as they register the configuration change. Restarting your CDN devices results in a temporary interruption in service across your CDN for the time it takes your devices to come back online—usually a few minutes.

See Appendix Appendix B, “Deploying SNMP on Content Delivery Networks,” for more information on using SNMP with your CDN.

Creating an SNMP Manager

Each Cisco Internet CDN Software Version 2.1 device comes with the software necessary to communicate information about device configuration and activity using the SNMP protocol. However, before you can begin logging SNMP data, your organization needs to acquire and deploy an SNMP manager application for use with the CDN.

You can create your SNMP manager using the published CISCO-CONTENT-NETWORK-MIB, which is available from Cisco.com or through FTP from:

```
ftp://ftpeng.cisco.com/pub/mibs
```

Cisco Internet CDN devices also support the Internet standard HOST-RESOURCES-MIB (RFC 1514). Once you have configured an SNMP manager on your network, use the SNMP Configuration feature on the Content Distribution Manager to point to that device.

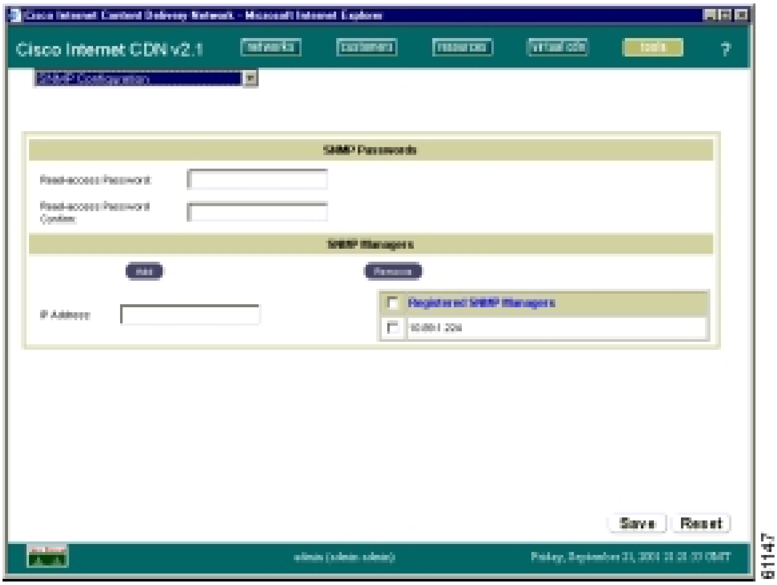
Registering an SNMP Manager with the CDN

To add an SNMP manager to your CDN:

Step 1 From the Cisco Internet CDN Software user interface, click **tools**.

Step 2 From the drop-down list, choose **SNMP Configuration**. The SNMP Configuration Tool page appears. (See Figure 4-1.)

Figure 4-1 SNMP Configuration Tool



Step 3 In the IP Address field, enter the address of your SNMP manager.

Step 4 Click **Add**. The manager is added to the list of registered SNMP Managers. Your CDN will temporarily go offline as each CDN node registers the new SNMP manager. This interruption should only last a few minutes.

Removing an SNMP Manager

To remove an SNMP manager from your CDN:

Step 1 From the Content Distribution Manager user interface, click **tools**.

Step 2 From the drop-down list, choose **SNMP Configuration**. The SNMP Configuration Tool page appears. (See Figure 4-1.)

Step 3 In the list of registered SNMP managers, check the check box adjacent to the IP address of your SNMP manager.

Tips To choose all SNMP Managers, check the box at the top of the column in the header area.

Step 4 Click **Remove**. You are prompted to confirm your decision to remove the manager.

Step 5 Click **OK**. The manager is removed from the list of registered SNMP managers.

Changing System Passwords

All CDN devices maintain two separate passwords for each login account:

- HTTP password—This is used by CDN administrators to log in to CDN devices using a web browser.
- Root password—This is used by CDN administrators to log in directly to a CDN device to gain access to the command-line interface for that device.

All CDN devices are shipped to customers with both the HTTP and root passwords set to a default value, called the “system password.” This default value can be initially used to log in to either the device’s web interface or its command-line interface.

Note Default passwords for each device should be changed at the earliest possible opportunity, with the root and HTTP passwords set to different alphanumeric values.

For information about changing the root or HTTP password for individual Content Engines or Content Routers, see the "Modifying Content Engine Passwords" section on page 3-13 and the "Modifying Content Router Passwords" section on page 3-22.

Once the HTTP and root passwords have been changed, the system password can no longer be used to log in to devices from either the web interface or the command-line interface. Instead, the system password you define acts as an "override" password for your Content Distribution Manager and other CDN devices.

The system passwords feature is used to manage your system passwords only *after* the default password values have been changed. System passwords ensure that administrators can access their devices either through the web interface (HTTP password) or through the command-line interface (CLI password), even when an individual device password has been lost or forgotten.

For example, if you have a different password for each device on your CDN and the password for one of your Content Engines has been forgotten or lost, you can substitute the system password for the forgotten password on the Modify a Content Engine page of the Content Distribution Manager graphical user interface and reset either the HTTP or root passwords currently assigned to that device.

Use the sections that follow to change the system password for either the Content Distribution Manager or your Content Engines and Content Routers.

Changing the Content Distribution Manager System CLI Password

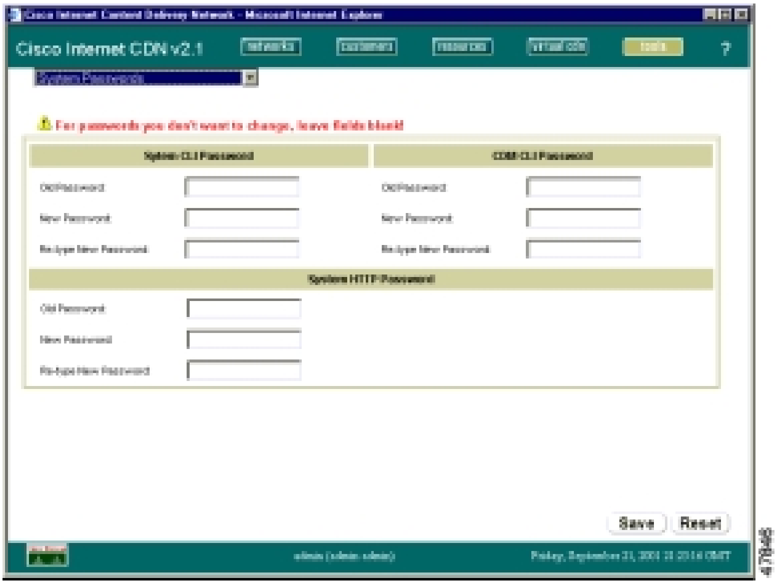
To change the Content Distribution Manager CLI password, follow these steps:

Step 1 From the Cisco Internet CDN Software user interface, click **tools**.

Step 2 From the System Tools drop-down list, choose **System Passwords**.

The System Passwords page appears. (See Figure 4-2.)

Figure 4-2 System Passwords



For passwords you don't want to change, leave fields blank!

System CLI Password		CDM CLI Password	
Old Password		Old Password	
New Password		New Password	
Re-type New Password		Re-type New Password	

System HTTP Password	
Old Password	
New Password	
Re-type New Password	

admin (admin: admin)

Friday, September 21, 2001 11:20:14 GMT

Step 3 Under the CDM CLI Password heading, enter the old and the new passwords in the Old Password and New Password fields, and then reenter the new password in the Re-type New Password field. This updates the password used to access the command-line interface on the device that serves as your primary Content Distribution Manager.

Note All passwords should contain exactly eight characters.

Step 4 Click **Save**. You may be prompted to enter the new password value into the CDM login dialog. If prompted, enter the new password into the Password field and click **OK**.

The System Passwords page refreshes. If the password was successfully changed, a green circle with a check mark is displayed next to the affected password field. See the "Content Distribution Manager Icons" section on page 1-23 for details.

Changing the CLI System Password for Content Engines and Content Routers

You change the CLI password for all your Content Engines and Content Routers by entering new password values into the field provided in the System CLI Password area of the System Passwords page.

When you click **Save**, the system password on each Content Engine and Content Router on your CDN is overwritten with the new password value you specified.

Once you have a usable system password value, use it to modify a Content Engine or Content Router password, as outlined in the "Modifying Content Engine Passwords" section on page 3-13 and the "Modifying Content Router Passwords" section on page 3-22 if the original password has been forgotten.

To change the system CLI password for your Content Engines and Content Routers, follow these steps:

Step 1 From the Cisco Internet CDN Software user interface, click **tools**.

Step 2 From the System Tools drop-down list, choose **System Passwords**.

The System Passwords page appears. (See Figure 4-2.)

Step 3 Under the System CLI Password heading, enter the old and the new passwords in the Old Password and New Password fields, and then reenter the new password in the Re-type New Password field. This updates the system password used to access the command-line interface on all Content Engines and Content Routers.

Note All passwords should contain exactly eight characters.

Step 4 Click **Save**. The system CLI password change is circulated to all Content Engines and Content Routers on your CDN. This may take a few minutes.

Changing the HTTP System Password for CDN Devices

The HTTP system password is used to gain access to the web interface for any CDN device. In the case of the Content Distribution Manager, the system HTTP password can give an administrator access to the Content Distribution Manager graphical user interface if the normal account password is lost or forgotten. In the case of Content Routers and Content Engines, the system HTTP password gives administrators access to high-level device configuration options that are accessible only from the device's web interface.

To change the system HTTP password for your CDN devices, follow these steps:

Step 1 From the Cisco Internet CDN Software user interface, click **tools**.

Step 2 From the System Tools drop-down list, choose **System Passwords**.

The System Passwords page appears. (See Figure 4-2.)

Step 3 Under the System HTTP Password heading, enter the old and the new passwords in the Old Password and New Password fields, and then reenter the new password in the Re-type New Password field. This updates the system password used to access the web interface on any CDN device.

Note All passwords should contain exactly eight characters.

Step 4 Click **Save**. The system HTTP password change will be circulated to all devices on your CDN. This may take a few minutes.

Resetting the CLI and HTTP Passwords for CDN Devices

If you lose access to your CDN devices, either by losing or forgetting the CLI or HTTP passwords, you can reset the device passwords for a given device to their default value.

Note Once you have access to the device using the default password, you must promptly use the password features available through the Content Distribution Manager graphic user interface to create a new password for the device.

See the "Modifying Content Engine Passwords" section on page 3-13 or the "Modifying Content Router Passwords" section on page 3-22 for information on changing device passwords from the Content Distribution Manager.

You need access to the device console for the devices in question in order to reset the CLI and HTTP passwords. Refer to the hardware documentation that came with your device for instructions on connecting a monitor and keyboard or serial connection to the device for console access.

To reset CDN device passwords to their default values:

Step 1 If the device in question is up and running, reboot it.

Step 2 At the LILO boot prompt, enter the following command:

```
LILO boot: linux single
```

The device loads Linux and the prompt changes to indicate that bash has been invoked.

Step 3 At the bash prompt, enter the following command:

```
bash# /cisco/merlot/etc/reset-passwd
```

You are notified that the system default passwords have been restored.

Step 4 Reboot the device a second time as follows:

```
bash# reboot
```

When the device comes back online, you can log in to the CLI using the default CLI password value, or access the device web interface using the default HTTP password.

Managing Symmetric Keys

Symmetric keys are used to provide content-based security on a per-hosted domain basis within the CDN. Using symmetric keys, end user requests are “signed” by the content provider using a symmetric key—essentially an algorithm used to encrypt the request.

Content Engines within the hosted domain maintain a copy of each symmetric key for the hosted domain. When Content Engines receive an encrypted request, they determine which key was used to sign it, and then use the appropriate key from their own set to reproduce the unique signature (or message authentication code, MAC) of the request. If the Content Engine’s generated MAC value matches that of the request, the Content Engine knows that the request is authentic and attempts to serve it.

See the “Configuring Content Security for Hosted Domains” section on page 2-57 for information on creating symmetric keys for a hosted domain.

Viewing Symmetric Keys

Using the Symmetric Key Content Authorization (SKCA) feature, you can view the symmetric keys assigned to a hosted domain.

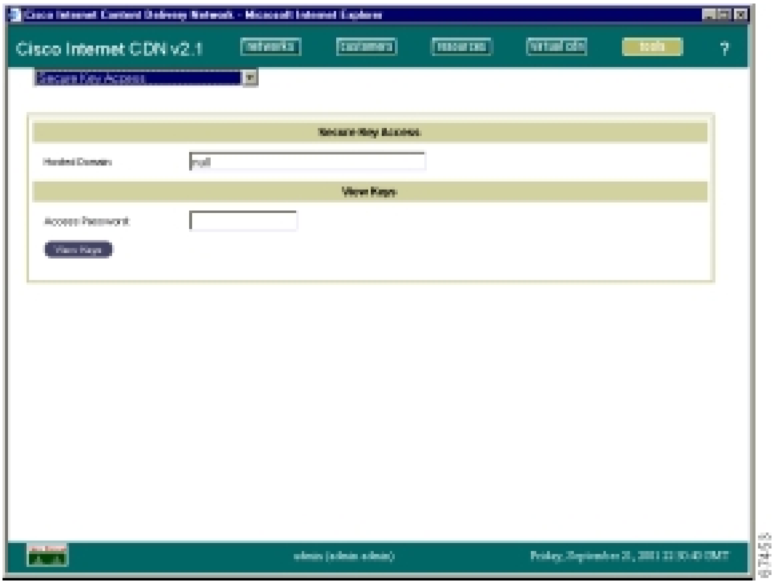
Note Before viewing symmetric keys for a hosted domain you must have the hosted domain address and secure access password.

To view the symmetric keys for a hosted domain:

Step 1 From the Cisco Internet CDN Software user interface, click **tools**.

Step 2 From the System Tools drop-down list, choose **Symmetric Key Access**. The Symmetric Key Access page appears. (See Figure 4-3.)

Figure 4-3 Symmetric Key Access



Secure Key Access

Hosted Domain: null

View Keys

Access Password:

Step 3 In the Hosted Domain field, enter the name of the hosted domain, exactly as it appears on the View Hosted Domains page. (See Figure 2-16.)

Step 4 In the Access Password field, enter the symmetric key access password. This password was created when you created your symmetric keys.

Step 5 Click the **View Keys** button. The Symmetric Key Access page appears, displaying the symmetric key ID value as well as start and expiration date.

Step 6 Use the **Next Key** and **Previous Key** buttons to view each of the symmetric keys for this hosted domain.

Changing the Symmetric Key Password

Symmetric key passwords allow content providers to view the authentication keys for their hosted domains. Passwords are created and maintained on the Modify a Hosted Domain page and should be changed periodically to protect symmetric keys from unauthorized access.

See the "Viewing Symmetric Keys" section on page 4-10 for information on viewing the symmetric keys for a hosted domain.

To change the symmetric key password for a hosted domain:

Step 1 From the Cisco Internet CDN Software user interface, click **resources**.

Step 2 Choose **Hosted Domains** from the drop-down list.

The View Hosted Domains page appears. (See Figure 2-16.)

Step 3 Click the icon adjacent to the name of the hosted domain that you want to change. The Modify a Hosted Domain page appears. (See Figure 3-7.)

Step 4 Under the Content Security heading, enter the existing symmetric key password in the Old Key Access Password field.

Note You may have to scroll through the Modify a Hosted Domain screen to see the content security configuration fields.

Step 5 In the New Key Access Password field, enter the new symmetric key access password.

Step 6 In the Confirm New Key Access Password field, reenter the new symmetric key access password value.

Step 7 Click **Save** to confirm your change to the symmetric key access password. The old password value and both of the new password values have to be entered correctly before the CDN will allow you to modify the symmetric key access password.

Modifying Playserver Configuration

Cisco Internet CDN devices support a wide variety of media types, including RealNetworks RealMedia, Microsoft Windows Media Server, and Apple QuickTime.

In order for your CDN devices (the Content Distribution Manager and Content Engines) to be able to serve these media types, you must tell the CDN that a particular playserver type is present.

If there is a particular media type that you *do not* want to serve through your CDN, you need to disable the corresponding playserver so that your CDN devices do not attempt to serve that media type.

Using the playserver mappings in the manifest file, you can customize your content type mappings from MIME content types or file extensions to configured playservers. See the "Manifest File Structure and Syntax" section on page 2-4 for more information on customizing content type mappings.

Note Modifying the configuration of any playserver causes any CDN nodes running that playserver software to restart and register the configuration change. Depending on the number and location of devices that restart following a playserver configuration change, you may experience a temporary interruption in service for the time it takes your devices to come back online—usually a few minutes.

Use the following information to enable, disable, or modify the configuration of your CDN playservers.

Modifying Windows Media Services Configuration

Cisco Internet CDN Software supports Windows Media Technologies for delivering static, pre-positioned, video-on-demand, and live streamed content to users over the Internet. Microsoft Windows Media Technologies consists of a suite of components that make possible the distribution of live streams and broadband content over the Internet.

Note In order to use Windows Media Technologies with your CDN, you must first obtain valid licenses from Cisco.com for each Content Engine that will be running Windows Media Services. See the "World Wide Web" section on page xviii or the "Obtaining Technical Assistance" section on page xix for information on obtaining Windows Media Technologies licenses for your Content Engines.

Using the Windows Media Server Configuration page on the Content Distribution Manager, you must first register your acceptance of the Windows Media Technologies license agreement, after which you can make changes to a number of Windows Media Services settings remotely, or deactivate Windows Media Services altogether.

After you have accepted the Windows Media Technologies license agreement and enable the use of Windows Media Services on your CDN, you can then activate Windows Media Services on your hosted domains.

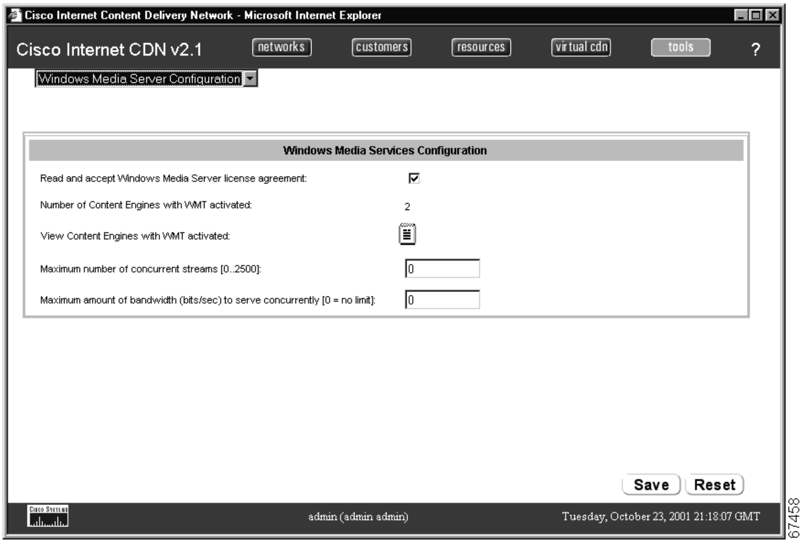
Enabling Windows Media Services on Your CDN

To enable the use of Windows Media Services on your CDN:

Step 1 From the Cisco Internet CDN Software user interface, click **tools**.

Step 2 From the drop-down list, choose **Windows Media Server Configuration**. The Windows Media Server Configuration page appears. (See Figure 4-4.)

Figure 4-4 Windows Media Server Configuration


Cisco Internet Content Delivery Network - Microsoft Internet Explorer
Cisco Internet CDN v2.1
networks
customers
resources
virtual cdn
tools
?
Windows Media Server Configuration
Save
Reset
admin (admin admin)
Tuesday, October 23, 2001 21:18:07 GMT
67458

Windows Media Services Configuration

Read and accept Windows Media Server license agreement: ☑

Number of Content Engines with WMT activated: 2

View Content Engines with WMT activated:

Maximum number of concurrent streams [0..2500]: 0

Maximum amount of bandwidth (bits/sec) to serve concurrently [0 = no limit]: 0

Step 3 Click the **Read and Approve Windows Media Server** option.

Step 4 Click **OK**. The Windows Media Technologies license agreement appears. You are required to scroll through and read the entire license agreement before continuing.

Step 5 At the bottom of the license agreement, click **Agree**. You are returned to the Windows Media Server Configuration page. Options appear for configuring your Windows Media Server. (See Figure 4-4.)

See the "Activating Windows Media Services for a Hosted Domain" section on page 2-56 for instructions on enabling Windows Media Services on your hosted domains.

See the next section, "Configuring Windows Media Technologies Streaming," for instructions on modifying your Windows Media Server settings.

Configuring Windows Media Technologies Streaming

Cisco Internet CDN Software supports streaming data for up to 2500 concurrent client connections per CDN device (Content Distribution Manager or Content Engines).

Using the Windows Media Services configuration feature, you can specify the maximum number of simultaneous client connections and the maximum amount of bandwidth that will be allowed for each CDN device that is serving client requests.

Limiting the number of concurrent sessions and the amount of total bandwidth devoted to serving client requests may potentially deny immediate access to CDN data to some clients. However, doing so also preserves system resources, resulting in optimal performance for clients who are being served. Consider the likely volume of requests you will receive, as well as the bandwidth requirements of the content you are serving and the needs of your customers, before making changes to the Windows Media Technologies streaming configuration.

To modify the Windows Media Technologies streaming configuration:

Step 1 From the Cisco Internet CDN Software user interface, click **tools**.

Step 2 From the drop-down list, choose **Windows Media Server Configuration**.

The Windows Media Services Configuration page appears. (See Figure 4-4.)

Step 3 In the Maximum number of concurrent streams field, enter a number corresponding to the maximum number of client connections each Content Engine and the Content Distribution Manager will allow. The maximum number of streams allowed by Cisco Internet CDN Software is 2500.

Step 4 In the Maximum amount of bandwidth (bits/second) to serve concurrently field, enter a value representing the amount of available network bandwidth, in bits per second, that each device can use to serve client requests.

For example, if you wanted to allocate 10 megabits per second for each Content Engine, you would enter:

```
10000000
```

Or, to allocate unlimited bandwidth, you would enter:

```
0
```

Step 5 Click **Save**. The settings used by Windows Media Services to stream content will be updated on all affected CDN devices. Content Engines in hosted domains on which Windows Media Services have been activated will restart following the change.

Viewing Content Engines Running Windows Media Services

Cisco Internet CDN Software automatically tracks the number and identity of Content Engines on which Windows Media Services have been activated.

Note Activating or deactivating Windows Media Services on a hosted domain affects all Content Engines on that domain. In addition, adding a Content Engine that has not had Windows Media Services activated to a hosted domain on which Windows Media Services have been activated will result in Windows Media Services automatically being activated on the newly added Content Engine.

To view the Content Engines on which Windows Media Services have been activated:

Step 1 From the Cisco Internet CDN Software user interface, click **tools**.

Step 2 From the drop-down list, choose **Windows Media Server Configuration**.

The Windows Media Services Configuration page appears. (See Figure 4-4.)

Step 3 Do one of the following:

- To view the number of Content Engines on your CDN on which Windows Media Services have been activated, refer to the Number of Content Engines with WMT activated field. This is a read-only field that is updated periodically by Cisco Internet CDN Software.
- To view which Content Engines on your CDN have had Windows Media Services activated, click the notepad icon labeled View Content Engines with WMT activated. A separate window opens, listing the names of Content Engines running Windows Media Services.

Modifying RealServer Configuration

Cisco Internet CDN Software supports RealServer for delivering static and live streamed content to users.

Note Although the Activate RealServer option is enabled by default on the Content Distribution Manager, in order to use RealServer with your CDN, you must first obtain a valid license from RealNetworks.

Using the Content Distribution Manager RealServer Configuration page, you can make changes to a number of RealServer settings remotely, or disable RealServer altogether.

Note For detailed instructions on managing your RealServer, refer to the RealNetworks documentation that came with your RealServer software, or visit the RealNetworks web page at http://www.realnetworks.com to access the RealServer documentation online.

Activating and Deactivating RealServer

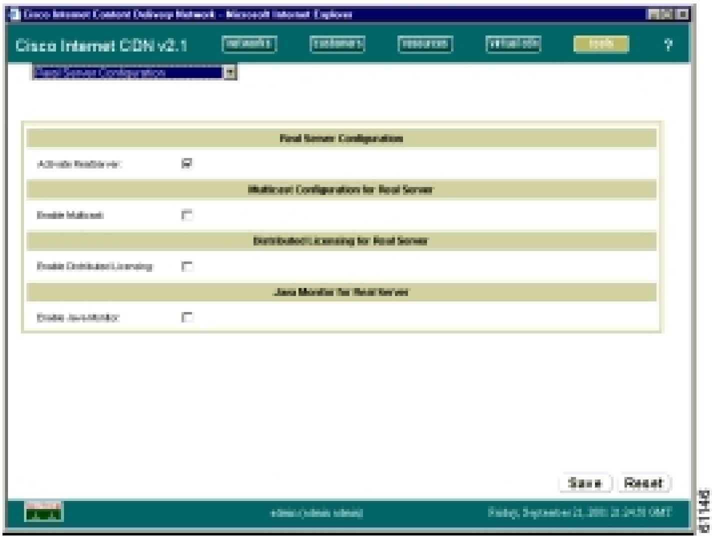
To modify your RealServer configuration:

Step 1 From the Cisco Internet CDN Software user interface, click **tools**.

Step 2 From the drop-down list, choose **Real Server Configuration**.

The Real Server Configuration page appears. (See Figure 4-5.)

Figure 4-5 RealServer Configuration



Real Server Configuration

Activate RealServer: ☑

Multicast Configuration for Real Server

Enable Multicast: ☐

Distributed Licensing for Real Server

Enable Distributed Licensing ☐

Java Monitor for Real Server

Enable JavaMonitor: ☐

Step 3 Check or uncheck the **Activate Real Server** box. When checked, this option instructs the CDN to serve RealMedia content using the RealServer installed on the serving Content Engine, as well as any other content types mapped to RealServer in the manifest file for each hosted domain.

Note Clicking **Reset** at any time before saving restores RealServer to its last configuration.

Step 4 Click **Save** to save your configuration changes. Any CDN devices with RealServer installed will restart in order to integrate the new configuration change.

Configuring RealServer Multicasting

When enabled, this option enables the RealServer multicasting feature on your network, enabling Cisco Internet CDN installations to conserve bandwidth by sending a single media stream to multiple clients, rather than streaming media to each requesting client individually.

When enabled, 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." RealServer multicasting allows you to track client behavior and display statistics during viewing, including real-time data on the number of clients receiving a presentation. Data collected can be reviewed and analyzed using the Java Monitor or RealSystem Administrator. See the "Modifying the RealServer Java Monitor Configuration" section on page 4-23 for more information on the Java Monitor.

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

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

To modify your RealServer multicasting settings:

Step 1 From the Cisco Internet CDN Software user interface, click **tools**.

Step 2 From the drop-down list, choose **Real Server Configuration**.

The Real Server Configuration Tool page appears. (See Figure 4-5.)

Step 3 To enable multicasting, check the **Enable Multicast** check box. Additional configuration options appear.

Step 4 Enter the base address of the address range to which you will be sending multicast streams in the **Address Base** field.

RealServer uses the first available address in the range you specify. Refer to the “Calculating Addresses for Back-Channel Multicasts” section in the *RealServer Version 8 Administration Guide* for more information on determining the number of required addresses for multicasting.

Step 5 Enter the value by which multicast addresses will be incremented in the **Address Step** field.

For example, if the base address is 240.3.0.0 and the address step is 32, then the first multicast address used is 240.3.0.0, and the second address used is 240.3.0.32.

Step 6 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 TTL 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 RealServer discards the packet.

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

Note Clicking **Reset** at any time before saving restores RealServer to its last configuration.

Step 7 Click **Save** to save your RealServer configuration changes. Any CDN devices with RealServer installed restart to integrate the new multicasting configuration change.

Configuring RealServer Live Splitting

Cisco Internet CDN Software supports splitting of live streams, enabling live broadcasts to be forwarded from an origin RealServer (referred to as a transmitter) to one or more receiver RealServers.

Splitting makes it possible to replicate streams to locations close to requesting clients, improving the response time for client requests and the quality of the streamed broadcast, while also making it possible to serve a larger number of clients.

Before taking advantage of the live splitting feature, you must configure your transmitting RealServer properly.

The following changes must be made to your RealServer transmitting server configuration:

- A pull-split source must be defined.
- If a pull-split listen port other than the default (2030) will be used, the manifest file for the hosted domain should identify the port to be used along with the host name under the server definition.

  For example, a manifest file would read:

  ```
  <server name=”transmitting-server”>
  <host name= ”10.89.1.1:2040”/>
  </server>
  ```

  If no port is defined after the host name, the default port is used as the listen port.
- The Security Type parameter must be set to *None*.

Refer to “Chapter 12: Splitting Live Presentations” in the *RealServer Administration Guide* for instructions on setting live stream security as well as configuring your transmitting server for pull splitting. The *RealServer Administration Guide* is available online at the following URL:

http://service.real.com/help/library/guides/server8/realsrvr.htm

See the “<host />” section on page 2-12 for instructions on modifying your manifest file to include the nondefault listen port on the transmitting RealServer.

Configuring RealServer Distributed Licensing

The RealServer distributed licensing feature enables you to purchase a single license to be used by multiple RealServers on your network that share a pool of streams.

The RealServers that share a license are called a *license group*. Each license group consists of a coordinating RealServer, referred to as the *publisher RealServer*, on which the license file is placed, and cooperating RealServers, referred to as *subscriber RealServers*, that are configured to look for the publisher RealServer and determine whether there are streams available for use under the license.

It is also possible to configure a secondary publisher RealServer if no connections are available for your primary publisher.

For more information on distributed licensing, refer to the "Distributed Licensing" section in the *RealServer Version 8 Administration Guide*

To modify your Real Server configuration and enable distributed licensing:

Step 1 From the Cisco Internet CDN Software user interface, click **tools**.

Step 2 From the drop-down list, choose **Real Server Configuration**.

The Real Server Configuration Tool page appears. (See Figure 4-5.)

Step 3 Check the **Enable Distributed Licensing** check box. Options for configuring distributed licensing appear.

Step 4 Under the Distributed Licensing URL heading, enter the URL that points to the license file on the publisher RealServer.

Step 5 Under the Primary Publisher heading, enter the IP address of the publisher RealServer in the IP field and the admin port number for the subscriber RealServer in the Port field.

Step 6 If you are deploying a backup publisher RealServer that can be contacted if connections to the primary publisher server are not available, repeat Step 5 for the fields under the Secondary Publisher heading; otherwise, proceed to Step 7.

Step 7 Under the Authorization heading, in the appropriate fields, enter the username and password required to access the publisher RealServer.

Note Clicking **Reset** at any time before saving restores RealServer to its last configuration.

Step 8 Click **Save** to save your configuration changes. Any CDN devices with RealServer installed will restart to integrate the new license distribution change.

Modifying the RealServer Java Monitor Configuration

RealServer comes supplied with a real-time monitor that displays activity on your RealServer. You can use the Java Monitor to:

- Manage content and change the server configuration remotely
- Make more informed business decisions

You can also create other external Java Monitors if you need to track more than one RealServer or monitor multiple RealServers side by side.

To configure the RealServer Java Monitor:

Step 1 From the Content Distribution Manager user interface, click **tools**.

Step 2 From the drop-down list, choose **Real Server Configuration**.

The Real Server Configuration Tool page appears. (See Figure 4-5.)

Step 3 To enable the Java Monitor, check the **Enable Java Monitor** check box.

Before using the RealServer Java Monitor, you must specify the port number that the monitor will use when connecting to your RealServer and, optionally, a password that can be used to access the monitor. The default value for the port is 9090.

Step 4 If necessary, in the **Port** field, change the default port number to the port your RealServer is using.

Step 5 If necessary, in the **Password** field, enter a new password for accessing the Java Monitor. Although it is not encrypted, this field does not display the password value once it has been saved, reading *invalid* instead.

Note Clicking **Reset** at any time before saving restores RealServer and the Java Monitor to their last configuration.

Step 6 Click **Save** to change your settings to the Java Monitor configuration. Any CDN devices with RealServer installed restart to integrate the new configuration change.

Modifying QuickTime Server Configuration

Your Cisco Internet CDN Content Distribution Manager and Content Engines come with the Apple Computer Darwin Streaming Server already installed. This server is used to stream QuickTime-format media to users.

By default, your Content Distribution Manager has the Darwin Streaming Server enabled. If you do not wish the Darwin Streaming Server to be enabled on your CDN, use the QuickTime Configuration page to disable this playserver.

To configure your QuickTime server:

Step 1 From the Content Distribution Manager user interface, click **tools**.

Step 2 From the drop-down list, choose **QuickTime Configuration**. The QuickTime Configuration page appears.

Step 3 To disable your QuickTime server, uncheck the **Activate QuickTime** check box. QuickTime content will not be served from your CDN, or will be served by the playserver specified in the manifest of each of your hosted domains.

Step 4 Click **Save** to change your QuickTime configuration. Any CDN devices with the QuickTime Darwin Streaming Server installed will restart to integrate the new configuration change.

Modifying Routing Properties

Cisco Internet CDN Software allows you to modify a number of configuration settings that affect content routing on the CDN, including the deployment of coverage zones used in static content routing.

For a detailed discussion of CDN content routing, see the "Routing End User Requests to Content Engines" section on page 1-12.

Note Configure your Domain Name System (DNS) server before making any changes to the routing properties. Refer to the "Configuring DNS" section in Chapter 2 of the *Cisco Internet CDN Software Configuration Guide*.

Modifying Dynamic Routing Properties

Most requests for CDN content are handled using dynamic routing, as described in the "Routing a Request" section on page 1-13. Using the routing properties feature, available from the Tools area of the Content Distribution Manager, you can adjust a number of configuration properties that affect the routing behavior of your Content Routers and Content Engines.

To modify dynamic routing properties on your CDN:

Step 1 From the Content Distribution Manager user interface, click **tools**.

Step 2 From the drop-down list, choose **Routing Properties**. The Routing Properties page appears.

Step 3 Modify any of the Time to Live (TTL) or name server (NS) configuration settings to match your organization's needs. See Table 4-1 for explanations of the various dynamic routing configuration settings.

Step 4 Click **Save**. A message appears, indicating that the dynamic routing settings have been modified.

Step 5 Click **OK**. You are returned to the Routing Properties page.

Table 4-1 Dynamic Routing Properties

Routing Property	Description
Time To Live (TTL) of a glue A record associated with NS records naming supernodes	Read only. This field shows the duration, in seconds, of the Content Engine address records contained in the name server records returned to the DNS proxy from the Content Router.
Time To Live (TTL) of NS records naming supernodes, if all supernodes are in preferred locations	This field affects the TTL of the name server records for supernodes returned to the DNS proxy by the Content Router when all supernodes are in preferred locations.
Time To Live (TTL) of NS records naming supernodes, if some supernodes are not in preferred locations	This field affects the TTL of the name server records for supernodes returned to the DNS proxy by the Content Router when some supernodes named are not in preferred locations.
Time To Live (TTL) of A records identifying Content Engines	This field affects the life span, in seconds, of the A(ddress) record returned by a Content Engine identifying the Content Engine content IP address or the virtual IP address of a Content Engine cluster.
Minimum number of NS records	This field affects the minimum number of NS records that the Content Router returns for any request, unless there are fewer supernodes and standalone Content Engines on the CDN than the minimum number.

Table 4-1 Dynamic Routing Properties(continued)

Routing Property	Description
Target number of NS records if any are in preferred locations	This field affects the number of name server records that the Content Router returns for any request in which some devices are in preferred locations. The Content Router will not select additional name server records to meet the target if that would require returning records from nonpreferred locations.
Target number of NS records if none are in preferred locations	This field affects the number of name server records that the Content Router returns for any request in which no devices are in preferred locations.
Force NS records to identify two different locations	This field, when enabled, forces the Content Router to select supernodes or standalone Content Engines from two locations in any response to the DNS proxy.

Configuring Static Routing

Coverage zones allow Cisco Internet CDN Software to select the most appropriate device for serving each user request, even in unusual network configurations in which requesting DNS proxies are not located near the clients they are serving. Using a separate coverage zone file maintained by the content provider, DNS proxies requiring static routing are named, and preferred locations are specified for handling requests from known client addresses or address ranges.

For more information on the role coverage zones in CDN routing, see the "Static Routing" section on page 1-15.

Note Static routing works only if all Content Routers on the CDN and all Content Engines that might be called on to serve content using static routing are running Cisco Internet CDN Software Version 2.1 or later.

Using the routing properties feature of the Content Distribution Manager, you identify the location of your coverage zone file, which is fetched by each Content Engine and Content Router on your CDN. In addition, you can set a number of configuration parameters governing routing, such as Time to Live (TTL) values for the address (A) and name server (NS) records, and the number of NS records returned from the Content Router to the DNS proxy for requests handled using both standard and hybrid routing.

To modify static routing properties on your CDN:

Step 1 From the Content Distribution Manager user interface, click **tools**.

Step 2 From the drop-down list, choose **Routing Properties**. The Routing Properties page appears.

Step 3 If you have not already done so, enter the full URL of the coverage zone file in the field provided. The coverage zone file must be placed in a location that is accessible to all Content Engines and Content Routers on the CDN.

Step 4 Modify any of the Time to Live (TTL) or name server (NS) configuration settings to match your organization’s needs. See Table 4-2 for explanations of the various static routing configuration settings.

Step 5 Click **Save**. A message appears, indicating that the static routing settings have been modified.

Step 6 Click **OK**. You are returned to the Routing Properties page.

Table 4-2 Static Routing Properties

Routing Property	Description
Time To Live (TTL) of a glue A record associated with NS records naming supernodes	Read only. This field shows the life span, in seconds, of the Content Engine address records contained in the name server records returned to the DNS proxy from the Content Router.
Time To Live (TTL) of NS records naming supernodes, if some supernodes are not in preferred locations	This field affects the life span, in seconds, of the name server records for supernodes returned to the DNS proxy by the Content Router when the client address uses static routing.
Time To Live (TTL) of A records identifying Content Engines	This field affects the life span, in seconds, of the A(ddress) record returned by a Content Engine identifying the Content Engine content IP address or the virtual IP address of the Content Engine cluster.
Number of NS records to return when DNS client is in coverage zone	This field affects the number of name server records that the Content Router returns if the requesting client's IP address is in the range defined for a coverage zone.
URL of the coverage zone file	This is the full web address of the file specifying coverage zone information for the CDN. This file typically resides on a server maintained by the content provider, but must be accessible to all Content Engines and Content Routers on the CDN.

Sample Coverage Zone File

Coverage zone files can be created using any ASCII text editing tool. A single coverage zone text-format file defines all the coverage zones for a CDN.

Coverage zones are defined in the file by lists of DNS proxies from which requests are to be handled using static routing, and lists matching client addresses (or address ranges) with recommended locations on the CDN for handling requests from those clients.

When creating a coverage zone file, make sure that the following are true:

- The first line of the file reads *CZ1*, a tag that identifies the file to Cisco Internet CDN Software as a coverage zone file.
- DNS proxies are specified under the DNS heading.
- Addresses or address ranges are specified under the network heading when client machines that should be mapped to CDN locations are identified.
- Locations are listed in order of preference, with the locations designated “best” locations listed first, and locations designated “second-best” listed next, with a semicolon separating best from second-best.
- Locations are identified by the names assigned to them using the Content Distribution Manager.
- Names of locations containing spaces are enclosed within quotations (“ ”).
- Comment lines are preceded by a hash mark (#).

For example, the following could be a coverage zone file:

```
CZ1
#One or more DNS Proxies
DNS 10.89.11.1
#Addresses or address ranges mapped to CDN best locations
network 10.89.0.0/12  Waltham

#One or more DNS Proxies
DNS 10.89.11.1 10.89.50.113
#Addresses or address ranges mapped to CDN best locations
network 10.89.13.20/32Plymouth; Boxborough “North Adams”
```

Setting Up Remote Logging

Each Content Engine logs the following information locally:

- HTTP requests that the device processes
- RealServer activity
- QuickTime server activity

You can specify that these log files be periodically deposited (in compressed form) on an FTP site. You can then use this information for billing content providers.

Note Make sure that the FTP server is set to accept only ACTIVE-mode sessions from clients before configuring remote logging on the Content Distribution Manager. Only ACTIVE-mode transfers of the CDN logs will work.

If you choose not to enable remote logging, log files are stored locally for a time on the Content Engine but are eventually removed from the device to make room for more recent log files. Each Content Engine stores approximately 100 to 150 MB of archived log files. Log files are removed from the Content Engine based upon their age, with the oldest log files being deleted first.

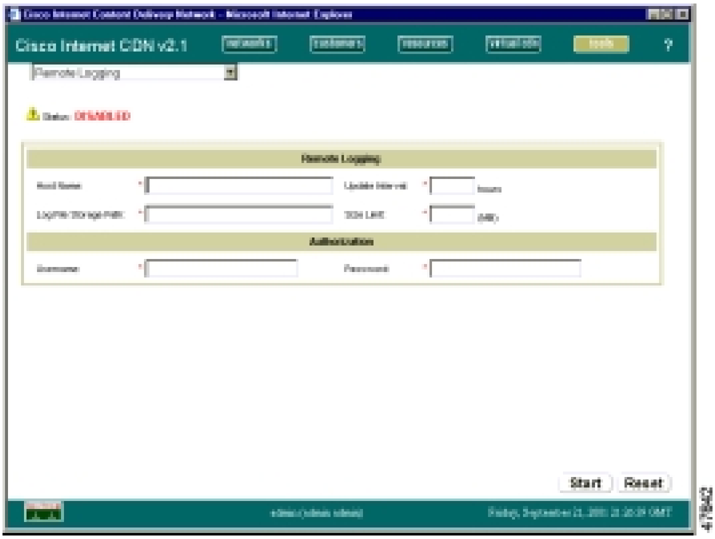
To specify that Content Engines deposit log information about HTTP requests, follow these steps:

Step 1 From the Cisco Internet CDN Software user interface, click **tools**.

Step 2 From the drop-down list, choose **Remote Logging**.

The Remote Logging page appears. (See Figure 4-6.) The status of the Remote Logging feature appears at the top of the page. Verify that the status is *disabled* before proceeding.

Figure 4-6 Remote Logging



Step 3 In the Host Name field, enter the DNS name or the IP address of the remote FTP site where you want the Content Engine usage information logs to be deposited. For example, enter:

`ftp.mydomain.com`

Step 4 In the Log Files Storage Path field, enter the path on the remote FTP server where you want the log files deposited. For example, enter:

`/cenglog/path`

Step 5 In the Update Interval field, enter the frequency (in hours) that the system checks for log files on the selected device to be transferred to the remote FTP server. If log files are not available for transfer, no action is taken.

Step 6 In the Size Limit field, enter the maximum allowed size for log files transferred to the remote server. Log files that are larger than the maximum allowed size are not transported to the remote FTP server, so be sure to use a conservative estimate when supplying this ceiling.

Step 7 In the Username and Password fields, enter a username and a password to access the remote FTP server.

Step 8 Click **Start** to begin remote logging on the selected device. Once you have started remote logging, clicking **Stop** cancels it.

Secure Transfer of Internet CDN Software Log Files

Cisco Internet CDN Software supports the secure transfer of log files from CDN devices to a remote logging server. This feature prevents outsiders from "sniffing," intercepting, and gaining access to the information in CDN log files as they are being transferred between Content Engines on your CDN and your designated remote logging server.

Encrypted log files have a GPG extension on your remote logging server, for example:

```
192.168.3.24~access.log.1~20010628082504.cdn.gpg
```

You need to have the Gnu Privacy Guard (GPG) software installed on your remote logging server in order to decrypt the CDN log files once they are received. GPG is freely available as shareware on the Internet. Refer to the Gnu Privacy Guard web page at:

http://www.gnupg.org

To specify that Content Engines deposit log information about HTTP requests in a secure, encrypted format, follow these steps:

Step 1 From the Cisco Internet CDN Software user interface, click **tools**.

Step 2 From the drop-down list, choose **System Configuration**.

The System Configuration page appears.

Step 3 Locate the enableLogFileEncryption option in the left-hand column.

Step 4 In the middle column, enter **true** in the field provided. This enables the secure log file transfer feature.

Step 5 Locate the LogFileEncryptionKey option in the left-hand column.

Step 6 In the middle column, enter an alphanumeric encryption password in the field provided.

This password is used to encrypt outgoing log files and then decrypt the same files once they have been received on the remote logging FTP server. You must enter a value in this field in order for the encryption to take place.

Step 7 Click **Save**. The Secure log file transfer option is enabled on all Content Engines on your CDN.

See "Setting Up Remote Logging" section on page 4-31 for more information on configuring your Content Engines to transfer CDN log files to a remote server.

Note CDN log file packages (with a GZ extension) that are generated before the enableLogFileEncryption option is enabled are not encrypted before transfer to the remote logging server.

Understanding Remote Logging Output

Once it is enabled, remote logging occurs from the selected device to the designated remote FTP server at the intervals you specified in the preceding section. Remote logging generates a compressed access log file with a filename in the following format:

```
IP address~access.logfiletype.lognumber.timestampMilliseconds.cdn.gz
```

where:

- *IP address* is the Internet address of the CDN device.
- *logfiletype* is an abbreviation that identifies the kind of log file generated. Three kinds of logs are supported on any Content Engine:
  - *log*—SQuID cache log
  - *rmlog*—RealServer access log
  - *StreamingServerlog*—Darwin Streaming Server access log
- *lognumber* is the sequence number of the file generated at a given time stamp.
- *timestampMilliseconds* is the time at which the log file was created in the format YYYYMMDDHHMMSS.

Log files are migrated a minimum of once per calendar day. In addition, log files are migrated to the remote logging server automatically when the log file size reaches 10 MB, or when the Content Engine is restarted for any reason.

In addition to the main compressed file containing access data, a second and corresponding log file is also placed on the remote host server. This file, which has an *.ok extension and the same filename as the compressed file to which it belongs, verifies that the compressed log file was transferred successfully from CDN device to the remote host server. For example:

```
IP address~access.logfiletype.log number.timestampMilliseconds.cdn.gz.ok
```

If no *.ok file was created for the compressed log file archive you transferred to the remote server, the log file archive may not have been properly uploaded to the server. Repeat the instructions in the "Setting Up Remote Logging" section on page 4-31.

SQuID Cache Log File Format

The SQuID cache log tracks the origin of HTTP requests to a given Content Engine, as well as the time of arrival of the request and how the Content Engine disposed of the request.

In response to any request for content, the Content Engine either:

- Serves content directly from its own cache, if that content is present
- Forwards the request on to the origin server to fulfill, if the requested content is not present in the Content Engine cache

SQuID cache log files use the following naming convention:

```
IP address~access.log.log number.timestampMilliseconds.cdn.gz
```

Each log is compressed with the UNIX gzip archiver, and must be decompressed before it can be read. SQuID cache log files contain an entry for each content item requested in the following format:

```
[TIME in sec].[TIME microsec] [milliseconds] [client ip] [REQUEST
status] / [HTTP_CODE] [SIZE] [HTTP_METHOD] [HTTP_URL] [CACHE_IDENT]/
[HIER_HOST] / [CONTENT_TYPE]
```

For example:

```
985794537.211    499 10.89.0.203 TCP_MISS/200 5538 GET
http://good.niagara.sightpath.com/images/homepage/smb-jobs-npm.gif -
DIRECT/www.cisco.com image/gif

985796546.734      1 10.89.1.190 TCP_MEM_HIT/200 4553 GET
http://good.niagara.sightpath.com/images/guest_navbar.gif - NONE/-
image/gif
```

Descriptions of the log record components follow.

SQuID Cache Log Record Component	Description
TIME in sec.TIME in microseconds	Time of day at which the logged event occurred, recorded in seconds and microseconds.
Milliseconds	Length of time, in milliseconds, that the SQuID cache spent processing the request.
Client IP	IP address of the requesting client.
Request Status	Label indicating whether or not the TCP request found its target content. Possible values when requests do find content are: • TCP_HIT • TCP_MEM_HIT • TCP_REFRESH_HIT • TCP_IMS_HIT • TCP_NEGATIVE_HIT • TCP_REFRESH_MISS When requests do not find content, the value is TCP_MISS.

SQuID Cache Log Record Component	Description
HTTP Code	HTTP status code for the requested item. Possible values are: • 200 HTTP OK • 204 No Content • 205 Reset Content • 206 Partial Content • 404 File Not Found • 409 Conflict
Size	Size of the requested content item, in bytes.
HTTP Method	Action requested for the requested content item. The value is GET.
HTTP URL	URL followed to request the content item. This identifies a valid CDN hosted domain and can be used for billing purposes to differentiate among different Content Provider services.
CACHE_IDENT	Filename of the requested content item.

SQuID Cache Log Record Component	Description
HIER_HOST	Indicates whether or not the request was moved up the CDN hierarchy to the origin server. Possible values are: • DIRECT—Indicates that there was a TCP miss and that the content was fetched from the origin server rather than served from the Content Engine cache. • NONE—Indicates that there was a TCP hit, and that the content was served directly from the Content Engine cache.
CONTENT_TYPE	Content MIME type specified in the HTTP response Content-type header, for example: `text/html` When no content type is specified, this field is left blank.

QuickTime Server Log File Format

In addition to the SQuID cache log, Content Engines running the Apple Computer Darwin Streaming Server for QuickTime generate and migrate separate log files detailing Darwin Server activity on the device.

As with all other log files, Darwin Server logs are migrated a minimum of once per calendar day and are automatically migrated to the remote logging server when the log file size reaches 10 MB, or when the Content Engine is restarted.

Darwin Streaming Server access log files use the following naming convention:

```
IP address~access.StreamingServerlog.log number.timestampMilliseconds.cdn.gz
```

Darwin Server log files generated on the Content Engine follow the access log format, documented in the supporting materials for Darwin Streaming Server 2.

This document is available online at:

http://www.publicsource.apple.com/projects/streaming/StreamingServerHelp/

Descriptions of the purpose of these and other logging configuration elements can also be found in the online help for the Darwin Streaming Server, available on the Internet at:

http://www.publicsource.apple.com/projects/streaming/StreamingServerHelp/

RealServer Log File Format

In addition to the SQuID cache log, Content Engines running RealServer will generate and migrate separate log files detailing RealServer activity. As with all other log files, RealServer logs will be migrated a minimum of one time per calendar day, and will automatically be migrated to the remote logging server when the log file size reaches 10 MB, or when the Content Engine is restarted.

RealServer access log files use the following naming convention:

IP address~access.rm**log**.*log number*.*timestampMilliseconds*.cdn.gz

RealServer log files generated on the Content Engine follow the RealServer Access Log format, documented in the chapter “Reporting RealServer Activity” in the *RealServer Administration Guide* for RealServer Version 8.0. This document is available online at:

http://service.real.com/help/library/guides/server8/realsrvr.htm

When generating RealServer log files, Internet CDN Content Engines use the following logging configuration settings:

Logging Configuration Element	Description
LoggingStyle	This setting determines how much data about media clips is gathered in the RealServer access log. The default setting used by Content Engines is 5.
StatsMask	This setting determines how much data about requesting clients is gathered in the access log. The default setting used by Content Engines is 3.

Descriptions of the purpose of these and other logging configuration elements can also be found in the *RealServer Administration Guide*.

Windows Media Technologies Log File Format

As with all other log files, Windows Media Server logs are migrated a minimum of once per calendar day and are automatically migrated to the remote logging server when the log file size reaches 10 MB, or when the Content Engine running Windows Media Server is restarted.

Windows Media Technologies log files use the following naming convention:

```
mms_export.YYMMDD.###
```

where ### represents a sequential number for that day.

The following is a list of fields that appear in the Windows Media Technologies log file used with Cisco Internet CDN Software. Descriptions are provided for each field.

Field	Description
audiocodec	Audio codec used in stream.
avgbandwidth	Average bandwidth (in bits per second) at which the client was connected to the server.
c-buffercount	Number of times the client buffered data while playing the stream.
c-bytes	Number of bytes received by the client from the server. For a unicast, c-bytes and sc-bytes must be identical. If not, packet loss has occurred.
c-cpu	Client computer CPU type.
c-dns	Client computer Domain Name Server name.
c-hostexe	Host application, for example, a web page in a browser (Iexplore.exe) or a Microsoft Visual Basic applet (Vb.exe) or standalone Microsoft Windows Media Player (Mplayer2.exe).
c-hostexever	Host application version number.

Field	Description
c-ip	Client computer IP address. A client that is not connected properly provides a client proxy server IP address, not the client IP address.
c-os	Client computer operating system.
c-osversion	Client computer operating system version number.
c-pkts-lost-client	Number of packets lost during transmission from server to client and not recovered at the client layer through error correction or at the network layer through User Datagram Protocol (UDP) resends.
c-pkts-lost-cont-net	Maximum number of continuously lost packets on the network layer during transmission from server to client.
c-pkts-lost-net	Number of packets lost on the network layer. Packets lost at the network layer can be recovered if the client re-creates them through forward error correction. The difference between c-pkts-lost-net and c-pkts-lost-client is c-pkts-recovered-ECC.
c-pkts-received	Number of packets from the server (s-pkts-sent) that are received correctly by the client on the first try.
c-pkts-recovered-ECC	Number of packets repaired and recovered on the client layer. Packets repaired and recovered at the client layer are equal to the difference between c-pkts-lost-net and c-pkts-lost-client.
c-pkts-recovered-resent	Number of packets recovered because they were resent through UDP.
c-playerid	Globally unique identifier (GUID) of the player.
c-playerlanguage	Client language-country code.

Field	Description
c-playerversion	Version number of the player.
c-quality	Percentage of packets that were received by the client, indicating the quality of the stream. If cPacketsRendered is all packets received by the client including packets recovered by error correction and UDP resend (c-pkts-received + c-pkts-recovered-ECC + c-pkts-recovered-resent) then c-quality can be calculated as: [cPacketsRendered / (cPacketsRendered + c-pkts-lost-client)] * 100
c-rate	Mode of Windows Media Player when the last command event was sent.
c-resendreqs	Number of client requests to receive new packets. This field contains a value only if the client is using UDP resend.
c-starttime	Time stamp (in seconds) of the stream when an entry is generated in the log file.
c-status	Codes that describe client status, mapped to HTTP/1.1 and RTSP client status codes described in Request for Comments (RFC) 2068 and RFC 2326. Windows Media Services includes the extensible client status codes 480 (simultaneous client connections exceeded the maximum client limit of the server) and 483 (stream exceeded maximum file bit rate limit of the server).
c-totalbuffertime	Time (in seconds) that the client used to buffer the stream. If the client buffers the stream more than once before a log entry is generated, c-totalbuffertime is the total amount of time that the client spent buffering the stream.

Field	Description
channelURL	URL to the .nsc file. A unicast client information log file records a “-” (hyphen) for this field.
cs(Referer)	URL to the web page in which Windows Media Player was embedded (if it was embedded).
cs-uri-stem	Name of the file that is playing: an .asf file for a unicast or an .asx file for a multicast.
cs(User-Agent)	Browser type used if Windows Media Player was embedded in a browser, Mozilla/4.0_(compatible;_MSIE_4.01;_ Windows_98) date, date (in Greenwich Mean Time) when an entry is generated in the log file.
filelength	Length of the file (in seconds). This value is 0 for a live stream.
filesize	Size of the file (in bytes). This value is 0 for a live stream.
protocol	Protocol used to access the stream: MMS, HTTP, or ASFM (multicast protocol).
s-cpu-util	Average load on the server processor (0%-100%). If multiple processors exist, this value is the average for all processors.
s-dns	Server DNS.
s-ip	Server IP address.
s-pkts-sent	Packets sent by the server.

Updating Cisco Internet CDN Software

From the Software Update page, you can:

- Determine the current version of Cisco Internet CDN Software
- Import software updates from remote locations, such as Cisco.com

- Update Cisco Internet CDN Software on the devices you specify
- Delete obsolete software updates

Note Contact your Cisco sales representative for information about obtaining the latest software upgrades.

Determining the Current Software Version

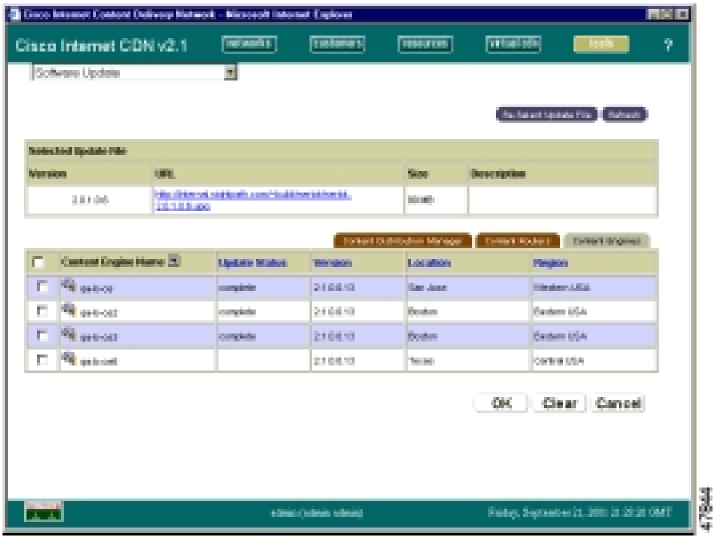
The Software Update page shows the current version of Cisco Internet CDN Software that you are using.

To determine the current Cisco Internet CDN Software version:

Step 1 From the Cisco Internet CDN Software user interface, click **tools**.

Step 2 From the drop-down list, choose **Software Update**. The Software Update page appears. (See Figure 4-7.)

Figure 4-7 Software Update Page



Selected Update File

Version	URL	Size	Description
2.0.1.06	[illegible]	[illegible]	

□	Content Engine Name	Update Status	Version	Location	Region
□	qa-b-ce	complete	2.1.0.8.13	San Jose	Western USA
□	qa-b-ce2	complete	2.1.0.8.13	Boston	Eastern USA
□	qa-b-ce3	complete	2.1.0.8.13	Boston	Eastern USA
□	qa-b-ce4		2.1.0.8.13	Texas	Central USA

Step 3 Click the tab corresponding to the type of device for which you wish to check the software version. The screen refreshes, listing the selected type of devices on your CDN.

Step 4 Locate the device and refer to the Version column for the device, where the number of the software version being used by the device is displayed.

Note The Version column is not updated until a software update has been successfully completed. If a software update is in progress, the Version column displays the base version, not the update version number.

Adding a New Update File

Before you can update your Cisco Internet CDN Software, you must first acquire the appropriate software update file from Cisco.

In order to acquire the software update from Cisco, you must first:

- Access the Cisco.com website and locate the software update files.
- Download the software update files to a web server within your own organization or copy the location (URL) for the files (see the "Adding a New Update File Directly from Cisco.com" section on page 4-47).
- Add the update to the CDN by copying the URL for the update files (pointing either to your web server or Cisco.com) to the Content Distribution Manager.
- Use the software update feature to import the update file pointed to by the link.

You must have a Cisco.com username and password before attempting to download a software update from Cisco.com. In order to acquire a Cisco.com login, go to http://www.cisco.com and click the **Register** link.

Note You need a service contract number, Cisco.com registration number and verification key, Partner Initiated Customer Access (PICA) registration number and verification key, or packaged service registration number in order to obtain a Cisco.com username and password.

To add an update file for the Cisco Internet CDN Software:

Step 1 Launch your preferred web browser and point it to:

`http://www.cisco.com/pcgi-bin/tablebuild.pl/cdn-sp`

Step 2 If prompted, log in to Cisco.com using your designated username and password.

The Cisco Internet CDN Software download page appears, listing the available software updates for the Cisco Internet CDN Software product.

Note Each software update consists of two files: a binary-format update file (*.upg) and a smaller meta file (*.meta). Both files must be downloaded in order to successfully complete a Cisco Internet CDN Software update.

Step 3 Locate the files you wish to download by referring to the Release column for the proper release version of the software.

Step 4 Click the link for the software update file you wish to download. The order in which you download the update files does not matter. The Software License Agreement page appears.

Step 5 After you have read the license agreement, click the **Yes** link at the bottom of the agreement to go to the software download page.

Step 6 Click the **Site 1 (San Jose, CA)** link. You are prompted to open the file or save it to your local hard drive.

Step 7 Click **Save to file** and then choose a location on your workstation to temporarily store the update file.

Step 8 Post the file you downloaded (*.meta or *.upg) to a designated area on your organization's web server and make note of the URL required to access this file. You will need it later.

Note It is imperative that the upgrade (*.upg) file be placed in the same directory as its corresponding meta file, or in a location that is relative to the location of the meta file.

Step 9 Repeat Step 3 through Step 8 for the other software update file.

Step 10 Launch the Cisco Internet CDN Software Content Distribution Manager and log in using an administrative username and password.

Step 11 Click **tools**.

Step 12 From the drop-down list, choose **Software Update**.

The Software Update page appears listing available software updates. (See Figure 4-7.) If there is currently no update available, a message appears.

Step 13 Click **Add New Update File**.

A page appears with a field for entering the URL of your software update.

Step 14 Paste the URL for the update meta file on your web server into the field provided. For example, a valid URL might look like this:

`http://internal.mysite.com/cdn/`*`internet-CDN-version`*`.meta`

where *internet-CDN-version* is the version number of the software update.

Note Do not attempt to link directly to the UPG file. The relative location of the update file is provided by the meta file.

Step 15 Click **OK**.

The version and URL for the update file appear, for example:

```
1.0.3 http://internal.mysite.com/cdnsw.upg
```

Adding a New Update File Directly from Cisco.com

It is also possible to add a software update to the CDN directly from Cisco.com, rather than posting it on a web server within your organization first.

To add the software update directly from Cisco.com:

Step 1 Launch your preferred web browser and point it to:

```
http://www.cisco.com/pcgi-bin/tablebuild.pl/cdn-sp
```

Step 2 If prompted, log in to Cisco.com using your designated username and password.

The Cisco Internet CDN Software (Cisco CDN Service Provider Software) download page appears, listing the available software updates for the Cisco Internet CDN Software product. Note that each software update consists of two files: a binary-format upgrade file (*.upg) and a smaller meta file (*.meta).

Locate the software update you wish to install by consulting the Release column for the proper release version of the software.

Step 3 Click the link for the meta (*.meta) file. The Software License Agreement page appears.

Step 4 After you have read the license agreement, click the **Yes** link at the bottom of the agreement to go to the software download page.

Step 5 Right-click **Site 1 (San Jose, CA)** and copy the URL by selecting the **Copy Shortcut** (Internet Explorer) or **Copy Link Location** (Netscape) option from the shortcut menu that appears.

Step 6 Point your browser to the address of your Cisco Internet CDN Software Content Distribution Manager and log in using an administrative username and password.

Step 7 Click **tools**.

Step 8 From the drop-down list, choose **Software Update**.

Step 9 The Software Update page appears (see Figure 4-7), listing available software updates. If there is currently no update available, a message appears.

Step 10 Click **Add New Update File**.

A page appears for specifying the URL for the update location.

Step 11 Paste the URL for the update meta file on your web server into the field provided. The URL should begin with:

```
http://www.cisco.com/pcgi-bin/Software/Tablebuild/download.cgi/
```

If the URL does not begin with http://www.cisco.com, return to Step 5 and verify that you copied the link from Site 1 (San Jose, CA).

Step 12 Click **OK**.

The version and URL for the update file appear, for example:

```
1.0.3 http://internal.mysite.com/cdnsw.upg
```

Updating the Software on a Content Engine or Content Router

You can update software on your devices as needed using the software update feature. When upgrading, begin with Content Engines and Content Routers before upgrading the Content Distribution Manager.

The Content Distribution Manager reboots at the conclusion of the upgrade procedure, causing you to temporarily lose contact with the device and the graphical user interface.

Once the Content Distribution Manager has updated its software and rebooted, it may be unable to communicate with devices running different versions of the Cisco Internet CDN Software.

Note Although Version 2.1 of Cisco Internet CDN Software supports CDNs in which some nodes are running earlier (2.0.x) CDN software releases, if you have deployed a failover Content Distribution Manager and supernodes on the same CDN, it is necessary to update the software on all Content Engines in your supernodes so that those supernodes will continue to communicate with the failover Content Distribution Manager.

To update the Cisco Internet CDN Software on your devices, follow these steps:

Step 1 From the Cisco Internet CDN Software user interface, click **tools**.

Step 2 From the drop-down list, choose **Software Update**.

The Software Update page appears. (See Figure 4-7.)

Step 3 If there are multiple updates listed, click the radio button next to the available update file you want to use. Otherwise, proceed to the next step.

Step 4 Click the tab corresponding to the type of device that you want to upgrade, for example, **Content Routers**. The window refreshes, listing the devices of the selected type on your CDN.

Note Always update Content Engines and Content Routers before the associated Content Distribution Manager.

Step 5 Refer to the column labeled Version to verify that the devices you are choosing are not already running the version you wish to upgrade to, or that the current version has an upgrade path to the version that you will upgrade to.

Note If you have questions regarding upgrade paths, contact Cisco Technical Support.

Step 6 Check the check boxes next to the name of the device you will be upgrading, or check the box in the column header to choose all devices.

Step 7 Click **OK**. The selected devices begin the update process and go offline temporarily.

Step 8 Repeat Step 4 through Step 7 for each device that you wish to upgrade.

Step 9 Click the **Refresh** button to see the status of your upgrade. When devices come back online, they will be recognized by the Content Distribution Manager.

Step 10 For information on the status of software updates on devices across your CDN, see the "Viewing System Event Logs" section on page 4-64.

Your CDN is now restored, and you are ready to begin serving user requests using the updated Cisco Internet CDN Software.

Updating the Software on a Warm Standby Content Distribution Manager

Unlike other CDN devices, a warm standby Content Distribution Manager must be upgraded manually using the command-line interface. Before upgrading the warm standby Content Distribution Manager, you must have first acquired the Cisco Internet CDN Software upgrade file from Cisco.com. See the "Adding a New Update File" section on page 4-45 for information on downloading a software update.

To update the Cisco Internet CDN Software on a warm standby Content Distribution Manager:

Step 1 Log in to the warm standby device using the admin account and password.

Step 2 At the prompt, enter **enable** to enable the administrative mode.

```
> enable
```

The prompt changes to a pound sign (#) to indicate that you are in administrative mode.

Step 3 Enter **ftp** to launch the file transfer application.

The prompt changes to indicate that you are in FTP mode.

Step 4 Enter the **open** command followed by the DNS name or IP address of the host machine containing the software upgrade package, for example:

```
ftp> open 10.89.11.1
```

You may need to log in separately to the host machine.

Step 5 Enter **bin** to switch to binary transfer mode.

Step 6 Enter the **cd** command followed by the remote path of the upgrade file, for example:

```
ftp> cd /upgrade
```

The directory changes to the location that you specified.

Step 7 Enter the **get** command followed by the name of the upgrade file, MERLOT.upg:

```
ftp> get MERLOT.upg
```

Step 8 Enter the **quit** command to close the file transfer application.

Step 9 Enter **upgrade swupgrade** to initiate the software update on the warm standby Content Distribution Manager:

```
# upgrade swupgrade
```

The warm standby Content Distribution Manager automatically restarts following the software update.

Updating the Software on a Content Services Switch

Each software update file contains an updated Content Services Switch (CSS) configuration script that provides your Content Services Switch with network configuration information such as IP address, gateway address, uplink address, and VLAN information if you are deploying VLANs.

Periodically this script is updated along with Cisco Internet CDN Software, providing new configuration options for your Content Services Switches.

Using the Content Distribution Manager user interface, you can upload the CSS configuration script from the Content Distribution Manager to any Content Services Switch on your CDN. This saves you the trouble of having to manually upload the CSS script to the Content Services Switch, a process that is detailed in the “Preparing the Content Services Switch and Uploading the Script” section in Chapter 3 of the *Cisco Internet CDN Software Configuration Guide*.

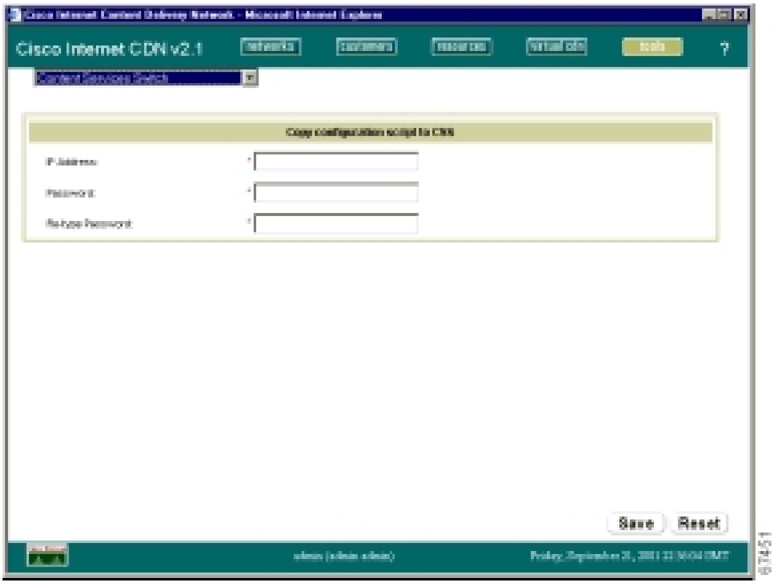
Once you have uploaded the configuration script to a Content Services Switch, refer to the “Configuring the Content Services Switch” section in Chapter 3 of the *Cisco Internet CDN Software Configuration Guide*.

To upload an updated configuration script to a Content Services Switch:

Step 1 From the Cisco Internet CDN Software user interface, click **tools**.

Step 2 From the drop-down list, choose **Content Services Switch**. The Content Services Switch page appears. (See Figure 4-8.)

Figure 4-8 Content Services Switch



Step 3 In the IP Address field, enter the network address of the Content Services Switch to which you wish to upload the updated configuration script.

Step 4 In the Password field, enter the *admin* account password.

Step 5 In the Re-type Password field, reenter the admin account password.

Step 6 Click the **Save** button to initiate transfer of the configuration script to the Content Services Switch you specified.

Step 7 Repeat Step 2 through Step 6 for each Content Services Switch to which you wish to upload the updated script.

Canceling a Software Update

You can cancel a software update before it has begun using the software update feature.

Canceling a software update removes the update software request from the Content Distribution Manager.

If a device has already received the update request and started the software update, that update process will continue regardless of the cancellation request. Once the device has completed the software update, it will report its status to the Content Distribution Manager as if no cancellation request had been issued.

Contact Cisco Technical Support for instructions on restoring an earlier version of the Cisco Internet CDN Software on a CDN device.

To cancel a software update:

Step 1 From the Cisco Internet CDN Software user interface, click **tools**.

Step 2 From the drop-down list, choose **Software Update**. The Software Update page appears. (See Figure 4-7.)

Step 3 Click the tab corresponding to the type of device for which you wish to cancel the software update. The screen refreshes, listing the selected type of devices on your CDN.

Step 4 Locate the device or devices for which the software update is scheduled. These have an update status of *pending*.

Step 5 Check the check box next to the device or devices on which you wish to cancel the software update.

Step 6 Click the **Clear** button. You are prompted to confirm your decision to cancel the software update.

Step 7 Click **OK** to proceed or **Cancel** to terminate the clear software update request and resume the software update on the selected devices.

Step 8 Repeat Step 3 through Step 7 for each type of device (Content Router, Content Engines, or Content Distribution Manager) on which you wish to cancel a software update.

Deleting an Update File

To delete a Cisco Internet CDN Software update file, follow these steps:

Step 1 On the Software Update page (see Figure 4-7), if there are multiple updates to choose from, click the button next to the update file that you want to delete. Otherwise, proceed to the next step.

Step 2 Click **Delete Update File**. You are prompted to confirm your decision to delete the software update file.

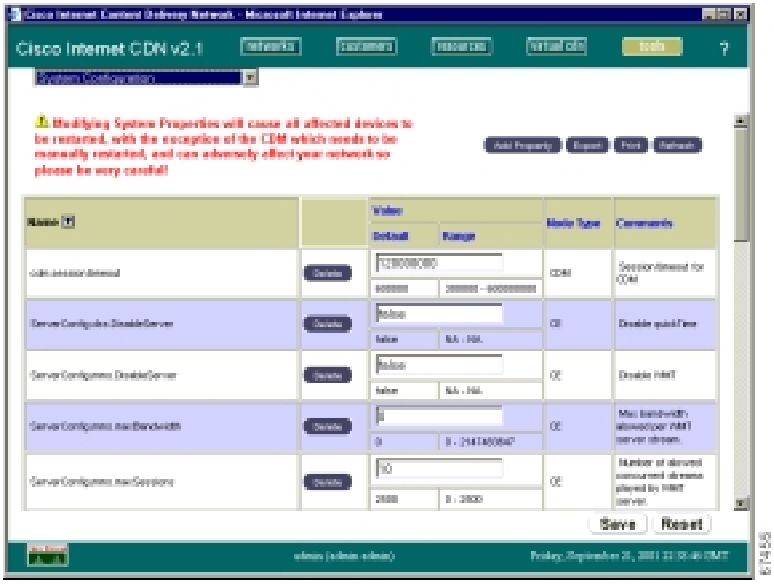
Step 3 Click **OK**. You are returned to the Software Update page with the selected software update removed from the CDN.

Modifying System Properties

You may need to modify one or more of the configuration settings used by a device, or even by your entire CDN—disabling a playserver, for example, or changing one of the runtime settings used by a particular server or device.

Using the System Configuration page (see Figure 4-9), available from the Tools area of the Content Distribution Manager user interface, you can modify a wide variety of system properties.

Figure 4-9 System Configuration



Modifying System Properties will cause all affected devices to be restarted, with the exception of the CDM which needs to be manually restarted, and can adversely affect your network so please be very careful!

Name		Value		Node Type	Comments
		Default	Range		
cdm.session.timeout	Delete	1230000000 600000	300000 - 600000000	CDM	Session timeout for CDM
ServerConfig.qtss.DisableServer	Delete	false false	NA - NA	CE	Disable quickTime
ServerConfig.wms.DisableServer	Delete	false false	NA - NA	CE	Disable WMT
ServerConfig.wms.maxBandwidth	Delete	0 0	0 - 2147483647	CE	Max bandwidth allowed per WMT server stream.
ServerConfig.wms.maxSessions	Delete	10 2000	0 - 2000	CE	Number of allowed concurrent streams played by WMT server.

Changes made using the System Configuration page cause any CDN devices affected by those changes to restart once the change has been saved. Depending on the number and location of affected devices that restart, you may experience a temporary interruption in your CDN after using the System Configuration page, as affected devices restart to integrate configuration changes.

Note Modifying system properties using the System Configuration page can adversely affect your network. Use the System Configuration page only under the direct supervision of a Cisco Technical Assistance Center representative.

Modifying the System Timeout Value

Access to the Content Distribution Manager web interface is secured, in part, using an automatic timeout feature that terminates open connections to the Content Distribution Manager after a set period of inactivity.

The Content Distribution Manager resets its timeout counter each time the Content Distribution Manager web interface is refreshed—following a save or cancel operation or the transition to a new screen.

Using the system configuration feature, available from the Tools area of the Content Distribution Manager, you can modify the length of time that the Content Distribution Manager will wait before terminating idle sessions.

To modify the Content Distribution Manager session timeout:

Step 1 From the Cisco Internet CDN Software user interface, click **tools**.

Step 2 From the System Tools drop-down list, choose **System Configuration**.

The System Configuration page appears. (See Figure 4-9.)

Step 3 Locate the cdm.session.timeout option.

Step 4 In the field provided, set the timeout value in milliseconds. For example, if you want the Content Distribution Manager to terminate sessions that are idle for more than 10 minutes, you would enter the following value in the CDN Session Timeout field:

```
600000000
```

Step 5 Click **Save**. The screen refreshes, displaying the new timeout value in the box beneath the cdm.session.timeout option.

Enabling and Disabling Telnet

The Cisco Internet CDN includes both SSH and Telnet software, which allow administrators to connect and issue commands to CDN devices remotely. The ability to remotely connect to your CDN devices is an integral part of maintenance and troubleshooting activities.

Because the information sent back and forth to CDN devices using SSH is encrypted, we recommend using SSH for all remote interaction with CDN devices.

If your organization does not use SSH or an SSH client is unavailable, you can use Telnet to communicate with your CDN devices. By default, all Cisco Internet CDN Version 2.1 devices have Telnet disabled.

To enable or disable Telnet on a CDN device:

Step 1 From the Cisco Internet CDN Software user interface, click **tools**.

Step 2 From the System Tools drop-down list, choose **Simple Peek**.

Step 3 Click the tab corresponding to the type of device for which you wish to enable Telnet.

Step 4 From the list of devices that appears, click the icon next to the name of the device you wish to edit.

Step 5 If you are prompted, click **Yes** to proceed and then enter your administrative login information a second time. A second browser window opens with the System Tools dialog box displayed.

Step 6 From the Features drop-down list, choose **Enable Telnet** or **Disable Telnet**, and then click **Go**. A message is displayed, indicating that the Telnet feature has been enabled or disabled.

Step 7 Close the System Tools dialog box and return to the Simple Peek page.

Step 8 Repeat Step 3 through Step 7 for each device on which you wish to enable or disable Telnet.

Setting the Maximum Cachable Object Size

Using the system configuration feature, you can adjust the maximum size of content items that can be cached by SQuID, the UNIX-based program that Cisco Internet CDN Software uses to store content on a proxy server close to requesting clients on the CDN.

By default, Cisco Internet CDN Software sets the maximum size of objects to 512000 kilobytes. However, it is possible to set the maximum cache size lower than this.

To modify the maximum cachable object size:

Step 1 From the Cisco Internet CDN Software user interface, click **tools**.

Step 2 From the drop-down list, choose **System Configuration**.

The System Configuration page appears, listing the system configuration properties that have been added for your CDN.

Step 3 Click the **Add Property** button. The Modify Properties page appears.

Step 4 Click the **Catalogs** tab. A list of CDN properties appears.

Step 5 Click the button next to the ServerConfig.squid.maxCacheableObjSize property. You can only add one system configuration property at a time.

Step 6 Click the **Add** button. The Modify Properties page refreshes, listing the name of the property in the Name field.

Step 7 In the Value field, enter a maximum object size, in kilobytes. The acceptable size range is between 4096 and 512000 kilobytes.

Step 8 Click the **CE** check box, indicating that this configuration option should be applied only to the Content Engines (CEs) on your CDN.

Note Applying a configuration option to a device that does not use that option does not affect the performance of the affected device—unusable configuration options are ignored.

Step 9 Click **Save**. You are prompted to confirm your decision to add the new configuration property to the CDN.

Step 10 Click **OK**. You are returned to the System Configuration page. The new configuration option is added to the bottom of the list of configuration options.

Setting System Message Log Parameters

Using the system configuration feature, you can adjust the operating parameters for the system message log, which records a range of CDN events. These parameters include:

- Maximum number of records stored in the system message log

- Maximum number of days to retain system message log records

By default, Cisco Internet CDN Software sets the maximum number of records retained in the system message log to 10000 and the maximum number of days records are retained to 180.

Modifying the system message log parameters can affect the size of the log itself, which has a bearing both on the amount of historical data stored in the log and on the amount of system resources required to maintain the log. In general, smaller log files require fewer system resources to maintain.

You can add only one system configuration property at a time.

To modify the system message log parameters:

Step 1 From the Cisco Internet CDN Software user interface, click **tools**.

Step 2 From the drop-down list, choose **System Configuration**.

The System Configuration page appears, listing the system configuration properties that have been added for your CDN.

Step 3 Click the **Add Property** button. The Modify Properties page appears.

Step 4 Click the **Catalogs** tab. A list of CDN properties appears.

Step 5 Do one of the following:

- To modify the maximum number of records allowed in the system message log, click the button next to the SysMessageLog.count property.
- To modify the maximum duration of records in the system message log, click the button next to the SysMessageLog.days property.

Step 6 Click the **Add** button. The Modify Properties page refreshes, listing the name of the property in the Name field.

Step 7 In the Value field, enter a value for the property as follows:

- For the SysMessageLog.count property, valid entries are between 0 and 65535 records.
- For the SysMessageLog.days property, valid entries are between 0 and 65535 days.

Step 8 Click the **CDM** check box, indicating that this configuration option should be applied only to the Content Distribution Manager.

Note Applying a configuration option to a device that does not use that option does not affect the performance of the affected node—unusable configuration options are ignored.

Step 9 Click **Save**. You are prompted to confirm your decision to add the new configuration property to the CDN.

Step 10 Click **OK**. You are returned to the System Configuration page. The new configuration option is added to the bottom of the list of configuration options.

Step 11 If necessary, repeat Step 4 through Step 10 for the next system log property you wish to modify.

Customizing the Network Time Protocol Server List

Cisco Internet CDN Software uses Network Time Protocol (NTP) to coordinate the computer clock time among CDN devices on your network. Your Content Distribution Manager is shipped with NTP client software installed, and periodically consults a default list of public servers that track the current Coordinated Universal Time (UTC). All CDN devices synchronize their own clock time based on the UTC reported by the NTP client on the Content Distribution Manager.

Using the NTP server option, you can customize the list of public servers consulted by the NTP client.

Note Enabling the NTP option will automatically overwrite the list of default public servers. Once you have enabled the NTP option, you must supply your own public servers to the Content Distribution Manager.

To customize the NTP server list:

Step 1 From the Cisco Internet CDN Software user interface, click **tools**.

Step 2 From the drop-down list, choose **System Configuration**.

The System Configuration page appears, listing the system configuration properties that have been added for your CDN. (See Figure 4-9.)

Step 3 Click the **Add Property** button. The Modify Properties page appears.

Step 4 Click the **Catalogs** tab. A list of CDN properties appears.

Step 5 Click the **NtpServer** option.

Step 6 Click the **Add** button. The Modify Properties page refreshes, listing the name of the property in the Name field.

Step 7 Click the **CDM** check box, indicating that this configuration option should be applied only to the Content Distribution Manager.

Note Applying a configuration option to a device that does not use that option does not affect the performance of the affected device—unusable configuration options are ignored.

Step 8 In the Name field, enter the URLs of the public or private NTP servers you want the Content Distribution Manager to reference, separated by commas, for example:

```
tick.usno.navy.mil,ntp.nasa.gov,time.nist.gov
```

Step 9 Click **Save**. You are prompted to confirm your decision to add the new configuration property to the CDN.

Step 10 Click **OK**. You are returned to the System Configuration page. The new configuration option is added to the list of configuration options.

Deleting a Configuration Property

Using the system configuration feature, available from the Tools area of the Content Distribution Manager, you can remove system configuration properties.

Note Removing system configuration properties may temporarily disrupt your CDN. Contact the Cisco Technical Assistance Center before attempting to remove any system configuration property.

To remove a system configuration property:

Step 1 From the Cisco Internet CDN Software user interface, click **tools**.

Step 2 From the drop-down list, choose **System Configuration**.

The System Configuration page appears, listing the system configuration properties that have been added for your CDN.

Step 3 Locate the system configuration option that you wish to delete.

Step 4 Click the **Delete** button. You are asked to confirm your decision to remove this configuration option.

Step 5 Click **OK**.

The system configuration property is removed. The System Configuration page refreshes.

Troubleshooting

The following sections provide information on the wide range of troubleshooting tools accessible from the Content Distribution Manager user interface.

Viewing System Event Logs

Using the system logs feature of the Cisco Internet CDN Content Distribution Manager, you can view information about events that have occurred in your CDNs. The following event logs are accessible from the System Logs page:

- System events—This log captures a variety of administrative messages regarding system activity. For example, if you add a new Content Engine to a CDN, change passwords, stop and restart a Content Router or a Content Engine, or perform a software upgrade, these events are logged in the system events log.

  Note Manifest file error messages generated by the Content Engine during import may take a few moments to appear in the CDN system logs.

- Software update—This log captures information regarding software updates taking place on your CDN. Information about the name and type of device being upgraded, the software version being applied, and the status of the update are all displayed.
- Trace—This log captures the output of the DNS trace feature on a device. When enabled, the DNS trace feature instructs all Content Engines and Content Routers on a hosted domain to log DNS requests and replies for the hosted domain, and to log the messages on the Content Distribution Manager. See the "Enabling and Disabling DNS Trace" section on page 4-70 for more information.

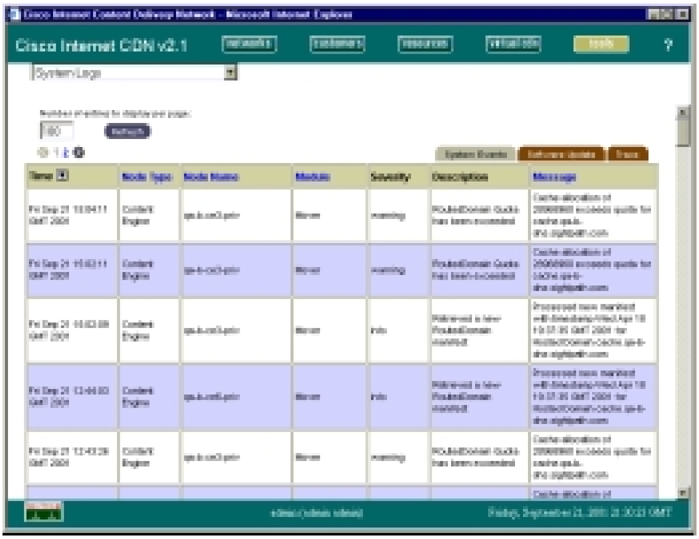
To view logged information for your CDN, follow these steps:

Step 1 From the Cisco Internet CDN Software user interface, click **tools**.

Step 2 From the drop-down list, choose **System Logs**.

The System Logs page appears, displaying the system events log by default. (See Figure 4-10.)

Figure 4-10 System Logs (Showing System Events Log)



Time	Node Type	Node Name	Module	Severity	Description	Message
Fri Sep 21 [illegible] GMT 2001	Content Engine	[illegible]	[illegible]	warning	RoutedDomain Quota has been exceeded	Cache allocation of [illegible] exceeds quota for cache [illegible]
Fri Sep 21 [illegible] GMT 2001	Content Engine	[illegible]	[illegible]	warning	RoutedDomain Quota has been exceeded	Cache allocation of [illegible] exceeds quota for cache [illegible]
Fri Sep 21 [illegible] GMT 2001	Content Engine	[illegible]	[illegible]	info	Retrieved a new RoutedDomain manifest	Processed new manifest [illegible]
Fri Sep 21 [illegible] GMT 2001	Content Engine	[illegible]	[illegible]	info	Retrieved a new RoutedDomain manifest	Processed new manifest [illegible]
Fri Sep 21 [illegible] GMT 2001	Content Engine	[illegible]	[illegible]	warning	RoutedDomain Quota has been exceeded	Cache allocation of [illegible] exceeds quota for cache [illegible]

Step 3 If you wish to view system events messages, proceed to the next step; otherwise, click the tab corresponding to the log you wish to view: **Software Update** or **Trace**.

Step 4 Click the appropriate header to sort the messages by the appropriate identifying information. By default, messages are listed chronologically. You can also sort the system log messages by node type, node name, module, severity, or message text. (See Figure 4-10.)

Note If no name is available for a node, the name displayed is “Unavailable.” This might occur if the node has been deleted or has been reregistered with Cisco Internet CDN Software.

Step 5 If you have many event messages, you may need to view multiple pages to view the activity that you are interested in. Click the forward (>) and back (<) buttons to move between pages. Alternatively, click the link for a specific page to jump to that page.

Note You can increase the number of records displayed per page using the field provided on the System Logs page, and click **Refresh**.

Changing the Warm Standby Content Distribution Manager Role

A warm standby Content Distribution Manager is a failover device that can quickly be moved to replace the primary Content Distribution Manager if that device unexpectedly fails or goes offline. The warm Standby Content Distribution Manager allows you to continue managing the CDN.

The warm standby Content Distribution Manager is kept online in anticipation of a failure by the primary Content Distribution Manager, and maintains a separate policy database which is periodically synchronized with that of the primary Content Distribution Manager so that both devices have an identical list of CDN transactions at the time of failure.

For information on activating a warm standby Content Distribution Manager, see the "Activating the Warm Standby Content Distribution Manager" section on page 2-30.

If the primary Content Distribution Manager suddenly goes offline, Content Engines and Content Routers continue to serve content requests but immediately attempt to contact another active Content Distribution Manager by reviewing a local list of IP addresses for warm standby devices.

Once the role of the warm standby Content Distribution Manager has been changed using the procedure below, it becomes the primary Content Distribution Manager; Content Engines and Content Routers begin using the device as the primary Content Distribution Manager. The warm standby Content Distribution Manager, now the primary Content Distribution Manager, processes CDN transactions using its own database, and send updates to Content Engines and Content Routers.

To activate a warm standby Content Distribution Manager following the failure of your primary Content Distribution Manager:

Step 1 Access the command-line interface of your current primary Content Distribution Manager, which will be referred to as CDM1 in these instructions for the purposes of clarity.

Step 2 If it is still responding, deactivate CDM1 using the **standbycdm** command. For example:

```
Host# standbycdm change-role-standby
```

This designates CDM1 as a warm standby Content Distribution Manager.

Step 3 Close any open web browser windows that were used to access CDM1.

Step 4 Access the CLI of your current warm standby Content Distribution Manager, which will be referred to as CDM2 in these instructions for the purposes of clarity.

Step 5 Activate CDM2 using the **standbycdm** command. For example:

```
Host# standbycdm change-role-primary
```

This designates CDM2 as the primary Content Distribution Manager.

Step 6 Launch your preferred web browser and point it to CDM2.

Step 7 Log on to the graphical user interface for CDM2 and verify that you can see the Content Engines and Content Routers on your CDN. These devices will begin to contact CDM2, the new primary Content Distribution Manager.

Note It may take up to 10 minutes for devices to establish contact with the warm standby Content Distribution Manager, during which time the devices appears on the user interface with a status of *pending*.

Once the devices have successfully contacted the CDM, their status changes to *online*.

For more information on using the **standbycdm** command, refer to the *Cisco Internet CDN Software Command Reference*.

Enabling and Disabling the Debug Logging Option

The Cisco Internet CDN allows administrators to enable or disable debug logging for Cisco Internet CDN devices using the Content Distribution Manager user interface. When enabled, debug logging records a range of events in the Cisco Internet CDN Software log file, *merlot.log*, that would otherwise be omitted.

With the additional logged information provided by debug logging, CDN administrators, working with the Cisco Technical Assistance Center, can more quickly isolate and resolve problems with Cisco Internet CDN devices.

Enabling Debug Logging on Internet CDN Devices

To enable debug logging on an Internet CDN device:

Step 1 From the Cisco Internet CDN Software user interface, click **tools**.

Step 2 From the System Tools drop-down list, choose **Simple Peek**. The Simple Peek page appears.

Step 3 Click the tab corresponding to the type of device on which you wish to enable debug logging.

Step 4 From the list of devices that appears, click the icon next to the name of the device on which you wish to enable debug logging.

- **a.** A message may appear regarding the security certificate being passed to your client. Click **Yes** to continue.
- **b.** You may be asked to log in a second time using your administrative login and password information. If so, enter the appropriate information in the fields provided, and click **OK**.

A second browser window opens with the System Tools page displayed.

Step 5 From the drop-down list, choose the **Enable Debugging** option, and then click **Go**. A message is displayed indicating that the debugging feature has been enabled.

Step 6 Close the System Tools dialog box.

Step 7 Repeat Step 3 through Step 6 for each device on which you wish to enable debug logging.

Disabling Debug Logging on Internet CDN Devices

To disable debug logging on an Internet CDN device:

Step 1 Follow Step 1 through Step 4 in the "Enabling Debug Logging on Internet CDN Devices" section on page 4-68.

Step 2 From the drop-down list, choose **Disable Debugging**, and then click **Go**. A message indicating that the debugging feature has been disabled is displayed.

Step 3 Close the System Tools dialog box.

Step 4 Repeat these steps for each device on which you wish to disable debug logging.

Generating a Debug File Package

Cisco Internet CDN Software enables users or administrators to generate a tape archive (or "tar" file) containing configuration and log files that can help troubleshoot problems that may be occurring on a CDN device.

Debug file packages are generated as TGZ-format archives on the device that is experiencing problems. They are then downloaded to the local drive of the CDN user or administrator's workstation. Debug packages can be unpacked using any archive program, such as WinZip for the Windows operating system.

To generate a debug file package for an Internet CDN device:

Step 1 From the Cisco Internet CDN Software user interface, click **tools**.

Step 2 From the System Tools drop-down list, choose **Simple Peek**.

Step 3 Click the tab corresponding to the type of device for which you wish to generate a debug file package.

Step 4 From the list of devices that appears, click the icon next to the name of the device that you wish to use to generate a debug file package.

- **a.** A message may appear regarding the security certificate being passed to your client. Click **Yes** to continue.
- **b.** You may be asked to log in a second time using your administrative login and password information. If so, enter the appropriate information in the fields provided, and click **OK**.

A second browser window opens with the System Tools dialog displayed.

Step 5 From the drop-down list, choose **Create Debug Package** and then click **Go** to generate a debug file package for the selected device. A message is displayed, indicating that the debug file package is being generated.

Note It may take several minutes for the debug file package to be generated. Be patient.

Step 6 Click the link provided to download the debug file package from the remote device. You are prompted to choose a location on your local hard drive for the downloaded debug tar file (TGZ file extension).

Step 7 Use the dialog box to choose a directory on your workstation to hold the tar file, and then click **OK** to generate the tar file and deposit it on your local hard drive.

Step 8 Close the System Tools dialog box and return to the Simple Peek page on the Content Distribution Manager.

Step 9 Repeat Step 3 through Step 8 for each device for which you wish to generate a debug file package.

Step 10 Using Winzip or another file decompression application capable of handling TGZ files, decompress the debug file package and view its contents.

Enabling and Disabling DNS Trace

Use the DNS trace feature to help troubleshoot routing problems that may arise with your hosted domain. When enabled, the DNS trace feature instructs all Content Engines and Content Routers on a hosted domain to log DNS requests and replies for the hosted domain, and to log these messages on the Content Distribution Manager. Administrators can access the DNS trace logs through the System Logs feature.

To enable DNS trace:

Step 1 From the Cisco Internet CDN Software user interface, click **resources**.

Step 2 From the drop-down list, choose **Hosted Domains**.

The View Hosted Domains page appears. (See Figure 2-16.)

Step 3 Click the edit icon next to the name of the hosted domain that you wish to edit. The browser window refreshes, displaying fields for editing the selected hosted domain.

Step 4 In the Enable DNS Trace field, enter the number of minutes that you want to log DNS request and reply messages. DNS trace can be enabled for up to 99 minutes.

Step 5 Click **Save**.

Accessing Logged DNS Trace Information

Once DNS trace has been enabled, you will want to access the information recorded by the feature.

To access logged DNS information:

Step 1 From the Cisco Internet CDN Software user interface, click **tools**.

Step 2 From the drop-down list, choose **System Logs**.

The System Logs page appears. (See Figure 4-10.)

Step 3 Click the **DNS Trace** link. The browser window refreshes, displaying a list of messages logged for the hosted domain while DNS trace was enabled.

Note If you are viewing the log while the DNS trace feature is activated, you can update the list of logged messages by clicking **Refresh**.

Mapping Out Failed or Damaged Content Engine Drives

If one or more *nonsystem* drives on a Content Engine have failed, the device should continue to function. However, replacing or repairing the damaged drive is critical.

A diagnostic script called *cache-repair* identifies Content Engines with failed drives for the Content Distribution Manager, and provides tools that you can use to bring these Content Engines back online.

If you have a Content Engine with a damaged or failed drive, contact Cisco Technical Support for instructions on using the cache-repair script to repair the drive. See the "Obtaining Technical Assistance" section on page xix for instructions on contacting the Cisco Technical Assistance Center.

Recovering from Catastrophic Failure

If any of your CDN devices fail as a result of a catastrophic event (for example, power failure or power surge, media failure, and so on), the affected device attempts to restart itself as soon as its operating environment is restored.

CDN devices continue to try to recover until they are successful. If the device is unable to restart, it automatically reboots itself at 30-minute intervals until the restart operation succeeds.

Error and Event Messages

This appendix describes error messages that may appear when you use 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, Content Engines, Content Routers, or Content Services Switch when they attempt 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.

This chapter contains the following sections:

- User Interface Errors, page A-1
- System Log Event Messages, page A-3
- System Log Error Messages, page A-6
- Content Authentication Errors, page A-10

User Interface Errors

The Cisco Internet CDN Software user interface enforces the integrity of CDN data through the use of required fields and data type verification. When errors are produced as a result of user interaction with the user interface, visual and text indicators provide users with information to help them resolve the problem.

See the “Content Distribution Manager Icons” section on page 1-23 for descriptions of the various visual icons used to indicate problems with CDN data.

Common causes of user interface errors are:

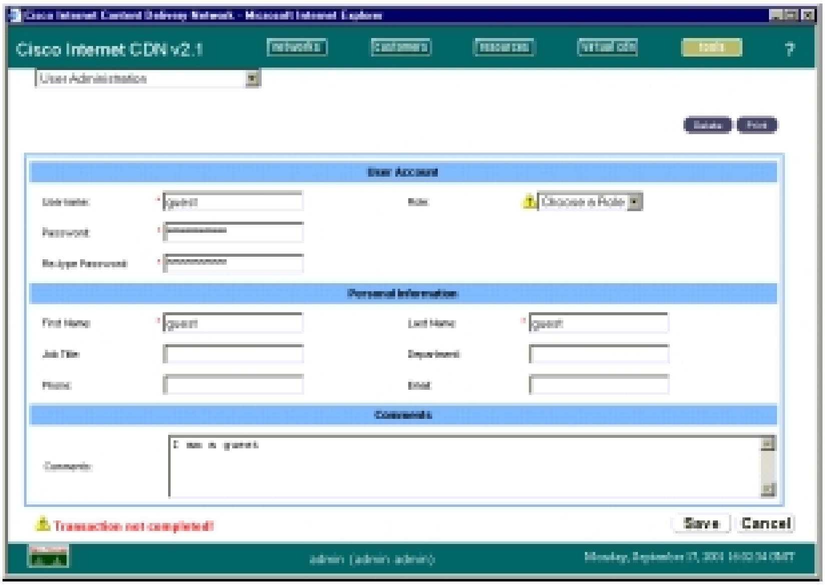
- Required field(s) left blank—Look for the required field indicator (*) and make sure that the field is filled in completely.
- Field(s) contains invalid data—Make sure that fields requiring numbers do not contain text, that dates are entered in the correct format, that valid dates or date ranges are used, and that drop-down lists are not set to default values.

To view error text generated by the user interface:

Step 1 From the Cisco Internet CDN Software user interface, locate the error symbol. This icon appears next to each field that generated an error.

For example, in Figure A-1, the Role field is displaying an error symbol.

Figure A-1 User Interface Showing User Interface Errors



User Name: * guest
Password: * **********
Re-type Password: * **********
Role: ⚠ Choose a Role
First Name: * guest
Last Name: * guest
Job Title:
Department:
Phone:
Email:
Comments: I am a guest

⚠ Transaction not completed!

admin (admin admin)

Monday, September 17, 2001 16:02:34 GMT

Step 2 Move your cursor over the error symbol. A message explaining the error appears above the cursor in a "tool tip" style popup.

Additional error information appears in red lettering near the footer area of the page.

Step 3 Address each field displaying an error symbol and correct any formatting errors before attempting to resubmit your data to the CDN.

System Log Event Messages

```
Changed the HTTP password
```

Explanation The HTTP password for a device has been changed. The HTTP password allows administrators to secure access to configuration information for selected devices from the Content Distribution Manager. This password can be changed from the modify screen for a Content Engine or Content Router.

Action No action is required.

```
Changed the root password
```

Explanation The root password allows administrators to overwrite the root account password and gain direct, command-line access to the device. This password can be changed from the modify screen for a Content Engine or Content Router.

Action No action is required.

```
DNS trace message for some rds
```

Explanation Identifies a DNS trace message for the named hosted domain.

Action No action is required. See the "Enabling and Disabling DNS Trace" section on page 4-70 for more information on the DNS trace feature.

```
Passed store invalidation
```

Explanation The Content Distribution Manager was able to successfully review damaged records on the Oracle policy database and mark them invalid. Invalid database records are not loaded with the rest of the Oracle database.

Action Using the store–invalidation tool enables you to quickly bring your policy database (and thus your Content Distribution Manager) online even when errors are encountered during validation. However, you should still attempt to repair any damaged database records. Review the text of the invalidation messages and attempt to resolve damaged records on your Oracle policy database.

```
Passed store validation
```

Explanation The Content Distribution Manager's check of the Oracle policy database was completed successfully, without finding any database errors.

Action No action is required.

```
Registered a new Content Engine
```

Explanation A new Content Engine has registered itself with the Content Distribution Manager.

Action Once a new Content Engine is registered, it must be activated from the Content Distribution Manager before content is routed to the new device. See the "Activating and Defining a Content Engine" section on page 2-36 for instructions on activating the new Content Engine.

```
Registered a new Content Router
```

Explanation A new Content Router has registered itself with the Content Distribution Manager.

Action Once a new Content Router is registered, it must be activated from the Content Distribution Manager before it is added to the CDN and begins routing requests. See the "Activating and Defining a Content Router" section on page 2-33 for instructions on activating the new Content Router.

```
Server is shutting down
```

Explanation The named device is in the process of shutting down. Shutdown can be initiated from the command-line interface or from the Content Distribution Manager.

Action No action is required. See the "Stopping, Shutting Down, Restarting, and Rebooting a Content Engine" section on page 3-14 or the "Stopping, Shutting Down, Restarting, and Rebooting a Content Router" section on page 3-23 for more information.

```
Server Started
```

Explanation The named device is in the process of restarting. Restart operations can be initiated from the command-line interface or remotely from the Content Distribution Manager.

Action No action is required. See the "Stopping, Shutting Down, Restarting, and Rebooting a Content Engine" section on page 3-14 or "Stopping, Shutting Down, Restarting, and Rebooting a Content Router" section on page 3-23 for more information.

```
Started store invalidation
```

Explanation An administrator has logged on to the Content Distribution Manager and launched the store–invalidation tool. This tool locates records marked *damaged* by the store–validation tool and marks them *invalid*, enabling the Content Distribution Manager to ignore them when loading the policy database.

Action No action is required. The results of the store–invalidation tool review of your policy database—a list of records that have been marked *invalid* and will not be loaded by the CDN software—are written to the validation.log file, which is stored in the /state directory on the Content Distribution Manager.

```
Started store validation
```

Explanation An administrator has logged on to the Content Distribution Manager and launched the store–validation tool. This tool checks the Oracle policy database for damaged records or internal inconsistencies and outputs its result in a log file, validation.log, located in the /state directory on the Content Distribution Manager.

Action When the tool has completed its review of the Oracle policy database, review the validation.log file and determine whether or not damaged records were located. If damaged records exist, run the store–invalidation tool on the Content Distribution Manager to mark those records *invalid* and enable the Content Distribution Manager to come online.

System Log Error Messages

```
Current operation causes assigned Hosted Domains to no longer
have a valid Root Location. Please check Hosted Domain to cluster
assignments.
```

Explanation You are attempting to remove the node (supernode, standalone Content Engine, or Content Engine cluster) from the root location of a hosted domain. When a location is selected as the root location for a hosted domain, it must maintain a minimum of one node.

Action Change the root location for the hosted domain, or assign other nodes from the root location to the hosted domain and then try again to delete or relocate the Content Engine, supernode, or cluster. See the "Modifying Hosted Domains" section on page 3-36 for instructions on adding Content Engines to a hosted domain, the "Modifying a Supernode" section on page 3-25 or the "Modifying a Cluster" section on page 3-30 for instructions on adding Content Engines to a supernode or cluster, or the "Modifying Content Engines" section on page 3-11 for instructions on changing the location of a Content Engine.

```
Error occurred while processing received data
```

Explanation A problem occurred during the loading or processing of cached content. Either the Content Distribution Manager did not pass correct data to the Content Engine or Content Router, or the Content Engine or Content Router did not cache data from the Content Distribution Manager correctly.

Action Reboot the device on which the error was generated. If the problem returns, contact Cisco Technical Support.

```
Error occurred while transferring log file
```

Explanation A log file from the named device could not be transferred to your remote logging server.

Action This could be the result of an interruption in service or insufficient resources on your remote logging server to accommodate the new log file. Verify that your remote logging server is online and that it has sufficient disk space to accommodate the log files being transferred to it. Also, review recent remote logging activity, and verify that confirmation (*.ok) files exist for each log file. See the "Setting Up Remote Logging" section on page 4-31 for more information.

```
Failed configuring a CSS
```

Explanation An attempt to configure or reconfigure a Content Services Switch on your CDN has failed.

Action Review configuration procedures in the *Cisco Internet CDN Software Configuration Guide* and try again to configure your switch. If configuration fails a second time, contact Cisco Technical Support.

```
Failed parsing a RoutedDomain Manifest
```

Explanation The CDN device encountered syntax errors in the manifest file.

Action Use the replication log for the selected device as well as the system events log to find detailed information on the nature of the problem with the manifest file. Then use your preferred ASCII text or XML editor to correct the manifest file syntax. See the "Viewing the Content Replication Log for a Content Engine" section on page 3-45 for information on viewing the replication log for a Content Engine, and "Creating a Manifest File for Importing Media" section on page 2-3 for instructions on the manifest file syntax.

```
Failed store invalidation, review validation log
```

Explanation Damaged records named by the store–validation tool in the validation.log file could not be marked *invalid* by the store–invalidation tool. This means that the Content Distribution Manager will not be able to overlook these damaged records when attempting to come online.

Action Review the validation.log file in the /state directory on the Content Distribution Manager for more information on the records that failed, and then contact Cisco Technical Support.

```
Failed store validation, review validation log
```

Explanation An administrator has logged on to the Content Distribution Manager and launched the store–validation tool, which encountered internal inconsistencies in the Oracle policy database during a routine check following startup. There could be a problem with your policy database.

Action Review the validation.log file in the /state directory on your Content Distribution Manager for a list of the database records that failed the store–validation review. In order to bring your Content Distribution Manager online, log on to the Content Distribution Manager and use the store–invalidation tool to mark the problem database records *invalid*, enabling the Content Distribution Manager to come back online.

```
Failed to retrieve a RoutedDomain manifest
```

Explanation The manifest file for the hosted domain could not be retrieved from the specified location.

Action Correct the manifest file URL so that it points to a valid manifest file. See the "Replicating Content from the Origin Server to a Hosted Domain" section on page 2-59 for instructions on pointing your hosted domain to a valid manifest file.

```
[X] Number of system messages dropped
```

Explanation The device has deleted the reported number of system messages from its log in order to make room for new messages.

Action This occurs when the volume of system messages being logged by the device exceeds the limit set by the CDN. Older messages are deleted to enable the device to accommodate the large number of new messages being added. Review the messages being logged and address the problem that is producing the high volume of logged messages.

```
RoutedDomain Quota has been exceeded
```

Explanation The available disk space on the hosted domain is not adequate to store all the contents named in the manifest file. Some of the contents named by the manifest file will not be pre-positioned.

Action Add more disk space to your hosted domain. After more space is made available, any content that has not been pre-positioned will be replicated. See the "Adding and Removing Content Engines from a Hosted Domain" section on page 3-39 for more information.

```
Store is corrupted
```

Explanation Checks run by the Content Distribution Manager against the Oracle policy database have indicated that the database has been corrupted.

Action Contact Cisco Technical Support immediately for help in resolving this problem.

Content Authentication Errors

If a request for protected content fails using the hosted domain-based SKCA content authentication feature, Content Engines direct user requests to a predetermined web page to display one of five content authentication errors. Those errors are:

```
EXPIRED
```

Explanation The time stamp in the SKCA cookie has expired. This request is no longer valid.

Action The user must generate a new request to the hosted domain using SKCA.

```
BADMAC
```

Explanation The information in the SKCA cookie appears to be altered.

Action The user must generate a new request to the hosted domain using SKCA.

```
BADKEY
```

Explanation There was no key in the secrets file matching the given index in the cookie.

Action The user must generate a new request to the hosted domain using SKCA.

```
BADURL
```

Explanation The requested URL did not match the URL field of the cookie.

Action The user must generate a new request to the hosted domain using SKCA.

```
NOTOKEN
```

Explanation No token was found when accessing a protected URL.

Action The user must generate a new request to the hosted domain using SKCA.

APPENDIX B

Deploying SNMP on Content Delivery Networks

This appendix contains information on deploying SNMP for use with the Cisco CDN product, including detailed information on the CISCO-CONTENT-NETWORK-MIB.

The chapter contains the following sections:

- Defining a Device as an SNMP Agent, page B-1
- CISCO-CONTENT-NETWORK-MIB, page B-2
- Using SNMP to Monitor CDN Devices, page B-14

Defining a Device as an SNMP Agent

Before defining a device as an SNMP agent, you must configure the SNMP manager so that it recognizes the CDN devices.

Refer to your SNMP manager documentation for further information on configuring your SNMP manager.

See the "Adding and Removing SNMP Managers" section on page 4-2 for information on registering your SNMP managers with Cisco Internet CDN Software.

CISCO-CONTENT-NETWORK-MIB

The contents of the CISCO-CONTENT-NETWORK-MIB follow. The end of the MIB is marked END. See the sections that follow for instructions on obtaining an online copy of the MIB from Cisco and on implementing the SNMP traps defined in the MIB.

Note If you have questions regarding the MIB or implementing SNMP on your CDN, e-mail Cisco's content network MIB support desk at content-network-mib@cisco.com, or see the "Obtaining Technical Assistance" section on page xix for instructions on contacting the Cisco Technical Assistance Center.

```
************************************************************

CISCO-CONTENT-NETWORK-MIB.my

Cisco Content Network Management Information Base

Copyright (c) 2001 by Cisco Systems, Inc.

All rights reserved.

************************************************************


CISCO-CONTENT-NETWORK-MIB DEFINITIONS ::= BEGIN


IMPORTS
    MODULE-IDENTITY,
    OBJECT-TYPE,
    NOTIFICATION-TYPE,
    Gauge32
        FROM SNMPv2-SMI
    ZeroBasedCounter32
        FROM RMON2-MIB
    NOTIFICATION-GROUP,
    OBJECT-GROUP,
    MODULE-COMPLIANCE
        FROM SNMPv2-CONF
    ciscoMgmt
        FROM CISCO-SMI;

ciscoContentNetworkMIB MODULE-IDENTITY
    LAST-UPDATED "200109101459Z"
    ORGANIZATION "Cisco Systems, Inc."
    CONTACT-INFO
        "Cisco Systems Customer Service
         Postal: 170 W Tasman Drive
                 San Jose, CA 95134-1706 USA
         Tel: +1 800 553-NETS
         E-mail: content-network-mib@cisco.com"
    DESCRIPTION
"This MIB module defines objects for Content Network devices. A Content
Network is a collection of devices that optimizes the delivery of Internet content
(such as HTML documents and MPEG files) by caching content near clients, by
pushing content into those caches, and by routing each client request to the best
device available at that moment to serve the particular content requested.

Content Network devices include Content Engines (CEs) for serving content,
Content Routers (CRs) for routing client requests, and Content Distribution
Managers (CDMs) for administering the network."

    REVISION     "200109101459Z"
    DESCRIPTION
        "Deprecated:
            ccnNotifServerStart
            ccnNotifServerStop
        Added:
            ccnNotifOffline
            ccnNotifNeedsAttention
            ccnNotifWaitingForCdm
            ccnNotifOnline”

    REVISION    “200105232134Z”
    DESCRIPTION
“Initial version of this MIB module.”
    ::= { ciscoMgmt 216 }

ciscoContentNetworkMIBObjects
    OBJECT IDENTIFIER ::= { ciscoContentNetworkMIB 1 }

—Application groups
ccnReport
    OBJECT IDENTIFIER ::= { ciscoContentNetworkMIBObjects 1 }

-- Categories for the report group.
ccnReportDns      OBJECT IDENTIFIER  ::= { ccnReport 1 }
ccnReportAcct     OBJECT IDENTIFIER  ::= { ccnReport 2 }

—Objects for the ccnReportDns category.
ccnReportDnsRequestRate OBJECT-TYPE
    SYNTAX          Gauge32
    UNITS           “requests-per-second”
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
"Number of DNS requests per second."
    ::= { ccnReportDns 1 }

ccnReportDnsClientCount OBJECT-TYPE
    SYNTAX          ZeroBasedCounter32
    UNITS          "clients"
    MAX-ACCESS       read-only
    STATUS          current
    DESCRIPTION
"Total number of DNS clients that have contacted this device since the DNS
server last started."
    ::= { ccnReportDns 2 }

ccnReportDnsRequests OBJECT-TYPE
    SYNTAX          ZeroBasedCounter32
    UNITS          "requests"
    MAX-ACCESS       read-only
    STATUS          current
    DESCRIPTION
"Total number of DNS requests since the DNS server last started."
    ::= { ccnReportDns 3 }

—Objects for the ccnReportAcct category.
ccnReportAcctBytesServed OBJECT-TYPE
    SYNTAX          ZeroBasedCounter32
    UNITS          "bytes"
    MAX-ACCESS       read-only
    STATUS          current
    DESCRIPTION
"Total number of bytes of content served to clients from this device since the
servers on this device last started."
    ::= { ccnReportAcct 1 }

ccnReportAcctObjectsCached OBJECT-TYPE
    SYNTAX          Gauge32
    UNITS           "objects"
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
"Total number of objects in the content cache."
    ::= { ccnReportAcct 2 }

ccnReportAcctCacheHitRate OBJECT-TYPE
    SYNTAX         Gauge32
    UNITS          "objects-per-minute"
    MAX-ACCESS     read-only
    STATUS         current
    DESCRIPTION
"Number of cache hits per minute."
    ::= { ccnReportAcct 3 }

ccnReportAcctCacheMissRate OBJECT-TYPE
    SYNTAX         Gauge32
    UNITS          "objects-per-minute"
    MAX-ACCESS     read-only
    STATUS         current
```

```
   DESCRIPTION
“Number of cache misses per minute.”
   ::= { ccnReportAcct 4 }

—Notification Events

ciscoContentNetworkMIBNotif
   OBJECT IDENTIFIER ::= { ciscoContentNetworkMIB 2 }

ccnNotifications
   OBJECT IDENTIFIER ::= { ciscoContentNetworkMIBNotif 0 }

ccnNotifServerStart    NOTIFICATION-TYPE
   STATUS          deprecated — See ccnNotifOnline.
   DESCRIPTION
“The servers on this device are being started.”
   ::= { ccnNotifications 1 }

ccnNotifServerStop     NOTIFICATION-TYPE
   STATUS          deprecated — See ccnNotifOffline,
                     -— ccnNotifNeedsAttention, and
                     -— ccnNotifWaitingForCdm.
   DESCRIPTION
“The servers on this device are being stopped.”
   ::= { ccnNotifications 2 }

ccnNotifOffline        NOTIFICATION-TYPE
   STATUS          current
   DESCRIPTION
"The device is about to disconnect from the network."
   ::= { ccnNotifications 3 }


ccnNotifNeedsAttention  NOTIFICATION-TYPE
   STATUS          current
   DESCRIPTION
"The device is on the network, but is unregistered (not associated with any CDN)
or needs some other adjustment that cannot be done through the CDM
administrator interface (such as repairing a disk, completing a software upgrade,
or configuring the CDM database)."
   ::= { ccnNotifications 4 }


ccnNotifWaitingForCdm   NOTIFICATION-TYPE
   STATUS          current
   DESCRIPTION
"The device (CE or CR) is waiting for configuration information from the CDM.
The device is on the network and is either failing to communicate with the CDM
or is being told explicate by the CDM to continue waiting pending activation by
the CDN administrator."
   ::= { ccnNotifications 5 }


ccnNotifOnline          NOTIFICATION-TYPE
   STATUS          current
   DESCRIPTION
"The device is operational and ready to participate in the CDN."
   ::= { ccnNotifications 6 }
```

```
—compliance specification

ccnMIBConformance
   OBJECT IDENTIFIER ::= { ciscoContentNetworkMIB 3 }

ccnMIBCompliances
   OBJECT IDENTIFIER ::= { ccnMIBConformance 1 }

ccnMIBGroups
   OBJECT IDENTIFIER ::= { ccnMIBConformance 2 }

—Conformance
ccnMIBCompliance    MODULE-COMPLIANCE
   STATUS        deprecated —See ccnMIBComplianceRev1.
   DESCRIPTION
"The compliance statement for Cisco Systems entities that implement the Content
Network applications."
   MODULE  — this module
   MANDATORY-GROUPS {
      ccnReportingGroup,
      ccnNotifGroup
   }
   ::= { ccnMIBCompliances 1 }

ccnMIBComplianceRev1    MODULE-COMPLIANCE
   STATUS           current
   DESCRIPTION
"The compliance statement for Cisco Systems entities that implement the Content
Network applications."
```

```
   MODULE  — this module
   MANDATORY-GROUPS {
      ccnReportingGroup,
      ccnNotifGroupRev1
   }
   ::= { ccnMIBCompliances 2 }

—Units of Conformance
ccnReportingGroup  OBJECT-GROUP
   OBJECTS {
      ccnReportDnsRequestRate,
      ccnReportDnsClientCount,
      ccnReportDnsRequests,
      ccnReportAcctBytesServed,
      ccnReportAcctObjectsCached,
      ccnReportAcctCacheHitRate,
      ccnReportAcctCacheMissRate
   }
   STATUS current
   DESCRIPTION
“DNS and Accounting with low capacity Counter32 and Gauge32 objects.”
   ::= { ccnMIBGroups 1 }

ccnNotifGroup  NOTIFICATION-GROUP
   NOTIFICATIONS {
      ccnNotifServerStart,
      ccnNotifServerStop
   }
   STATUS deprecated -- See ccnNotifGroupRev1.
   DESCRIPTION
"Notifications for the Cisco Content Network."
   ::= { ccnMIBGroups 2 }

ccnNotifGroupRev1  NOTIFICATION-GROUP
   NOTIFICATIONS {
      ccnNotifOffline,
      ccnNotifNeedsAttention,
      ccnNotifWaitingForCdm,
      ccnNotifOnline
   }
   STATUS current
   DESCRIPTION
"Notifications for the Cisco Content Network."
   ::= { ccnMIBGroups 3 }

END
```

Obtaining the CISCO-CONTENT-NETWORK-MIB

You can find the definition of the CISCO-CONTENT-NETWORK-MIB at ftp://ftp.cisco.com/pub/mibs/v2/CISCO-CONTENT-NETWORK-MIB.my.

CISCO-CONTENT-NETWORK-MIB Variables

Table B-1 describes variables in the CISCO-NETWORK-MIB.

Table B-1 Variables in the CISCO-NETWORK-MIB

MIB Variable	Device Monitored	Description
ccnReportDnsRequestRate	Content Router	Number of DNS requests per second. The SNMP agent gathers this information at 15-minute intervals.
ccnReportDnsClientCount	Content Route	Total number of DNS clients that have contacted this device since the DNS server last started. To determine when the DNS server last started, check the system logs of the Content Router.
ccnReportDnsRequests	Content Router	Total number of DNS requests since the DNS server last started. This value indicates how much load is being put on Content Engines. To determine when the DNS server last started, check the system logs of the Content Router.
ccnReportAcctBytesServed	Content Engine	Total number of bytes of content served to clients from this device since the servers on this device last started. To determine when the servers last started, check the system logs of the Content Engine.
ccnReportAcctObjectsCached	Content Engine	Total number of files in the Content Engine.

Table B-1 Variables in the CISCO-NETWORK-MIB (continued)

MIB Variable	Device Monitored	Description
ccnReportAcctCacheHitRate	Content Engine	Number of cache hits per minute. The SNMP agent gathers this information at 15-minute intervals.
ccnReportAcctCacheMissRate	Content Engine	Number of cache misses per minute. The SNMP agent gathers this information at 15-minute intervals. Possible reasons for a high rate of cache misses are: • The URLs that the content provider chose for caching may not be cachable. The content is therefore being fetched from the content provider origin server every time it is requested. • The TTL (Time To Live) value of the cached content may be very low. Frequent expirations of content lead to frequent fetches from the origin server. Monitoring the number of cache misses per minute is useful for billing purposes and to ensure that the highest number of requests is served through the CDN and not through the content provider origin server.

CISCO-CONTENT-NETWORK-MIB SNMP Traps

The SNMP agent on a Cisco Internet CDN device sends an unsolicited notification to the SNMP manager if any of the events described in Table B-2 occurs on the device. This message is called a trap. You can configure your trap host (most likely your SNMP management station) to perform a specified action when a trap is detected.

Table B-2 Traps in the CISCO-CONTENT-NETWORK-MIB

SNMP Traps	Device Monitored	Description
ccnNotifOffline	Content Router Content Engine Content Distribution Manager	The device is about to disconnect from the network, possibly because of a reboot.
ccnNotifNeedsAttention	Content Router Content Engine Content Distribution Manager	The device is on the network but is unregistered (not associated with any CDN) or needs some other adjustment that cannot be done through the CDM administrator interface (such as repairing a disk, completing a software upgrade, or configuring the CDM database).
ccnNotifWaitingForCdm	Content Router Content Engine	The device is waiting for configuration information from the CDM. The device is on the network and is either failing to communicate with the CDM or is receiving instructions from the CDM to continue waiting pending activation by the CDN administrator.
ccnNotifOnline	Content Router Content Engine Content Distribution Manager	The device is operational and ready to participate in the CDN.

Using SNMP to Monitor CDN Devices

SNMP can be used to monitor CDN devices, as described in the following sections;

Monitoring Content Routers

The following variables provide information about Content Routers:

ccnReportDnsRequestRate—Number of DNS requests per second.

ccnReportDnsClientCount—Total number of DNS clients that have contacted this device since the DNS server last started.

ccnReportDnsRequests—Total number of DNS requests since the DNS server last started.

If the values of all three of the preceding variables for a Content Router are greater than 0, then the router is working. You will not see the values incrementing in real time, because the SNMP agent collects this information at 15-minute intervals.

Monitoring Content Engines

The following variables provide information about Content Engines:

ccnReportAcctBytesServed—Total number of bytes of content served to clients from this device since the servers on this device last started.

ccnReportAcctObjectsCached—Total number of objects in the content cache.

ccnReportAcctCacheHitRate—Number of cache hits per minute.

CcnReportAcctCacheMissRate—Number of cache misses per minute.

If the values of the preceding variables for a Content Engine are greater than 0, then the Content Engine is serving content.

Note Monitoring the Content Engine-specific variables *does not* enable you to detect when a Content Engine is about to reach its serving threshold.

When a Content Engine reaches its serving capacity, further requests sent to it will not be fulfilled. If a Content Engine cannot serve further content and is part of a cluster, the request will be served by another Content Engine within the cluster that is hosting the same content.

Identifying Overburdened Devices

The following conditions indicate overload or maximum CPU utilization on CDN devices.

- A device that generates the ccnNotifOffline, ccnNotifNeedsAttention, or ccnNotifWaitingForCdm traps needs attention.
- A device that frequently generates the ccnNotifOnline and ccnNotifServerStart traps needs attention.
- A device that shows sustained high levels of CPU utilization (between 80 and 90 percent) indicates overload. If your devices show 100 percent utilization for more than 5 minutes, you should consider either adding more Content Engines to your CDN or reducing the content load.

Also consider the following device-specific indicators.

Content Router

If the ccnReportDnsRequestRate variable approaches a value of 5000 requests per second, the potential exists for an overload of the Content Router.

Note Even if your system does approach this figure, the CDN will tolerate overload of individual Content Routers. As the response time slows and packets are dropped, clients will switch to other, more reliable servers.

Content Engine

The combined value of the ccnReportAcctCacheHitRate and ccnReportAcctCacheMissRate is a good measure of HTTP load on a Content Engine. However, there is no defined threshold for this load, because the threshold depends on the content mix served by the Content Engine.

APPENDIX C

CDN Supported Time Zones

Appendix C lists time zone designations and abbreviations that are supported by the Cisco Internet CDN Software. Time zones can be specified for any content item or content item group using the manifest file.

Specifying a time zone for a content item affects the expiration or activation of that item in a CDN where remote nodes are dispersed across different time zones.

This chapter contains the following sections:

- Supported Time Zone Abbreviations, page C-1
- Supported Time Zone Designations by Continent, page C-3

Supported Time Zone Abbreviations

ACT—Australian Central Time

AET—Australian Eastern Time

AGT

ART—Argentina Time

AST—Arabia Standard Time

BET—Bering Standard Time

BST—Bering Summer Time

CAT—Central Africa Time

CNT

CTT

EAT—East Africa Time

ECT—Ecuador Time

EET—East European Time

EST—Eastern Standard Time (U.S.)

GMT—Greenwich Mean Time

HST—Hawaiian Standard Time

IET

IST—Israeli Standard Time

JST—Japan Standard Time

MET—Middle European Time

MIT

MST—Mountain Standard Time

NET

NST—Newfoundland Standard Time

PLT

PNT—Pitcairn Time

PRT

PST—Pacific Standard Time

SST—Samoa Standard Time

UTC—Coordinated Universal Time

VST

WET—Western European Time

Supported Time Zone Designations by Continent

Africa

Africa/Abidjan

Africa/Accra

Africa/Addis_Ababa

Africa/Algiers

Africa/Asmera

Africa/Bangui

Africa/Banjul

Africa/Bissau

Africa/Blantyre

Africa/Bujumbura

Africa/Cairo

Africa/Casablanca

Africa/Conakry

Africa/Dakar

Africa/Dar_es_Salaam

Africa/Djibouti

Africa/Douala

Africa/Freetown

Africa/Gaborone

Africa/Harare

Africa/Johannesburg

Africa/Kampala

Africa/Khartoum

Africa/Kigali

Africa/Kinshasa

Africa/Lagos

Africa/Libreville

Africa/Lome

Africa/Luanda

Africa/Lubumbashi

Africa/Lusaka

Africa/Mbabane

Africa/Malabo

Africa/Maseru

Africa/Mogadishu

Africa/Monrovia

Africa/Nairobi

Africa/Ndjamena

Africa/Niamey

Africa/Nouakchott

Africa/Ouagadougou

Africa/Porto-Novo

Africa/Sao_Tome

Africa/Timbuktu

Africa/Tripoli

Africa/Tunis

Africa/Windhoek

Americas

America/Adak

America/Anchorage

America/Anguilla

America/Antigua

America/Aruba

America/Asuncion

America/Barbados

America/Belize

Atlantic/Bermuda

America/Bogota

America/Buenos_Aires

America/Caracas

America/Cayenne

America/Cayman

America/Chicago

America/Costa_Rica

America/Curacao

America/Dawson_Creek

America/Denver

America/Dominica

America/Edmonton

America/El_Salvador

America/Fortaleza

America/Godthab

America/Grand_Turk

America/Grenada

America/Guadeloupe

America/Guatemala

America/Guayaquil

America/Guyana

America/Halifax

America/Havana

America/Indianapolis

America/Jamaica

America/La_Paz

America/Lima

America/Los_Angeles

America/Managua

America/Manaus

America/Martinique

America/Mazatlan

America/Mexico_City

America/Montevideo

America/Montreal

America/Montserrat

America/Nassau

America/New_York

America/Noronha

Antarctica/Palmer

America/Panama

America/Paramaribo

America/Phoenix

America/Porto_Acre

America/Port-au-Prince

America/Port_of_Spain

America/Puerto_Rico

America/Regina

America/Santiago

America/Santo_Domingo

America/Sao_Paulo

America/Scoresbysund

America/St_Johns

America/St_Kitts

America/St_Lucia

America/St_Thomas

America/St_Vincent

Atlantic/Stanley

America/Tegucigalpa

America/Thule

America/Tijuana

America/Tortola

America/Vancouver

America/Winnipeg

Antarctica

Antarctica/Casey

Antarctica/DumontDUrville

Antarctica/Mawson

Antarctica/McMurdo

Asia and India

Asia/Aden

Asia/Almaty

Asia/Amman

Asia/Anadyr

Asia/Aqtau

Asia/Aqtobe

Asia/Ashkhabad

Asia/Baghdad

Asia/Bahrain

Asia/Baku

Asia/Bangkok

Asia/Beirut

Asia/Bishkek

Asia/Brunei

Asia/Calcutta

Asia/Colombo

Asia/Dacca

Asia/Damascus

Asia/Dubai

Asia/Dushanbe

Asia/Hong_Kong

Asia/Irkutsk

Asia/Jakarta

Asia/Jayapura

Asia/Jerusalem

Asia/Kabul

Asia/Kamchatka

Asia/Karachi

Asia/Katmandu

Asia/Krasnoyarsk

Asia/Kuala_Lumpur

Asia/Kuwait

Asia/Macao

Asia/Magadan

Asia/Manila

Asia/Muscat

Asia/Nicosia

Asia/Novosibirsk

Asia/Phnom_Penh

Asia/Pyongyang

Asia/Qatar

Asia/Rangoon

Asia/Riyadh

Asia/Saigon

Asia/Seoul

Asia/Shanghai

Asia/Singapore

Asia/Taipei

Asia/Tashkent

Asia/Tbilisi

Asia/Tehran

Asia/Thimbu

Asia/Tokyo

Asia/Ujung_Pandang

Asia/Ulan_Bator

Asia/Vientiane

Asia/Vladivostok

Asia/Yakutsk

Asia/Yekaterinburg

Asia/Yerevan

Indian/Antananarivo

Indian/Chagos

Indian/Christmas

Indian/Cocos

Indian/Comoro

Indian/Kerguelen

Indian/Mahe

Indian/Maldives

Indian/Mauritius

Indian/Mayotte

Indian/Reunion

Atlantic Nations

Atlantic/Azores

Atlantic/Canary

Atlantic/Cape_Verde

Atlantic/Faeroe

Atlantic/Jan_Mayen

Atlantic/Reykjavik

Atlantic/South_Georgia

Atlantic/St_Helena

Australia

Australia/Adelaide

Australia/Brisbane

Australia/Broken_Hill

Australia/Darwin

Australia/Hobart

Australia/Lord_Howe

Australia/Perth

Australia/Sydney

Europe

Europe/Andorra

Europe/Amsterdam

Europe/Athens

Europe/Belgrade

Europe/Berlin

Europe/Brussels

Europe/Bucharest

Europe/Budapest

Europe/Chisinau

Europe/Copenhagen

Europe/Dublin

Europe/Gibraltar

Europe/Helsinki

Europe/Istanbul

Europe/Kaliningrad

Europe/Kiev

Europe/Lisbon

Europe/London

Europe/Luxembourg

Europe/Madrid

Europe/Malta

Europe/Minsk

Europe/Monaco

Europe/Moscow

Europe/Oslo

Europe/Paris

Europe/Prague

Europe/Riga

Europe/Rome

Europe/Samara

Europe/Simferopol

Europe/Sofia

Europe/Stockholm

Europe/Tallinn

Europe/Tirane

Europe/Vaduz

Europe/Vienna

Europe/Vilnius

Europe/Warsaw

Europe/Zurich

Pacific Nations

Pacific/Apia

Pacific/Auckland

Pacific/Chatham

Pacific/Easter

Pacific/Efate

Pacific/Enderbury

Pacific/Fakaofo

Pacific/Fiji

Pacific/Funafuti

Pacific/Galapagos

Pacific/Gambier

Pacific/Guadalcanal

Pacific/Guam

Pacific/Kiritimati

Pacific/Kosrae

Pacific/Majuro

Pacific/Marquesas

Pacific/Nauru

Pacific/Niue

Pacific/Norfolk

Pacific/Noumea

Pacific/Pago_Pago

Pacific/Palau

Pacific/Pitcairn

Pacific/Ponape

Pacific/Port_Moresby

Pacific/Rarotonga

Pacific/Saipan

Pacific/Tahiti

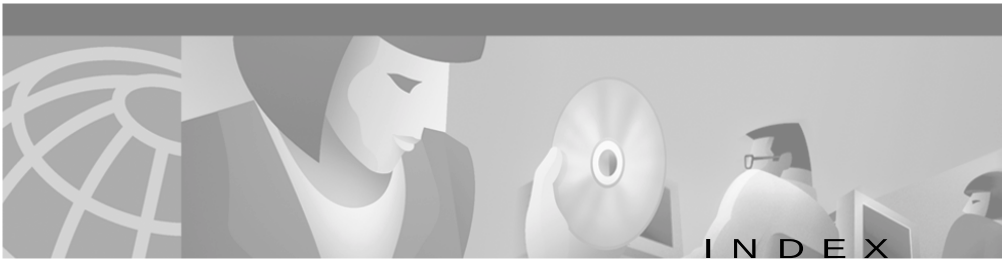
Pacific/Tarawa

Pacific/Tongatapu

Pacific/Truk

Pacific/Wake

Pacific/Wallis



INDEX