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 Configuration Guide

Part Number: 78-13578-01 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 information is accurate.
_____ The document is complete.
_____ The information I wanted was easy to find.
_____ The information is well organized.
_____ The information I found was useful to my job.

Please comment on our lowest scores:

Mailing Information

Company Name Date

Contact Name Job Title

Mailing Address

City State/Province ZIP/Postal Code

Country Phone ( ) Extension

Fax ( ) E-mail

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

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

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 4631 SAN JOSE CA

POSTAGE WILL BE PAID BY ADDRESSEE

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

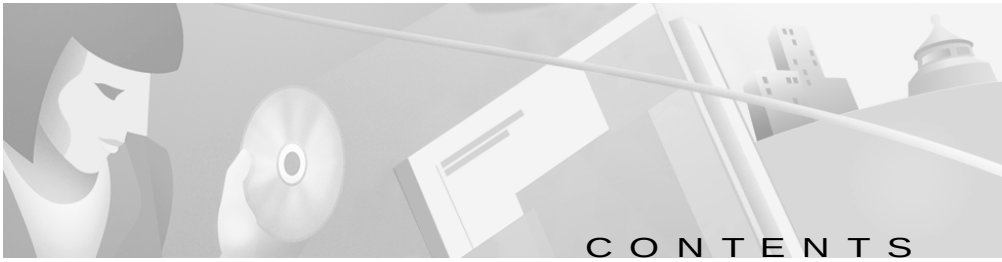
Cisco Internet CDN Software Configuration Guide

Version 2.1

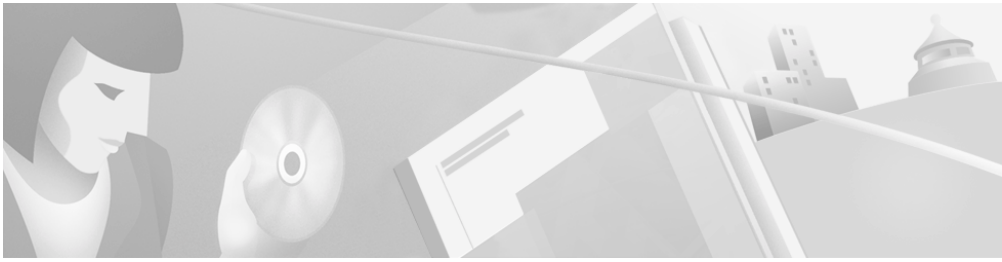
Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number: DOC-7813578=
Text Part Number: 78-13578-01

Cisco Internet CDN Software Configuration Guide



CONTENTS



Preface

Welcome to the Cisco Internet Content Delivery Network (CDN) solution for offering high-performance Internet content delivery services. Cisco Internet CDN Software Version 2.1 provides a powerful medium for adding intelligence to the network by routing requests to the best source, using bandwidth more efficiently, and adapting dynamically to changing network conditions.

Although Cisco CDN devices are delivered to you with the Cisco Internet CDN Software already installed, you must configure the devices before you can start creating and working with your CDN. This configuration guide describes what you need to do before configuration, and how to configure Cisco Internet CDN Software Version 2.1 devices.

This preface contains the following sections:

Audience

This guide is intended for network managers who configure Cisco Internet CDN Software Version 2.1 devices.

The network manager should be familiar with the following topics:

- Software installation and configuration
- Internet browsers
- Network routers
- IP network configuration
- Domain Name System (DNS) configuration
- Oracle 8i database installation and configuration

Organization

This document is organized in the following manner:

Chapter	Title	Description
Chapter 1	System Requirements	Describes the minimum hardware and software requirements for properly operating the Internet CDN Software.
Chapter 2	Preparing to Configure CDN Devices	Describes what you must do before you begin the configuration process and what information you should have available to use during the configuration process.
Chapter 3	Configuring CDN Devices	Describes how to configure CDN devices.

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.
`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.
	This pointer highlights an important line of text in an example.
^	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 User Guide Version 2.1*
- *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 500 Hardware Installation Guide*
- *Cisco Content Engine 500 Series Hardware Release Note*
- *Cisco Content Engine 7320 Product Description Note*
- *Cisco Content Router 4450 Product Description Note*
- *Cisco Content Networking Hardware Installation Guide for the Seven-Rack Unit Chassis*
- *Catalyst 5000 Family Software Configuration Guide*
- *Services Switch Configuration Guide—Catalyst 4000 Family, 2948G, and 2980G Switches*
- *Regulatory Compliance and Safety Information for the Cisco Content Networking Product Series*
- *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*

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

System Requirements

This chapter contains information on the minimum system requirements for the Cisco Internet CDN Software Version 2.1.

Minimum System Requirements

Cisco CDN Devices

Cisco Internet CDN Software Version 2.1 operates with the Content Distribution Manager CDM-4670-ICDN-K9, the Content Router CR-4450-ICDN-K9, the Content Engine CE-590-ICDN-K9, the Content Engine CE-590-DC-ICDN-K9, the Content Engine CE-7320-ICDN-K9, the Content Engine CE-7320-DC-ICDN-K9, the Content Services Switch 1115x and 1180x, the Storage Array SA6-SHF-6Disk-AC, the Storage Array SA6-SHF-6Disk-DC, and the Storage Array SA12-SHF-12Disk-AC. Refer to the Cisco documentation that came with each device for detailed, device-specific instructions on handling, installation, and configuration of your Cisco CDN hardware.

Workstations for Accessing the Web-Based User Interface

You interact with Cisco Internet CDN Software using the web-based graphical user interface that is installed on the Content Distribution Manager. The following minimum hardware and software requirements apply to each machine that is used as a workstation for accessing the graphical user interface.

Network

- Ethernet connection
- Connection to the Internet

Platform and Operating System

- Windows 95/98 Pentium-class system, 266 MHz, 64 MB of RAM
- Windows NT/2000 Pentium-class system, 266 MHz, 64 MB of RAM

Software

- Microsoft Internet Explorer 4.x/5.0 (or later)
- Netscape 4.7 (or later)
- RealNetworks RealPlayer (if deploying RealMedia content)
- Apple QuickTime player (if deploying QuickTime content)

Database Management System

Cisco Internet CDN Software requires that the Oracle 8i database management system (DBMS) be installed on your host network. The Internet CDN Content Distribution Manager uses an Oracle database for persistent storage of system information and statistics.

The Internet CDN *does not* require a dedicated Oracle database. If you already have an Oracle database in use within your organization, that database can also be used with your Internet CDN.

If you have not already done so, you must purchase Oracle 8i from Oracle. The DBMS requirement is Oracle 8i Version 8.1.6 or later.

For information about setting up the Oracle 8i database, refer to the Oracle documentation, and see the "Setting Up the Oracle 8i DBMS" section on page 2-6.

Domain Name System

Cisco Internet CDN Software uses the Domain Name System (DNS) to route requests to Content Engines. To serve content using your CDN, you must configure DNS. For information, see the "Configuring DNS" section on page 2-2.

RealServer, Darwin Streaming Server, and Windows Media Technologies Server

Devices such as Content Distribution Managers and Content Engines that serve QuickTime media files using the Apple Computer Darwin Streaming Server or RealNetworks RealMedia files or Windows Media files also require that the server software be installed.

Cisco Internet CDN Software Version 2.1 devices ship with the Darwin Streaming Server, RealNetworks RealServer, and Starbak Windows Media Technologies (WMT) Server already installed. However, if you wish to distribute RealMedia content over your Internet CDN, you must also purchase a server license from RealNetworks in order to use the RealServer feature. You also need to purchase a license to serve WMT content.

In addition, if you intend to serve live content using RealServer with Cisco Internet CDN Software Version 2.1, you will have to upgrade the RealServer software on your origin server to RealServer Version 8.0 if you have not already done so.

File Transfer Protocol Server

You need a File Transfer Protocol (FTP) server configured to receive ACTIVE-mode transmissions if you want to enable remote logging. For information, refer to the Cisco Internet CDN Software online help or the *Cisco Internet CDN Software User Guide*.

Simple Network Management Protocol

You need a Simple Network Management Protocol (SNMP) manager if you want to monitor system statistics using SNMP. For information about creating and registering an SNMP manager with your CDN, refer to Chapter 4, “Maintaining the Cisco Internet CDN Software,” in the *Cisco Internet CDN Software User Guide*.

Preparing to Configure CDN Devices

Before you configure CDN devices on your network, you must prepare for the configuration. This chapter tells you what you must do before you begin the configuration process and what information you need during the configuration process.

This chapter contains the following sections:

What to Do Before Configuration

When you set up a Content Delivery Network, you work with three types of devices: a Content Distribution Manager, Content Routers, and Content Engines. Optionally, a fourth and fifth device type can be added: Content Services Switches for the creation of supernodes, and Cisco Catalyst 4000 or 5000 Family switches.

Before you begin configuring CDN devices, you must do the following:

- Configure DNS.

  DNS must be configured before you use your CDN to deliver content, or the CDN will not deliver the content. Configuring DNS correctly is critical, so do it first. For information, see the "Configuring DNS" section on page 2-2.

- Determine whether your network uses a Dynamic Host Configuration Protocol (DHCP) server.

  If your network does not use a DHCP server or if it uses a DHCP server that does not assign static IP addresses, you must provide network information when you configure the Content Distribution Manager, Content Routers, and Content Engines. For information, see the "Determining Whether Your Network Uses a DHCP Server" section on page 2-5.

- Set up the Oracle 8i database.

  The Content Distribution Manager uses an external Oracle 8i database to store current CDN policies, so you must set up the database. For information, see the "Setting Up the Oracle 8i DBMS" section on page 2-6.

- Obtain the information you need for configuring your CDN devices.

  During the configuration process, you need to enter information about your network to respond to prompts from the setup script. For information, see the "Gathering Device Configuration Information" section on page 2-12.

Configuring DNS

When end users click CDN URLs to request content, the Cisco Internet CDN Software uses DNS to route the requests, using Content Routers, to the Content Engines hosting the content requested. Content Routers and Content Engines run DNS servers that know how to answer requests related to the CDN. Before your CDN can serve content associated with a domain, you must have DNS configured properly. It is important that you understand the following definitions before you proceed with configuring DNS.

- Hosted domain—A hosted domain name always has a minimum of four components. An example of a hosted domain is www.cdn.example.com.

- Delegated Domain—A delegated domain is the name that is delegated from some other DNS server to the CDN. It comprises the last three parts of a hosted domain. An example of a delegated domain is cdn.example.com. It is possible to have multiple domains delegated to the CDN, and to create many hosted domains per delegated domain.

Configuring DNS involves defining the delegated domain on your DNS server and creating mappings in the configuration file (also known as a "zone file") of a domain to the Content Routers that will handle requests for that domain.

Note You should create CDN parent domains on your DNS server before you create the hosted domain on the Content Distribution Manager user interface.

For instructions on creating hosted domains through the Content Distribution Manage user interface, refer to Chapter 2 of the *Cisco Internet CDN Software User Guide*.

Parent domains must be configured using conventional DNS tools.

To configure a delegated domain, list the Content Router host names as name servers for the domain. The Cisco Internet CDN Software allows you to configure a maximum of eight Content Routers.

Note Be careful to create only as many name servers as you have Content Routers at hand—even if you plan on adding Content Routers to your CDN later.

Reserving IP addresses for Content Routers that you are not assigning to actual devices will adversely affect content routing on your CDN.

To create your delegated domains, apply one of the following three naming conventions to the domain names:

- If you want the hosted domain to appear as a subdomain of the customer, a delegated domain (*cdn*, in the following example) must be created within each customer domain. A sample DNS zone file fragment follows:

```
$ORIGIN example.com
...
cdn
IN NS 1d hostname_of_content_router_1.example.com.
IN NS 1d hostname_of_content_router_2.example.com.
IN NS 1d hostname_of_content_router_3.example.com.
```

  where:

  example.com is the company for which you are serving content.

  cdn is the subdomain you created within www.example.com.

  hostname_of_content_router_x is the host name of the Content Router to which you want to map this domain.

  1d is one day, the TTL (Time To Live) value of the NS (Name Server) record. You can specify the TTL value in days (d), hours (h), minutes (m), or seconds (s).

  With the preceding DNS configuration, the following hosted domain is mapped to the Content Routers that you specified:

  `www.cdn.example.com`

- If you want the hosted domain to appear as a subdomain of the Internet service provider's domain, a single delegated domain (*content*, in the following example) can be shared by all content providers as follows:

```
$ORIGIN ISP.net
...
content
IN NS hostname_of_content_router_1.ISP.net.
IN NS hostname_of_content_router_2.ISP.net.
IN NS hostname_of_content_router_3.ISP.net.
```

  where:

  ISP.net is you, the service provider.

  content is the subdomain you created within www.ISP.net

  hostname_of_content_router_x is the host name of the Content Router to which you want to map this domain.

Using the preceding DNS configuration, you could create the following hosted domains mapped to the Content Routers that you specified:

```
www.customer1.content.ISP.net
www.customer2.content.ISP.net
```

- If you want to assign an alias to the hosted domain, for example, to advertise a name with only three components, you must enter the alias name in the Edit Hosted Domain page of the Content Distribution Manager. You must also enter the following in the configuration file of the hosted domain:

```
$ORIGIN example.com
...
www IN CNAME 1d www.cdn.
```

or

```
www IN CNAME 1d example.content.ISP.net.
```

Determining Whether Your Network Uses a DHCP Server

We recommend that you determine whether your network uses a DHCP server, and what kind of a DHCP server it is.

- If your network uses a DHCP server, the DHCP server automatically provides your CDN devices with network configuration information.

Warning **Do not use your DHCP server if it cannot assign static IP addresses. This is because every MAC address on your network needs to have a single, fixed IP address and fully-qualified domain name associated with it.**

- If your network does not use a DHCP server or if it uses a DHCP server that does not assign static IP addresses, you must provide network configuration information (the IP address, netmask, and gateway address) when you configure your CDN devices.

For the network information you must provide, see the "Gathering Device Configuration Information" section on page 2-12.

Setting Up the Oracle 8i DBMS

You must have an Oracle 8i database in use at your organization that can be used as the Internet CDN policy database. The Oracle server does not need to be dedicated to the Internet CDN. Use the instructions below to properly install the Oracle database, if you have not already done so, and to reserve resources on the Oracle database that will be used by the Internet CDN.

Installing the Oracle DBMS

You must install the Oracle 8i database management system (DBMS) on your host network. To do so, follow the instructions included with the Oracle DBMS.

During the installation, note the port number that the Oracle listener is configured to use. You need this port number when you configure the Content Distribution Manager.

Note The default listener port number is 1521.

You also need the database administrator account username and password.

Note The default database administrator account username is **system,** and the default password is **manager**.

Use the Oracle tools to create a database and note the session name you assign when you create the database.

Configuring the Oracle Database

From a Windows, Linux, or UNIX client, log in as the database administrator to the Oracle session and host previously created using a database administration tool such as SQL*Plus.

Note You may need to enter the connection information in the tnsnames.ora file found under the Oracle/networks/admin directory on your client system.

Perform the following SQL commands.

Note The following SQL commands are provided as an example. Refer to an SQL command reference for more information.

Step 1 Create a tablespace and temporary tablespace for use by the Cisco Internet CDN Software. A tablespace can be helpful with future administration of your CDN database.

Note Change the data file path to match the physical drives on the host Oracle server. SQL*Plus allows you to enter a single command as multiple lines.

```
SQL> create tablespace cdn DATAFILE 'datafile path on Oracle Server'
SIZE 250M REUSE default storage(initial 25K next 10K minextents 1
maxextents unlimited pctincrease 50);

SQL> create tablespace cdntemp DATAFILE
'datafile path on Oracle Server' SIZE 250M REUSE default
storage(initial 25K next 10K minextents 1 maxextents unlimited
pctincrease 50);
```

Additional data files can be associated with the tablespace using the following command.

```
SQL> alter tablespace cdn add DATAFILE
'datafile path on Oracle Server' SIZE 250M REUSE default
storage(initial 25K next 20K minextents 1 maxextents unlimited
pctincrease 50);
```

Step 2 List the names of the rollback segments:

```
SQL> select segment_name from dba_rollback_segs;
```

Rollback segments are used to keep information about the current transaction so that if an error occurs, the database can be returned to the state it was in before the transaction began.

Step 3 For the rollback segment listed in Step 2, change the max extents to be unlimited.

```
SQL> alter rollback segment rollback_segment_name STORAGE (NEXT 2 M
MAXEXTENTS unlimited);
```

You may also want to create a database user for the Cisco Internet CDN Software at this time.

Step 4 Use the following command to create a Cisco Internet CDN Software user account and password along with default tablespaces.

```
SQL> create user username identified by password default tablespace
cdn temporary tablespace cdntemp;
```

Note When prompted to enter a database username during the dbsetup component of the device setup routine, do not enter the database username you created here. Instead, enter the default Oracle administrator username and password. See Chapter 3, "Configuring CDN Devices," for information on using dbsetup to configure CDN devices.

Step 5 Grant access rights to the new user.

```
SQL> grant CREATE SESSION, connect, resource to username;
```

You can use dbsetup to create your database schema (see the "Configuring the Content Distribution Manager" section on page 3-23), but you can also install the Cisco Internet CDN Software database schema by using an SQL script shipped with the Cisco Internet CDN Software. This script contains the table definitions for the Cisco Internet CDN Software and can be modified to change things such as tablespace declarations, but the actual table column definition should remain unchanged.

Step 6 To load and run the script, you must first reconnect to the database using SQL*Plus and log in as the database user for the Cisco Internet CDN Software. Then use the **start** command to run the following MerlotCreate.sql script:

```
SQL> start LOCALPATH\MerlotCreate.sql
```

About Configuring CDN Devices

With the exception of the Content Services Switch, CDN devices must be configured using the setup program. Setup is a comprehensive configuration program that encompasses three other configuration routines:

- **netsetup**—This routine captures network configuration for the device such as the primary and content IP addresses, subnet, gateway, and DHCP information.
- **dbsetup**—This routine validates the Oracle 8i database that stores CDN data.
- **register**—This routine connects Content Engines and Content Routers to their assigned Content Distribution Manager.

You run the setup program on each device to name the device, specify the Oracle database information and DNS server information for the Content Distribution Manager, specify network interfaces and network information, bring the network online, generate certificates, and register the Content Distribution Manager, Content Routers, and Content Engines.

Note If you have not completed the preconfiguration tasks described in the "What to Do Before Configuration" section on page 2-1, do them before you start configuring your CDN devices. Otherwise, your CDN will not deliver content to users.

Configuration Priorities

When you begin your CDN device configuration, configure your devices according to the following priorities:

1. Content Services Switch and Catalyst switch (if used)
2. Content Distribution Manager
3. Content Routers and Content Engines

See the following sections for CDN device configuration information:

- "Configuration Information for Content Services Switches" section on page 2-14
- "Configuring the Content Services Switch" section on page 3-8

- "Configuration Information for Content Distribution Manager, Content Engines, and Content Routers" section on page 2-12
- "Configuring the Content Distribution Manager" section on page 3-23
- "Configuring a Content Router" section on page 3-28
- "Configuring a Content Engine" section on page 3-32

CDN Device Network Addressing

Your CDN devices use a number of different network addresses to manage different types of content requests from end users and from other devices on the CDN. This section identifies and explains the different kinds of addresses you are asked to supply during configuration of your CDN devices. Make sure that you understand the purpose of each type of network address before continuing with device configuration.

Primary Versus Content IP Address

Content Routers and Content Engines require two IP addresses to operate: a *primary IP address* and a *content IP address*. The Content Distribution Manager requires only a single address, the primary IP address.

- The primary IP address is used for inter-CDN communication and administration of the system: for example, passing configuration information from the Content Distribution Manager to the devices it manages.

  The primary IP address will not change. If DHCP is used for the primary IP address, an administrator must make sure the Content Router or Content Engine is always assigned the same IP address by the server.

- The content IP address is used by devices to respond to DNS queries originating from web browsers, media players, and DNS servers located outside the CDN. Content Routers accept DNS queries at their content IP address. Content Engines accept DNS queries, as well as HTTP and RTSP requests at their content IP address. Content Distribution Managers do not have a content IP address.

You must assign each IP address to an Ethernet port. The primary and content IP addresses can each use a unique Ethernet port, or they can share a single port.

- The primary IP address should be assigned to the first Ethernet port interface, eth0.
- The content IP address can be assigned to either eth0 or a different port.

If you decide to use separate Ethernet ports for the primary and content IP addresses, you must provide separate subnet and gateway information for each port. In this case, DHCP is capable of assigning one IP address per interface.

See the "CDN Device Wiring Configuration" section on page 3-21 for more information on assigning your primary and content IP addresses to the appropriate port on your CDN device.

Virtual Address

The Content Services Switch is configured with one or more *virtual IP addresses*. These addresses are assigned one per cluster for each cluster associated with the Content Services Switch.

When requests are received for a particular cluster using that cluster's virtual IP address, the Content Services Switch uses Network Address Translation (NAT) to map the virtual IP address to the content IP addresses of the Content Engines in that cluster.

Internal Subnet Addresses

The Content Services Switch maintains an internal subnet of Content Engine 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.

CSS Configuration Address

The Content Services Switch maintains an address, the *CSS configuration address*, through which it communicates with the Content Distribution Manager. Requests and commands are sent from the Content Distribution Manager, programmatically, to the Content Services Switch at the CSS configuration address using Secure Shell (SSH) to encrypt this traffic.

Gathering Device Configuration Information

Before you configure your CDN devices, you need to have specific information available so you can respond to prompts during configuration.

Configuration Information for Content Distribution Manager, Content Engines, and Content Routers

Table 2-1 shows the device information you need when you configure the Content Distribution Manager, Content Routers, and Content Engines.

Table 2-1 Device Information for Configuring the Content Distribution Manager, Content Routers, and Content Engines

Device Information	Description
Meaningful name for each device	Names you want to assign to the Content Distribution Manager, Content Routers, and Content Engines. It can be helpful if a name identifies the device type and the location. This name *cannot* contain any spaces.
Content Distribution Manager port number	For the Content Distribution Manager configuration, provide a port number, or use the default port number, 2001.

If your network uses a DHCP server, then you do not provide network configuration information when you configure CDN devices. If your network does not use a DHCP server, then you must provide network configuration information when you configure your CDN devices. Table 2-2 shows the network information you need for the Content Distribution Manager, Content Routers, and Content Engines.

Table 2-2 Network Information for Configuring the Content Distribution Manager, Content Routers, and Content Engines

CDN Device Information	Description
Wiring configuration	Content Engines, Content Routers, and the Content Distribution Manager come supplied with (and the Cisco Internet CDN software supports) both Fast Ethernet (10/100) and Gigabit Ethernet (GigE) cards. Before attempting to configure your CDN, decide which type of Ethernet card you will be using.
IP addresses	The Content Distribution Manager requires only one IP address—the primary IP address. The Content Routers and Content Engines require a primary IP address and a content IP address. See the "CDN Device Network Addressing" section on page 2-10 for more information.
Ethernet interface	Content Engines and Content Routers require two IP addresses: the primary IP address and a content IP address. These addresses can be assigned to a single Ethernet interface on the Content Engine, or each address can be assigned to a separate Ethernet interface. Decide in advance whether you want the primary and content IP addresses to share an Ethernet interface or to use separate Ethernet interfaces on your Content Engine. The Content Distribution Manager requires a single network interface for the primary IP address. See the "CDN Device Wiring Configuration" section on page 3-21 for more information.
Netmask	Address that represents your local-area subnet mask.
Gateway address	Address of a gateway device or router on the network.

The Content Distribution Manager uses an external Oracle 8i database to store current CDN policies. Table 2-3 shows the Oracle database server information you need during the Content Distribution Manager configuration.

Table 2-3 Oracle Database Information for Configuring Content Distribution Manager

Oracle Database Information	Description
Database server name or address	Fully qualified domain name or the IP address of the Oracle 8i database server on the host network.
Database listener port	Port number specified when the Oracle listener was installed. If no port number was specified, use the default listener port number, 1521.
Database service name	Service name specified when the Oracle database was installed. If no port was specified, use the default.
Database username	Valid Oracle database usernames. The default database username is *system*.
Database password	Valid Oracle database password that was specified when the username was created. The default database password is *manager*.

After you have the database and network information, you are ready to configure your CDN devices.

Configuration Information for Content Services Switches

The Content Services Switch is an optional component of the Internet CDN Software. If you are not deploying a Content Services Switch on your CDN, continue with the next chapter.

Note Before you can use the Content Services Switch with your other CDN devices, you must first obtain a valid Secure Shell (SSH) license and license key and then activate your SSH software. The SSH software license key is on a sticker attached to the cover of your Content Services Switch documentation.

Table 2-4 shows the device information you need when you configure the Content Services Switch, which is used to create supernodes.

Table 2-4 Content Services Switch Configuration Information

Content Services Switch Configuration Information	Description
Wiring configuration	Decide in advance whether Content Engines will connect directly to the Content Services Switch, or whether both Content Engines and the Content Services Switch will be connected to one another and the Internet through a Catalyst switch.
VLAN configuration	Decide whether you will be implementing one or two virtual local-area networks (VLANs) consisting of a virtual and internal IP address and subnet on the Content Services Switch. With two VLANs, the Content Engines and Content Services Switch use one VLAN address for internal communication between Content Engines and the Content Services Switch, and the second VLAN for communication between the switch and the public Internet (the *uplink* VLAN). When only one VLAN is deployed, only that VLAN address is used for internal and external communication.
SSH software license key	Unique key that enables the SSH software on the Content Services Switch. SSH is required for the Content Services Switch to communicate with the Content Distribution Manager. The SSH software license key is on a sticker attached to the cover of your Content Services Switch documentation.
Uplink address	Address at which the Content Services Switch is connected with the uplink switch. This address is necessary only when the Content Services Switch is configured using a dual-VLAN configuration, in which one VLAN is used as an uplink VLAN.
Configuration IP address	Address at which the Content Distribution Manager connects to the Content Services Switch using SSH.
Configuration subnet mask	Subnet mask of the configuration IP address. This is the subnet of addresses from which the Content Engine contents are chosen in a supernode.
Internal subnet	Nonroutable subnet for the Content Services Switch. This is the set of internal addresses from which Content Engine content IP addresses are assigned when Content Engines are associated with a Content Services Switch.

Table 2-4 Content Services Switch Configuration Information (continued)

Content Services Switch Configuration Information	Description
Internal address	First address on the subnet that will contain the content IP addresses of the Content Engines. For example, if the internal subnet is 192.168.128.0, the internal address is 192.168.128.1.
Redundancy subnet	When a redundant Content Services Switch is configured, this is the nonroutable subnet shared by both the master (primary) and backup (redundant) Content Services Switch.
Master address	First address on the redundancy subnet. For example, if the redundancy subnet is 192.168.128.0/17, the master address is 192.168.128.1.
Backup address	Second address on the redundancy subnet. For example, if the redundancy subnet is 192.168.128.0/17, the backup address is 192.168.128.2.

Connecting to CDN Devices Using the Command-Line Interface

Although the Content Distribution Manager graphical user interface (GUI) can be used to modify many CDN device configuration settings once a device has been properly configured, initial device setup takes place using the CDN command-line interface (CLI). After initial setup, certain maintenance and troubleshooting activities—such as modifying a device network address or restarting a device that has been stopped—also require you to interact with CDN devices using the CLI.

You can access the CLI for a CDN device by connecting a console cable to the designated console cable port on the device and attaching the device to a console terminal or a PC running terminal emulation software such as Telnet or SSH. Refer to the Cisco hardware documentation that came with your CDN device for instructions on connecting the console cable.

Note Before you can use the Content Services Switch with your other CDN devices, you must first obtain a valid SSH license and license key and then activate your SSH software. The SSH software license key is on a sticker attached to the cover of your Content Services Switch documentation.

Refer to the Cisco hardware documentation that came with your CDN device for detailed information on cabling and accessing the device's CLI or web-based management interface (where applicable). Also refer to the *Cisco Internet CDN Software Command Reference* for detailed instructions on using Cisco Internet CDN Software commands.

CHAPTER 3

Configuring CDN Devices

The Cisco Internet CDN Software is already installed on your CDN devices. This chapter tells you how to use the Internet CDN software to configure these devices on your network.

This chapter contains the following sections:

Content Services Switch Wiring Configuration

Content Services Switches are an *optional* component of the Cisco Internet CDN.

Before you attempt to configure your Content Services Switch, you must decide how your switch and the Content Engines located behind it will be connected to the switch and to the rest of the CDN.

Your Content Services Switch can be connected as follows:

- Directly to the Content Engines
- To a Catalyst switch with connections to the Content Engines
- To a Catalyst switch with connections to the Content Engines and to a redundant Content Services Switch

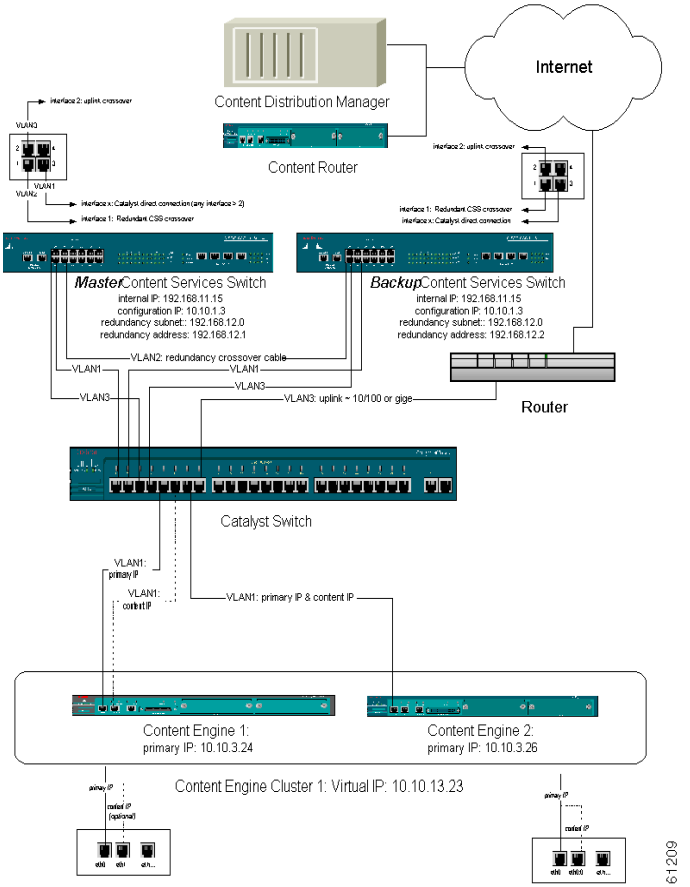
In addition to the various physical wiring configurations available to you, Content Services Switches also support the deployment of multiple virtual LANs (VLANs), an arrangement that provides additional address space for Content Engines grouped behind Content Services Switches in deployments in which more than one Content Services Switch is deployed on the same CDN.

See the wiring diagrams that follow for more information on the different options available to you when configuring your Content Services Switch and structuring your Content Delivery Network. Also see the “Gathering Device Configuration Information” section on page 2-12 for information on the configuration information you need to have before beginning configuration of the Content Services Switch.

Figure 3-1 illustrates deployment of redundant Content Services Switches on a CDN connected to Content Engines through a Catalyst switch, with a second VLAN (VLAN3) assigned to the uplink connection.

In Figure 3-1, both the master Content Services Switch and the backup Content Services Switch are connected using a crossover Ethernet cable connected to interface 1 on each switch. These devices communicate using unique redundancy addresses assigned to VLAN2, the default redundancy subnet.

Figure 3-1 Redundant Content Services Switches Connected to a Catalyst Switch with Two VLANs



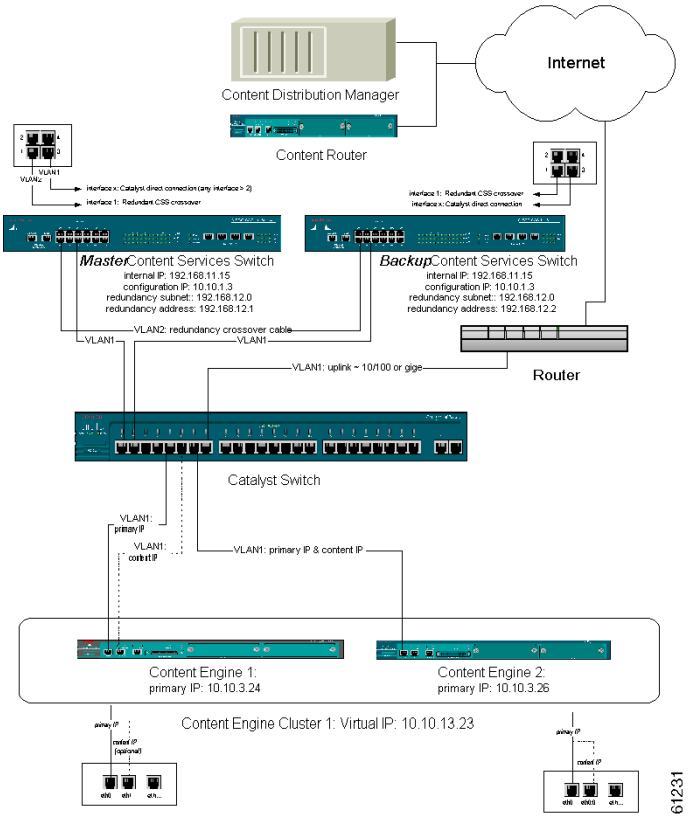
Primary communication among the Content Services Switch, Catalyst switch, and Content Engines takes place on VLAN1, the default VLAN for the switch. Connections for VLAN1 are made to any Content Services Switch interface after interface 2.

VLAN3 is configured for the uplink connection from the Content Services Switch to the uplink subnet using interface 2 on both the master and the backup Content Services Switch.

Figure 3-2 illustrates deployment of redundant Content Services Switches on a CDN connected to Content Engines through a Catalyst switch, with a single VLAN (VLAN1) assigned to both internal communication and the uplink connection.

In Figure 3-2 both the master Content Services Switch and the backup Content Services Switch are connected using a crossover Ethernet cable connected to interface 1 on each switch. These devices communicate using unique redundancy addresses assigned to VLAN2, the default redundancy subnet.

Figure 3-2 Redundant Content Services Switches Connected to a Catalyst Switch with One VLAN



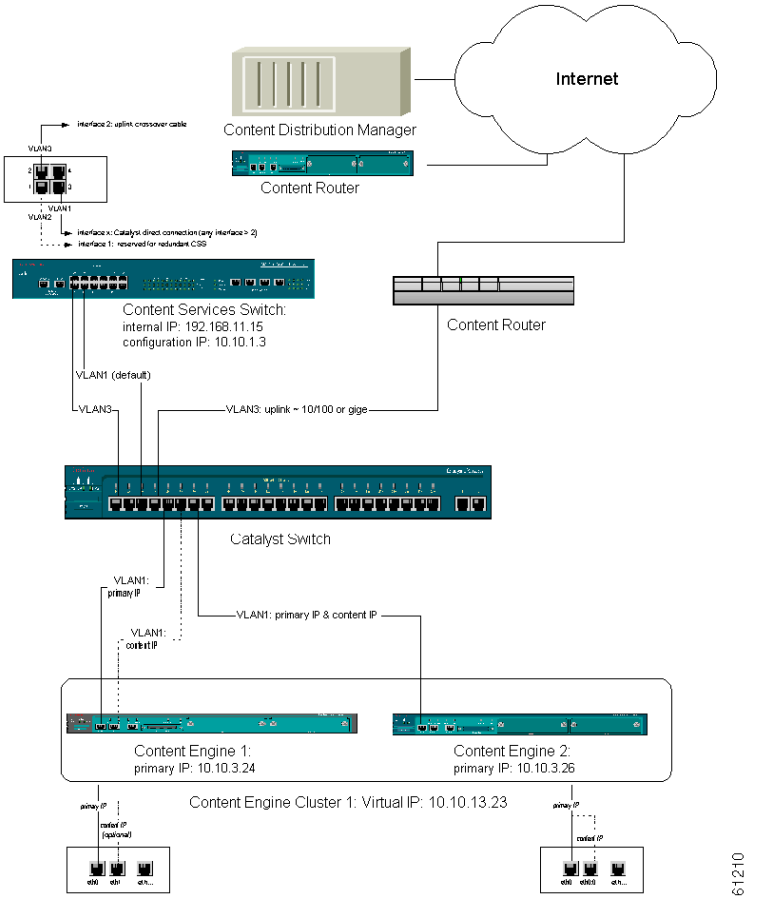
Primary communication among the Content Services Switch, Catalyst switch, and Content Engines takes place on VLAN1, the default VLAN for the switch. Connections for VLAN1 are made from any Content Services Switch interface after interface 2.

VLAN1 is also assigned to the uplink connection from the Content Services Switch to the uplink subnet using interface 2 on both the master and the backup Content Services Switch.

Figure 3-3 illustrates deployment of a nonredundant Content Services Switch on a CDN connected to Content Engines through a Catalyst switch, with a second VLAN (VLAN3) assigned to the uplink connection.

Primary communication among the Content Services Switch, Catalyst switch, and Content Engines takes place on VLAN1, the default VLAN for the switch. Connections for VLAN1 are made from any Content Services Switch interface after interface2.

Figure 3-3 Nonredundant Content Services Switch Connected to a Catalyst Switch with Two VLANs

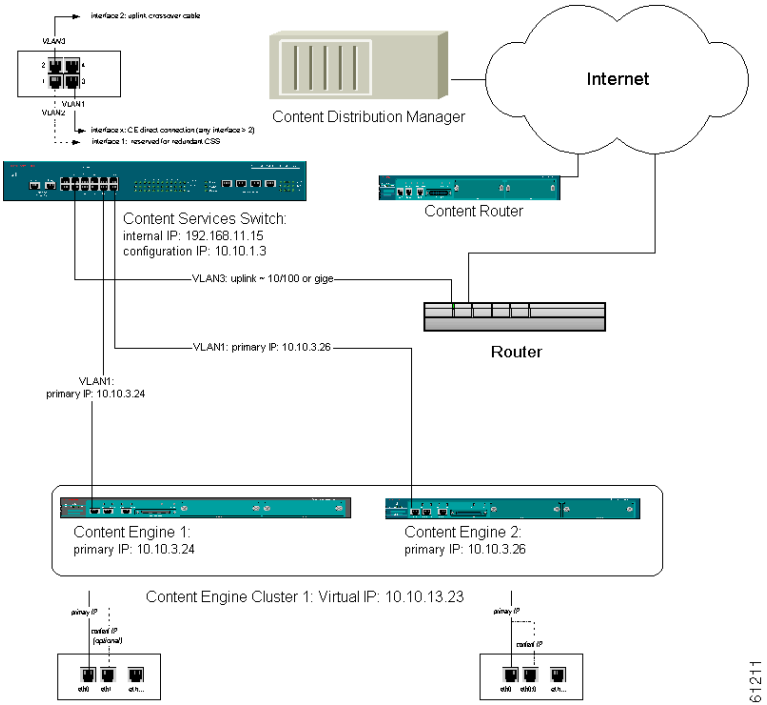


VLAN3 is configured for the uplink connection from the Content Services Switch and the uplink subnet using interface 2 on both the master and the backup Content Services Switch.

Figure 3-4 illustrates deployment of a nonredundant Content Services Switch on a CDN connected directly to Content Engines through a Catalyst switch, with a second VLAN (VLAN3) assigned to the uplink connection (interface 2) on the Content Services Switch.

Primary communication among the Content Services Switch and Content Engines takes place on VLAN1, the default VLAN for the switch. Connections for VLAN1 are made from any Content Services Switch interface after interface 2.

Figure 3-4 Nonredundant Content Services Switch Connected to Content Engines with Two VLANs



Configuring the Content Services Switch

If you are deploying a Content Services Switch and will be creating supernodes that use the switch, you must set up the switch before configuring your Content Engines, creating supernodes, or creating Content Engine clusters.

See the "Configuring a Content Engine" section on page 3-32 for information on configuring the Content Engines that will be grouped behind the switch. Also, refer to the "Activating and Defining Content Routers and Content Engines" and "Adding Supernodes and Content Engine Clusters" sections in Chapter 2 of the *Cisco Internet CDN Software User Guide* for information on activating Content Engines once they are configured, and on creating supernodes containing Content Engine clusters.

Before attempting to configure your Content Services Switch, make sure that you have reviewed the "Gathering Device Configuration Information" section on page 2-12.

Configuring the Content Services Switch Using the Configuration Script

In order to facilitate Content Services Switch configuration, we provide a configuration script that walks you through the steps required to properly configure your Content Services Switch for use with the Cisco Internet CDN Software. This script uses simple prompts to collect the information necessary to configure a Content Services Switch.

It is also possible to manually configure your switch without using the script. See the "Manually Configuring the Content Services Switch" section on page 3-16 for instructions on manually configuring a Content Services Switch.

The setup script can be uploaded to the Content Services Switch manually or through the CDM user interface. From the Content Distribution Manager user interface, click Tools and choose Content Services Switch from the drop-down list. For more information on using the CDM user interface to upload the script, see the "Updating the Software on a Content Services Switch" section in Chapter 4 of the *Cisco Internet CDN Software User Guide*.

Use the following procedure to manually install and run the Content Services Switch configuration script.

Preparing the Content Services Switch and Uploading the Script

Before you can run the Content Services Switch setup script, you must first place the script on the Content Services Switch you wish to configure. In order to do this, you must:

- Access the Content Services Switch device by connecting a terminal to the device, or using terminal emulation software installed on a desktop workstation.
- Enable the File Transfer Protocol (FTP) on the Content Services Switch on which you will be running the setup script.
- Access the Content Distribution Manager by connecting a terminal to the device, or using terminal emulation software installed on a desktop workstation.
- Transfer the setup script from the Content Distribution Manager to the Content Services Switch using FTP.

Use the following procedure to upload the setup script from the Content Distribution Manager to the Content Services Switch:

Step 1 Log in to the Content Services Switch using the login **admin** and password **system**.

Step 2 Enter into configuration mode by entering the **configure** command, as follows:

```
# configure
```

The # prompt changes to (config)#, indicating that you are in configuration mode.

Step 3 To enable FTP on the switch, enter the **no restrict ftp** command. For example:

```
(config)# no restrict ftp
```

Step 4 Exit configuration mode by entering the **exit** command, and then exit the Content Services Switch command-line interface by entering the **exit** command at the prompt. For example:

```
(config)# exit
# exit
```

Step 5 Log in to the Content Distribution Manager using the login **admin** and password **default**.

Step 6 Navigate to the /cisco/merlot/etc directory on the Content Distribution Manager.

```
cdm-device-name> cd cisco/merlot/etc
```

Step 7 Locate the file *merlot-css-setup*. This is the Content Services Switch setup script.

Step 8 Launch FTP on the Content Distribution Manager and connect to the Content Services Switch. You need to provide a user login and password for the Content Services Switch. For example:

```
cdm-device-name> ftp Content Services Switch IP address
name: admin
password: system
```

Step 9 Navigate to the /script directory on the Content Services Switch. The setup script must be placed in the /script directory to work properly. For example:

```
ftp> cd script
```

Step 10 Transfer the merlot-css-setup script file from the Content Distribution Manager to the Content Services Switch. For example:

```
ftp> put merlot-css-setup
```

Step 11 If you are configuring a redundant Content Services Switch, repeat Step 8 through Step 10 for the redundant switch.

Step 12 Exit FTP by entering **quit** at the ftp prompt. You are returned to the Content Distribution Manager prompt.

Step 13 Exit the Content Distribution Manager command-line interface by entering the **exit** command.

You are now ready to log on to the Content Services Switch and begin setup of the device using the merlot-css-setup script. See the next section for details on running the Content Services Switch setup.

Running the Content Services Switch Setup Script

Use the following procedure to guide you in using the merlot-css-setup script. Clicking **q** (quit) at any time aborts the setup procedure, saving any configuration settings already changed by the script.

Step 1 Log in to the Content Services Switch using the login **admin** and **default** password.

Step 2 From the prompt, discard any existing configuration settings using the **clear running-config** command as follows:

```
css-device-name> clear running-config
```

Note If you are unsure whether or not the switch has been configured previously, proceed to Step 3. The Content Services Switch setup program automatically detects any previous configurations and prompts you to discard them before continuing. Enter **y** (yes) when prompted to run the **clear running-config** command.

Step 3 From the prompt, launch the setup script by entering the following command:

```
css-device-name> script play merlot-css-setup
```

Step 4 When prompted to continue with setup, enter **y** (yes).

```
No startup-config was found, continue with the setup script [y/n]? y
```

Step 5 When prompted to indicate the number that will be used to identify the VLAN for the configuration and internal subnet, enter a number between 1 and 4095.

- If you are using a Cisco Catalyst Switch on your CDN, as well as the Content Services Switch, make sure that the VLAN number you choose is consistent with the number assigned to the same VLAN on the Catalyst switch.
- If you are not deploying a Catalyst switch, choose any number that suits you. The default VLAN number is 1. Make sure that subsequent VLANs on this device are assigned different numbers.

Step 6 When prompted to identify the interfaces (or ports) that are assigned to this VLAN, enter the interface number in the proper format for the switch you are configuring:

- For CS-800 model switches, enter the slot and interface number for each interface. For example, if interfaces 1 and 2 on slot 2 belong to this VLAN, you would enter:

  2/1 2/2

- For CS-500 model switches, enter the interface number in the format *ethernet-x*, where *x* is the number of the interface. For example, if interfaces 5, 6, and 7 belong to this VLAN, you would enter:

  ethernet-5 ethernet-6 ethernet-7

- If you are unsure of the proper format for the device you are configuring, enter **q** to quit the setup script and then enter **show interface** to display information on your interfaces in the proper format.

  css-device-name> **sh interface**

Step 7 When prompted, enter the configuration IP address and subnet mask for the Content Services Switch. For example:

```
What is the CONFIGURATION address of this CSS? [default = 192.168.0.1]
10.89.1.3

What is the CONFIGURATION subnet mask of this CSS?
[default = 255.255.0.0] 255.255.240.0
```

Step 8 When prompted, enter the default gateway for the Content Services Switch. For example:

```
What is the default gateway of this CSS? [default = 192.168.0.1]
10.89.0.1
```

Step 9 When prompted, enter the internal subnet and internal subnet mask for the Content Services Switch. For example:

```
What is the INTERNAL SUBNET of this CSS? [default = 192.168.0.0]
192.168.1.0
```

The Content Services Switch setup script automatically sets the internal IP address (also referred to as the hidden address in the script) to the first available address in the subnet. For example,

```
The hidden address of this CSS is set to the first address of this
CSS: 192.168.1.1

What is the INTERNAL subnet mask of this CSS? [default = 255.255.0.0]
255.255.255.0
```

Step 10 When prompted, indicate whether you will be designating a separate VLAN for the uplink connection from the device to your CDN. For example:

```
Do you want a separate VLAN for the uplink? [y/n]? y
```

Step 11 Perform one of the following actions:

- If you are not configuring a separate uplink VLAN, skip to Step 13.
- If you are configuring a separate VLAN for the uplink interface, enter a number between 1 and 4095 to identify the VLAN. For example:

  ```
  What is the number [1-4095] of this VLAN? [default = 3] 200
  ```

Step 12 When prompted, identify the interfaces (or ports) that are assigned to the uplink VLAN; enter the interface number in the proper format for the switch you are configuring:

- For CS-800 model switches, enter the slot and interface number for each interface. For example, if interface 2 on slot 1 belongs to the uplink VLAN, you would enter:

  ```
  1/2
  ```

- For CS-500 model switches, enter the interface number in the format *ethernet-x*, where *x* is the number of the interface. For example, if interfaces 2 belongs to the uplink VLAN, you would enter:

  ```
  ethernet-2
  ```

- If you are unsure of the proper format for the device you are configuring, enter **q** to quit the setup script and then enter **show interface** command to display information on your interfaces in the proper format.

  ```
  css-device-name> sh interface
  ```

Step 13 When prompted, enter the uplink IP address and subnet mask for the Content Services Switch. This is the address and subnet used by the Content Services Switch to communicate with the uplink subnet. For example:

```
What is the UPLINK IP address of this CSS? [default = 192.168.0.1]
192.168.128.12

What is the subnet mask of the UPLINK? [default = 255.255.0.0]
255.255.128.0
```

Step 14 When prompted to indicate whether you will be deploying a redundant Content Services Switch, enter **y** (yes) or **n** (no), depending on your own network configuration. For example:

```
Is this a redundant CSS configuration? [y/n]? y
```

Note Enter **y** even if the Content Services Switch you are configuring is the master Content Services Switch. The setup program prompts you to configure the backup switch after you configure the master switch.

Redundancy addresses are configured on virtual LAN 2 (VLAN2).

Step 15 If you are not configuring a redundant Content Services Switch, you have successfully configured the Content Services Switch. The setup script will end, returning you to the Content Services Switch prompt.

If you are configuring a redundant Content Services Switch, continue with Step 16.

Step 16 When prompted, enter a number between 1 and 4095 to identify the redundancy VLAN. For example:

```
What is the number [1-4095] of this VLAN? [default = 3] 300
```

Step 17 When prompted identify the interface that is assigned to the redundancy VLAN; enter the interface number in the proper format for the switch you are configuring:

- For CS-800 model switches, enter the slot and interface number for each interface. For example, if interface 1 on slot 1 is used as the redundancy interface VLAN, you would enter:

  ```
  1/1
  ```

- For CS-500 model switches, enter the interface number in the format *ethernet-x*, where *x* is the number of the interface that will be used for redundancy. For example, if interface 1 is assigned to the redundancy VLAN, you would enter:

  ethernet-1

- If you are unsure of the proper format for the device you are configuring, enter **q** to quit the setup script and then enter **show interface** to display information on your interfaces in the proper format.

  ```
  css-device-name> show interface
  ```

Step 18 When prompted, enter the redundancy subnet and subnet mask of the Content Services Switch. The redundancy addresses are used for communication between master and backup Content Services Switches in a redundant CSS implementation. For example:

```
What is the redundancy subnet of this CSS? [default = 192.168.0.0]
192.168.128.0
```

Once you have assigned the redundancy subnet, the setup script automatically assigns the redundancy address to both the master and the backup Content Services Switch, even if the backup Content Services Switch has not yet been configured. The master CSS address will always be the first available address on the redundancy subnet, and the backup CSS address will always be the second available address. For example:

```
Master CSS address: 192.168.128.1, backup CSS address: 192.168.128.2

What is the redundancy subnet mask of this CSS?
[default = 255.255.0.0] 255.255.255.0
```

Step 19 When prompted, indicate whether the Content Services Switch is a master or backup switch. Enter **y** (yes) to indicate that it is a master switch. Enter **n** (no) to indicate that it is a backup switch. For example:

```
Is this master CSS? 'y' for master, 'n' for backup [y/n]? y
```

Step 20 If you are configuring a redundant Content Services Switch, connect a crossover Ethernet cable from interface 1 on the master Content Services Switch to interface 1 on the backup switch and then repeat Step 1 through Step 19 for the backup switch.

You have now completed configuration of your Content Services Switch. The setup script ends, returning you to the Content Services Switch prompt.

Manually Configuring the Content Services Switch

Use the following procedure to manually configure your nonredundant Content Services Switch for use in a one- or two-VLAN deployment.

Step 1 Log in to the Content Services Switch using the admin login with the default password, **system**.

Step 2 Clear the old configuration by entering the following command at the prompt:

```
# clear running-config
```

Step 3 Enter into configuration mode by entering the **config** command as follows:

```
# configure
```

The # prompt changes to (config)#, indicating that you are in configuration mode.

Step 4 Configure global parameters using the **ip route** command as follows:

```
(config)# ip route 0.0.0.0 0.0.0.0 default gateway
```

You must now configure the Content Services Switch circuit using the **circuit** command.

Step 5 Enter the **circuit** command as follows.

Note The internal address is the first address on the internal subnet.

The (config)# prompt changes to indicate that you are configuring the circuit:

```
(config)# circuit VLAN1
(config-circuit[VLAN1])#ip address configuration ip address
configuration subnet mask
(config-circuit[VLAN1])# no redirects
(config-circuit[VLAN1])# exit
(config)# ip address internal-address internal-subnet-mask
(config)# exit
(config)# exit
```

Step 6 If you are implementing a second VLAN, configure it now by entering the **circuit** command again as follows:

```
(config)# circuit VLAN3
(config-circuit[VLAN3])# ip address uplink address uplink subnet mask
(config-circuit[VLAN3])# exit
(config)# exit
(config)# interface ethernet-2
(config)# bridge vlan 3
(config)# exit
```

Step 7 Exit configuration mode by entering **exit** as follows:

```
(config)# exit
```

You must now activate the SSH software installed on the Content Services Switch using the software license key supplied to you with the switch.

Step 8 From the # prompt, enter the license command as follows:

```
# license
```

You are prompted to enter the software license key.

Step 9 Enter the license key value supplied on the front cover of your Content Services Switch documentation.

Step 10 Save the configuration by entering the **write memory** command at the # prompt as follows:

```
# write memory
```

Step 11 End your command-line session by entering the **exit** command at the # prompt as follows:

```
# exit
```

Manually Configuring Content Services Switches with Redundancy

When configuring your Content Services Switch for use in an implementation with a redundant (backup) Content Services Switch, the configuration of the redundant Content Services Switch and the primary (or master) Content Services Switch should be identical, except that the IP address used in the redundancy protocol and ArrowPoint Peer (APP) session is the first address of the redundancy subnet for the master Content Services Switch and the second redundancy subnet address for the backup Content Services Switch.

For example, if the redundancy subnet is 192.168.128.0/17, then the Content Services Switch master address is:

```
192.168.128.1
```

and the Content Services Switch backup address is:

```
192.168.128.2
```

Use the following procedure to manually configure your redundant Content Services Switches for use in a one- or two-VLAN deployment:

Step 1 Log in to the Content Services Switch using the admin login with the default password, **system**.

Step 2 Clear the old configuration by entering the following command at the prompt:

```
# clear running-config
```

Step 3 Enter into configuration mode by entering the **configure** command.

Step 4 Configure global parameters as follows:

```
(config)# ip route 0.0.0.0 0.0.0.0 default gateway
(config)# ip redundancy
(config)# app
(config)# app session backup-address
```

Step 5 Configure the Content Services Switch Ethernet port as follows:

```
(config) # interface ethernet-1
(config-if(ethernet-1)# bridge vlan 2
(config-if(ethernet-1)# exit
```

Step 6 Configure circuit VLAN1 as follows:

Note The internal address is the first address on the internal subnet.

```
(config)# circuit VLAN1
(config-circuit[VLAN1])# redundancy
(config-circuit[VLAN1])# ip address configuration ip address
configuration subnet mask
(config-circuit[VLAN1])# no redirects
(config-circuit[VLAN1])# exit
(config)# ip address internal-address internal-subnet-mask
(config)# exit
(config)# exit
```

Step 7 Configure circuit VLAN2 for the redundancy protocol as follows:

```
(config)# circuit VLAN2
(config…)# ip address master-address redundancy subnet mask
(config…)# redundancy protocol
(config…)# exit
(config…)# exit
```

Step 8 Configure an uplink to the default gateway to trigger failover when the switch is disconnected as follows:

```
(config)# service Upstream
(config…)# ip address default gateway
(config…)# type redundancy-up
(config…)# exit
(config…)# exit
```

Step 9 If you are using an uplink VLAN, configure it now, using the following commands:

```
(config)# circuit VLAN3
(config)# ip address uplink address uplink subnet mask
(config)# exit
(config)# exit
(config)# interface ethernet 2
(config)# bridge vlan 3
(config)# exit
```

Step 10 Exit configuration mode by entering the **exit** command.

```
(config)# exit
```

Step 11 Save changes by entering the **write memory** command as follows:

```
# write memory
```

Step 12 Configure the backup Content Services Switch by repeating Step 1 through Step 11, substituting the backup address for the master address.

Configuring the Catalyst Switch

If you are connecting your Content Engines and redundant Content Services Switches through a Cisco Catalyst switch, you need to configure that device for one- or two-VLAN deployment, matching the configuration of your Content Services Switch.

Refer to the software configuration guide that shipped with the model of the Catalyst switch that you are deploying. For the most part, you can follow the configuration guidelines detailed in the configuration guide. However, see the following sections for specific settings that are required when configuring the Catalyst switch for use with the Cisco Internet CDN Software.

Disabling VLAN Trunk Protocol

We recommend that you disable VLAN Trunk Protocol (VTP) on the Catalyst switch when using Cisco Internet CDN Software. Refer to the section “Disabling VTP (Virtual Transparent Mode)” in the Catalyst switch software configuration guide that shipped with your switch for instructions on disabling VTP.

Creating Multiple VLANs

If you are deploying multiple VLANs on your Content Services Switch (for example, a default VLAN in addition to a separate VLAN for the uplink connection to the uplink subnet), you need to configure your Catalyst switch to recognize those VLANs.

Refer to the section “Configuring VLANs” in the Catalyst switch software configuration guide that shipped with your switch for instructions on creating VLANs and assigning them to ports on your Catalyst switch. The following

example shows a new VLAN, number 500 and named CSVLAN, being created and then assigned to the ports connecting both the Content Services Switch and Content Engines to the Catalyst switch. In Example 3-1:

- VLAN 500 is the default VLAN.
- The master Content Services Switch is connected to module 2, port 13 of the Catalyst switch.
- The backup Content Services Switch is connected to module 2, port 16 of the Catalyst switch.
- Content Engine 4 is connected to module 2, port 14 of the Catalyst switch.
- Content Engine 5 is connected to module 2, port 15 of the Catalyst switch.

Example 3-1 Catalyst Switch Configured for Multiple VLAN Deployment

```
cs-device> enable
cs-device>(enable) set vlan 500 name CSVLAN
cs-device>(enable) set vlan 500 2/13
cs-device>(enable) set vlan 500 2/14
cs-device>(enable) set vlan 500 2/15
cs-device>(enable) set vlan 500 2/16
```

For detailed explanations of Catalyst switch configuration syntax, refer to the software configuration guide that shipped with your Catalyst switch.

CDN Device Wiring Configuration

During the netsetup component of device configuration for your Content Distribution Manager, Content Engines, and Content Routers, you are prompted to assign primary and content IP addresses to one or more of the Ethernet interfaces on the CDN device you are configuring. In order to properly assign your primary and content IP addresses, you must first have decided how you wish to assign these addresses.

Note The Content Distribution Manager is only assigned a primary IP address. It does not use a content IP address.

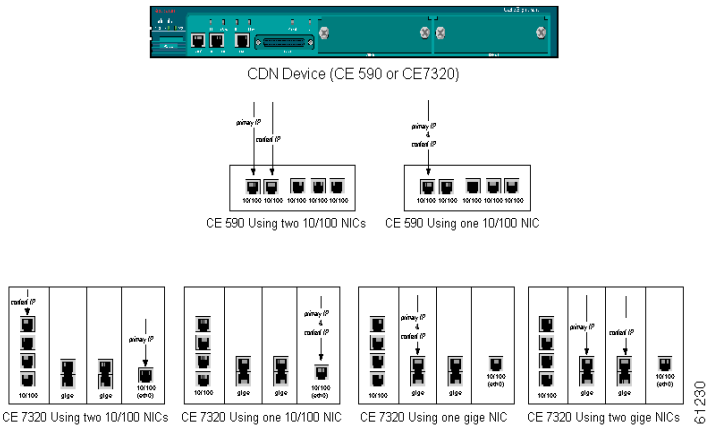
For devices with both 10/100 Ethernet/Fast Ethernet and Gigabit Ethernet interfaces, you are required to use interfaces of only one type. Mixing Ethernet interface types on the same device is not supported by the Cisco Internet CDN Software.

Note that if you will be using the Gigabit Ethernet ports, only Ethernet port 0 is supported. Netsetup will configure your Gigabit Ethernet port as Ethernet port 0 (eth0).

Note You need a connection to the 10/100 eth0 port when running the setup program. After the device reboots with Gigabit Ethernet support, the 10/100 ports are renumbered and are no longer needed.

Figure 3-5 illustrates the supported wiring configuration for CDN devices.

Figure 3-5 Supported Wiring Configurations for CDN Devices



Configuring the Content Distribution Manager

The Content Distribution Manager (CDM) is located at the logical central point of the network to control all operations associated with system policies, network device settings, content control, user interface, billing, and event logging.You may have more than one Content Distribution Manager on your CDN for failover purposes, but only one can serve as the primary Content Distribution Manager at any given time. A Content Distribution Manager is initially designated as primary or standby in the setup program. Subsequently, its status can be changed through the command-line interface. See the "Activating a Warm Standby Content Distribution Manager" section in Chapter 2of the *Cisco Internet CDN Software User Guide* for more information.

The following instructions explain how to configure the Content Distribution Manager(s). For information about configuring other devices, see the "Configuring the Content Services Switch" section on page 3-8, the "Configuring a Content Router" section on page 3-28, and the "Configuring a Content Engine" section on page 3-32.

Note You should configure DNS before you begin configuring the Content Distribution Manager. For your CDN to deliver content, DNS must be configured. For information about configuring DNS, see the "Configuring DNS" section on page 2-2.

To configure the Cisco Internet CDN Software for the Content Distribution Manager, follow these steps:

Step 1 Boot the Content Distribution Manager.

Step 2 Log in as **admin** with the password **default**.

Step 3 At the administrative prompt, enter **setup**.

Step 4 You are prompted to change the default system password. To retain the default password, enter **n**. To change the system password, enter **y**.

Note The new password that you enter is used as a temporary password until you access the Content Distribution Manager user interface and set the real system password.

Step 5 You are prompted to change the HTTP password. To retain the default password, enter **n**. To change the HTTP password, enter **y**.

Note The new password that you enter is used as a temporary password until you access the Content Distribution Manager user interface to set the real HTTP password.

Step 6 Enter **y** if you want the CDM you are configuring to serve as your primary CDM.

Step 7 When prompted by the setup program, enter a meaningful name for the Content Distribution Manager, for example:

```
OurcompanyCDM
```

Note The Content Distribution Manager name *cannot* contain spaces.

Step 8 Enter a meaningful description for the Content Distribution Manager.

Step 9 Enter a fully qualified domain name for the Content Distribution Manager.

Step 10 When you are prompted for the database host name, enter the fully qualified domain name of the Oracle8i database server.

Note Although you can also enter the IP address of the Oracle server at this point, we strongly recommend the use of the fully qualified domain name, which will continue to work even if the Oracle server address changes in the future.

Step 11 To accept the default database listener port number, press **Enter**.

This is the port that will be used by the Content Distribution Manager to communicate with the Oracle database containing Content Distribution Manager data. Alternatively, enter the port number that you specified when you installed the Oracle server listener.

Step 12 Enter the database service name that you specified when you installed the Oracle server listener.

Step 13 Enter a valid Oracle database username.

Note This can be a username created when you set up the Oracle database, or a new account name that you create dynamically. This new account will be confirmed later during the dbsetup portion of the setup program.

Step 14 Enter the database password that you specified when you created the Oracle username. If you are creating a new Oracle database user, enter the new password here.

Step 15 Enter the tablespace used in the Oracle database.

Step 16 Enter the temporary tablespace used in the Oracle database.

Step 17 All the information you entered now appears so that you can confirm it or correct it if needed. If the displayed information is correct, enter **y**. If the displayed information is incorrect, enter **n** and provide the correct information.

Step 18 If this is the first time you are configuring your CDM, the setup program notifies you that it is generating a certificate. This certificate is used to ensure security in interdevice communication.

Step 19 You are prompted to choose whether or not you want to use the default Cisco signature on the certificates. To retain the default signature, enter **y**. To use your company's information as the signature, enter **n**. If you choose **n**, you are prompted to enter the following information about your company: organizational unit, locality, organization, state, and country.

Step 20 The setup program now prompts you to run netsetup to set up the network. Enter **y** to run netsetup.

Note You can run netsetup, which is the network-specific portion of the setup program, at any time by entering **netsetup** at the prompt.

Step 21 A list of Ethernet ports on the Content Distribution Manager is displayed.

Enter the number of the Ethernet interface that you want to use for the primary IP address. For example, to use eth0, the first Ethernet port, for the primary IP address, you would enter:

```
0
```

Note The default Ethernet port is eth0.

Step 22 Enter the fully qualified domain name or IP address of the Content Distribution Manager.

Note We recommend using a domain name instead of the IP address to identify the Content Distribution Manager, because this makes it easier to change the address of the device later.

Step 23 You are asked if you want to use a DHCP server to configure the primary IP address. Perform one of the following:

Warning **Every MAC address on the network must have a single, fixed IP address and fully-qualified domain name associated with it. Do not use your DHCP server if it cannot assign static IP addresses.**

- If your network uses a DHCP server that always assigns the same IP address to a host, then enter **y**.
- If your network does not use a DHCP server, enter **n** and then enter the following information:
  - **Primary IP address**—Specifies the primary IP address assigned to the Content Distribution Manager.
  - **Primary netmask**—Specifies a primary mask that represents your local-area subnet mask.
  - **Gateway**—Specifies the address of a "gateway" device (or router) on the network.

Step 24 If a DHCP server provides the IP address information, press **Enter**. Alternatively, follow these steps:

a. Enter the DNS server IP address for each DNS server.

b. Press **Enter** to save the DNS server address. You are prompted to enter the address on another DNS server.

c. When you have specified the last DNS server, press **Enter**.

The Content Distribution Manager must be able to resolve DNS names, or it will not function correctly.

Step 25 To bring the network online, enter **y**.

Step 26 To register the Content Distribution Manager, enter **y**.

Step 27 You are prompted to set up the Oracle policy database. Enter **y** to launch the dbsetup program.

- If you set up the Oracle database before you began this configuration, the user exists. You are asked if you want to delete the user. Enter **n** to maintain the user.
- If you created a new Oracle user during setup, you are asked to confirm the new user. Enter **y** to confirm the new Oracle user account and password.

Step 28 The dbsetup program now verifies whether database tables exist. You create them now unless you already created the database schema using the script that shipped with the Cisco Internet CDN Software, described in the "Setting Up the Oracle 8i DBMS" section on page 2-6. To create the database tables, enter **y**.

Step 29 The dbsetup program now verifies whether the database tables have been initialized. To initialize the tables, enter **y**.

Step 30 Enter the database administrator username.

Step 31 Enter the database administrator password.

Step 32 When setup is complete, reboot the Content Distribution Manager.

Note When you bring up the Content Distribution Manager user interface in your browser, you must ensure that you have cookies enabled in your browser.

If you have just configured a primary Content Distribution Manager, it will automatically start the software. However, if you have just configured a standby Content Distribution Manager, you will need to launch the software by entering the **control start** command. After this, you must activate the standby Content Distribution Manager from the Resources > Content Distribution Manager page of the primary Content Distribution Manager's user interface.

You can now open the Content Distribution Manager user interface from your web browser by entering the following URL for the Content Distribution Manager:

https://*Name_of_Content_Distribution_Manager*

or by entering the IP address:

https://*IP_address_of_Content_Distribution_Manager*

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

A request for a username and password appears. If you did not change the default HTTP password during configuration, enter the default username **admin** and the default password **default**. If you chose to create a temporary http password during configuration, enter the username **admin** and the HTTP password that you specified.

Note Although you are provided with a default password for the admin account, you should change it as soon as possible after configuration is complete. Refer to the *Cisco Internet CDN Software User Guide* for instructions on changing system passwords.

Configuring a Content Router

Content Routers are deployed at strategic locations within the network and perform much of the work of routing by directing end user requests to a Content Engine that is authorized to store the requested content and is well positioned for that user.

Like all CDN devices, Content Routers must first be configured using the setup program before they can be deployed on a CDN.

For information about configuring other CDN devices, see the "Configuring the Content Distribution Manager" section on page 3-23 and the "Configuring a Content Engine" section on page 3-32.

Note You should configure DNS before you begin configuring Content Routers. In order for your CDN to deliver content, DNS must be configured. For information about configuring DNS, see the "Configuring DNS" section on page 2-2.

To configure the Cisco Internet CDN Software for a Content Router, follow these steps:

Step 1 Boot the Content Router.

Step 2 Log in as **admin** with the password **default**.

Step 3 At the prompt, enter **setup**.

Step 4 Enter a descriptive name for the Content Router.

Note The Content Router name *cannot* contain spaces.

Step 5 Enter a meaningful description for the Content Router.

Step 6 Enter the fully qualified domain name of the Content Distribution Manager with which the Content Router will be associated.

Note We recommend using a domain name instead of the IP address to identify the Content Distribution Manager, because this makes it easier to maintain connectivity should the Content Distribution Manager change addresses later.

Step 7 All the information you entered now appears so that you can confirm it or correct it if needed. If the displayed information is correct, enter **y**. If the displayed information is incorrect, enter **n** and then enter the correct information.

Step 8 The setup program now prompts you to run netsetup for setting up the network. Enter **y** to run netsetup.

Note You can run netsetup, which is the network-specific portion of setup, at any time by entering **netsetup** at the prompt.

Step 9 A list of Ethernet ports on the Content Router is displayed. Enter the number of the Ethernet interface that you want to use for the primary IP address. For example, to use eth0, the first Ethernet port, for the primary IP address, enter **0**.

See the "Primary Versus Content IP Address" section on page 2-10 for a discussion of primary versus content IP addresses.

Step 10 Enter the fully qualified domain name or IP address of the Content Router.

Note We recommend using a domain name instead of the IP address to identify the Content Router whenever possible. Using the domain name makes it possible to preserve connectivity with the Content Router if its network address changes.

Step 11 You are asked if you want to use a DHCP server to configure the primary IP address.

Warning **Every MAC address on the network must have a single, fixed IP address and fully-qualified domain name associated with it. Do not use your DHCP server if it cannot assign static IP addresses.**

Perform one of the following:

- If your network uses a DHCP server that always assigns the same IP address to a host, then enter **y**.
- If your network does not use a DHCP server, enter **n** and then enter the following information:
  - **Primary IP address**—Specifies the primary IP address assigned to the Content Router.
  - **Primary Netmask**—Specifies a primary mask that represents your local-area subnet mask.
  - **Gateway**—Specifies the address of a "gateway" device (or router) on the network.

Step 12 You are asked whether you want to configure the content IP address now, or do it later using the Content Distribution Manager graphical user interface. Perform one of the following actions:

- To configure the content IP address now, enter **y**. Then do the following:
  - Enter the content IP DNS name that will be used by the Content Router. You are notified when the DNS successfully resolves to an IP address.

Note The content IP can be changed later using the Content Distribution Manager graphical user interface. However, you will not be able to change the content IP address using netsetup after this initial configuration.

  - Enter the content netmask that will be used by the Content Router. You can either specify a netmask or press **Enter** to accept the default netmask that appears in square brackets.

- To configure the content IP address later, enter **n**. You can configure the content IP address later using the Content Distribution Manager graphical user interface.

Step 13 Perform one of the following actions:

- If the DHCP server provides the DNS information, press **Enter**.
- If the DHCP server does not provide DNS information, enter the DNS server IP address for each DNS server, and when you have specified the last DNS server, press **Enter**.

The Content Router must be able to resolve DNS names, or it will not function correctly.

Step 14 To bring the network online, enter **y**.

Step 15 To register the Content Router, enter **y**.

Step 16 If this is the first time you are configuring your Content Router, the setup program notifies you that it is generating a certificate. This certificate is used to ensure security in inter device communication. You are prompted to choose whether or not you want to use the default Cisco signature on the certificates. Perform one of the following actions:

- To retain the default signature, enter **y**.
- To use your company's information as the signature, enter **n**. If you choose **n**, you are prompted to enter the following information about your company: organizational unit, locality, organization, state, and country.

Step 17 At the prompt, reboot the Content Router.

Your Content Router is now configured and is ready to use with the CDN.

Note Before it can begin routing content to other CDN devices, the Content Router must first be activated. Refer to the *Cisco Internet CDN Software User Guide* for instructions on activating Content Routers from the Content Distribution Manager graphical user interface.

Configuring a Content Engine

Content Engines contain the actual cached content that is being delivered to end users. Content Engines are responsible for storing, or *pre-positioning*, video-on-demand (VOD) content, and for delivering content to end users. Content Engines provide access to content through HTTP, RealMedia, Windows Media, and QuickTime format files.They also participate in routing under the direction of the Content Routers.

Note If you are deploying supernodes on your CDN and intend to make this Content Engine part of a supernode, make sure that you have configured your Content Services Switch before configuring the Content Engine that will be assigned to it. Refer to the *Cisco Internet CDN Software User Guide* for instructions on creating and configuring supernodes.

Note You should configure DNS before you begin configuring the Content Engines. For your CDN to deliver content, DNS must be configured. For information about configuring DNS, see the "Configuring DNS" section on page 2-2.

Note Even if you will be configuring your Content Engine to assign the primary and content IP addresses to a Gigabit Ethernet port, you are still required to connect to the device through a 10/100-MB

Ethernet/Fast Ethernet port during initial setup and configuration. During setup, you indicate which Gigabit Ethernet ports you wish to use for each address. You must restart the device after setup, after which you will be able to connect to the Content Engine using the Gigabit Ethernet ports you selected.

For information about configuring other CDN devices, see the "Configuring the Content Distribution Manager" section on page 3-23 and the "Configuring a Content Router" section on page 3-28.

Configuring a Standalone Content Engine

To configure a standalone Content Engine, follow these steps:

Step 1 Boot the Content Engine.

Step 2 Log in as **admin** with the password **default**.

Step 3 At the prompt, enter **setup**.

Step 4 You are prompted to change the default system password. To retain the default password, enter **n**. To change the system password, enter **y**.

Note The new password that you enter is used as a temporary password until you set the real system password using the Content Distribution Manager user interface.

Step 5 You are prompted to change the HTTP password. To retain the default password, enter **n**. To change the HTTP password, enter **y**.

Note The new password that you enter is used as a temporary password until you set the real HTTP password using the Content Distribution Manager user interface.

Step 6 You are prompted to confirm whether or not the Content Engine you are configuring is a member of a supernode. Enter **n**.

Step 7 Enter a meaningful name for the Content Engine.

Note The Content Engine name *cannot* contain spaces.

Step 8 Enter a meaningful description for the Content Engine.

Step 9 Enter the fully qualified domain name of the Content Distribution Manager with which this Content Engine will be associated.

Note We recommend using a domain name instead of the IP address to identify the Content Distribution Manager, because this makes it easier to maintain connectivity should the Content Distribution Manager address change later.

Step 10 All the information you entered now appears so that you can confirm it or correct it if needed. Perform one of the following actions:

- If the displayed information is correct, enter **y**.
- If the displayed information is incorrect, enter **n**. You have the opportunity to enter the correct information.

Step 11 The setup program now prompts you to run netsetup to set up the network. Enter **y** to run netsetup.

Step 12 Perform one of the following actions:

- If your Content Engine shipped with both 10/100-MB Ethernet/Fast Ethernet and Gigabit Ethernet cards installed, you are prompted to choose which type of card you wish to use.
  - Enter **1** to have the Content Engine use the 10/100-MB Ethernet/Fast Ethernet cards.
  - Enter **2** to have the Content Engine use the Gigabit Ethernet cards.

  Note Only one port (eth0) is supported for Gigabit Ethernet cards. For the Gigabit Ethernet port to function, you must reboot the Content Engine after setting it up.

- If your Content Engine did not ship with two types of Ethernet cards, proceed to the next step.

Step 13 Enter the fully qualified domain name of the Content Engine.

Step 14 You are asked if you want to use a DHCP server to configure the primary IP address.

Warning **Every MAC address on the network must have a single, fixed IP address and fully-qualified domain name associated with it. Do not use your DHCP server if it cannot assign static IP addresses.**

- If your network uses a DHCP server that always assigns the same IP address to a host, then enter **y**.
- If your network does not use a DHCP server, enter **n** and then enter the following information:
  - **Primary IP address**—Specifies the primary IP address assigned to the Content Engine.
  - **Primary netmask**—Specifies a primary mask that represents your local-area subnet mask.
  - **Gateway**—Specifies the address of a "gateway" device (or router) on the network.

Step 15 If your Content Engine contains more than one Ethernet card, you are prompted to choose how you want those cards allocated:

- Enter **1** to use a single Ethernet port for both the primary IP address and the content IP address.
- Enter **2** to use one Ethernet port for the primary IP address and one Ethernet port for the content IP address.

Step 16 Perform one of the following actions:

- To configure the Content Engine content IP address now, enter **y** and then enter the content IP DNS name and the content netmask when prompted.You are given a default content netmask in square brackets. You can accept this by pressing **Enter**, or you can specify a different netmask.
- To configure the Content Engine content IP address later using the Content Distribution Manager graphical user interface, enter **n**

Step 17 To bring the network online, enter **y**.

Step 18 To register the Content Engine, enter **y**.

Step 19 If this is the first time you are configuring your Content Engine, the setup program notifies you that it is generating a certificate. This certificate is used to ensure security in interdevice communication.

Step 20 You are prompted to choose whether or not you want to use the default Cisco signature on the certificates. Perform one of the following actions:

- To retain the default signature, enter **y**.
- To use your company's information as the signature, enter **n**. If you choose **n**, you are prompted to enter the following information about your company: organizational unit, locality, organization, state, and country.

Step 21 At the prompt, reboot the Content Engine.

Step 22 Your Content Engine is now configured and is ready to use with the CDN.

Note Before it can begin receiving content to stream, however, it must first be activated. Refer to the *Cisco Internet CDN Software User Guide* for instructions on activating Content Engines from the Content Distribution Manager user interface.

Configuring a Content Engine As Part of a Supernode

To configure a Content Engine as part of a supernode, follow these steps:

Step 1 Boot the Content Engine.

Step 2 Log in as **admin** with the password **default**.

Step 3 At the prompt, enter **setup**.

Step 4 You are prompted to change the default system password. To retain the default password, enter **n**. To change the system password, enter **y**.

Note The new password that you enter is used as a temporary password until you set the real system password using the Content Distribution Manager user interface.

Step 5 You are prompted to change the HTTP password. To retain the default password, enter **n**. To change the HTTP password, enter **y**.

Note The new password that you enter is used as a temporary password until you set the real HTTP password using the Content Distribution Manager user interface.

Step 6 You are prompted to confirm whether or not the Content Engine you are configuring is a member of a supernode. Enter **y**.

Step 7 Enter a meaningful name for the Content Engine.

Note The Content Engine name *cannot* contain spaces.

Step 8 Enter a meaningful description for the Content Engine.

Step 9 Enter the fully qualified domain name of the Content Distribution Manager with which this Content Engine will be associated.

Note We recommend using a domain name instead of the IP address to identify the Content Distribution Manager, because this makes it easier to maintain connectivity should the Content Distribution Manager address change later.

Step 10 All the information you entered now appears so that you can confirm it or correct it if needed. Perform one of the following actions:

- If the displayed information is correct, enter **y**.
- If the displayed information is incorrect, enter **n**. You have the opportunity to enter the correct information.

Step 11 The setup program now prompts you to run netsetup to set up the network. Enter **y** to run netsetup.

Step 12 Perform one of the following actions:

- If your Content Engine shipped with both 10/100-MB Ethernet/Fast Ethernet and Gigabit Ethernet cards installed, you are prompted to choose which type of card you wish to use.

  - Enter **1** to have the Content Engine use the 10/100-MB Ethernet/Fast Ethernet cards.
  - Enter **2** to have the Content Engine use the Gigabit Ethernet cards.

Note Only one port (eth0) is supported for Gigabit Ethernet cards. For the Gigabit Ethernet port to function, you must reboot the Content Engine after setting it up.

- If your Content Engine did not ship with two types of Ethernet cards, proceed to the next step.

Step 13 Enter the configuration IP address of the Content Services Switch that this Content Engine will be associated with. The configuration IP address will be the gateway for this Content Engine.

Step 14 Enter the fully qualified domain name of the Content Engine.

Step 15 Enter the primary IP address assigned to the Content Engine.

Step 16 Enter a primary netmask that represents your local-area subnet mask.

Step 17 If your Content Engine contains more than one Ethernet card, you are prompted to choose how you want those cards allocated:

- Enter **1** to use a single Ethernet port for both the primary IP address and the content IP address.
- Enter **2** to use one Ethernet port for the primary IP address and one Ethernet port for the content IP address.

Step 18 Perform one of the following actions:

- If the DHCP server provides the DNS information, press **Enter**.
- If the DHCP server does not provide DNS information, enter the DNS server IP address for each DNS server, and when you have specified the last DNS server, press **Enter**.

Note The Content Engine must be able to resolve DNS names or it will not function correctly.

Step 19 To bring the network online, enter **y**.

Step 20 To register the Content Engine, enter **y**.

Step 21 If this is the first time you are configuring your Content Engine, the setup program notifies you that it is generating a certificate. This certificate is used to ensure security in interdevice communication.

Step 22 You are prompted to choose whether or not you want to use the default Cisco signature on the certificates. Perform one of the following actions:

- To retain the default signature, enter **y**.
- To use your company's information as the signature, enter **n**. If you choose **n**, you are prompted to enter the following information about your company: organizational unit, locality, organization, state, and country.

Step 23 At the prompt, reboot the Content Engine.

Your Content Engine is now configured and is ready to use with the CDN. Before it can begin receiving content to distribute, however, it must first be activated. Refer to the *Cisco Internet CDN Software User Guide* for instructions on activating Content Engines from the Content Distribution Manager user interface.

Configuring a Storage Array

The Cisco Storage Array 6 and Cisco Storage Array 12 are rack-mounted hard disk arrays that provide additional storage capacity to Cisco Content Engines. Once you have added a Storage Array to a Content Engine, there is no need to format or partition the drives.

The Cisco Storage Array 6 is compatible with a Content Engine 590, and the Cisco Storage Array 12 is compatible with a Content Engine 7320. Configurations that have multiple Storage Arrays cabled together or multiple Content Engines cabled to a single Storage Array are not supported.

To add a Storage Array to your Content Engine:

Step 1 Verify from the Resources > Content Engines page of the Content Distribution Manager user interface that the Content Engine is online.

Step 2 Attach a SCSI cable to the first SCSI bus connector of the Content Engine.

Note Make sure to tighten the jackscrews on the SCSI cable.

Step 3 Attach the other end of the SCSI cable to your Storage Array.

- If you are using a Storage Array 6, connect the cable to either the SCSI 0 or SCSI 1 port on the I/O module on the rear of the Storage Array.
- If you are using a Storage Array 12, connect the cable to the SCSI Management Module I/O connector on the rear of the Storage Array.

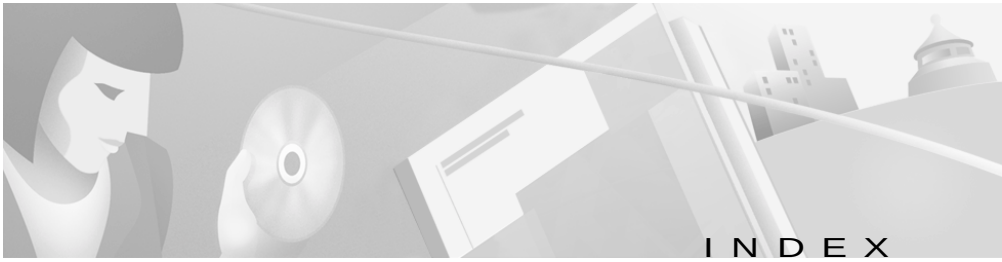
Step 4 Move the Storage Array's power switch to the on position.

Note You will not see the additional storage capacity registered in any way on the CDM user interface until you reboot the Content Engine.

Step 5 Enter the command-line interface of the Content Engine and execute the **reboot** command. For more information on using the command-line interface, refer to the *Cisco Internet CDN Software Command Reference Version 2.1*.

It takes several minutes for the Content Engine to come online on the CDM user interface. The total disk space figure on the Resources > Content Engines page now reflects the additional storage capacity. You can now configure as much of the total capacity for prepositioning as you would like. The following equation expresses the amount of disk space available for caching after you add a Storage Array.

(Storage capacity used for caching) = (Additional storage capacity not allocated for prepositioned content) — (overhead)



Numerics

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W

Z