



Cisco Content Services Switch Getting Started Guide

Software Versions 8.10 and 8.20
November 2006

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

Text Part Number: OL-7992-01



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0609R)

Cisco Content Services Switch Getting Started Guide

Copyright © 2006 Cisco Systems, Inc. All rights reserved.



Preface xi

- Audience **xii**
- How to Use This Guide **xii**
- Related Documentation **xiii**
- Symbols and Conventions **xvi**
- Obtaining Documentation **xviii**
 - Cisco.com **xviii**
 - Product Documentation DVD **xviii**
 - Ordering Documentation **xix**
- Documentation Feedback **xix**
- Cisco Product Security Overview **xix**
 - Reporting Security Problems in Cisco Products **xx**
- Product Alerts and Field Notices **xxi**
- Obtaining Technical Assistance **xxi**
 - Cisco Technical Support & Documentation Website **xxi**
 - Submitting a Service Request **xxii**
 - Definitions of Service Request Severity **xxiii**
- Obtaining Additional Publications and Information **xxiv**

CHAPTER 1

Booting, Logging In, and Getting Started 1-1

- Booting and Logging In Quick Start **1-2**
- Booting the CSS for the First Time **1-3**
 - Entering Your Software License Key **1-3**
 - Configuring the Ethernet Management Port **1-4**

- Changing the Default Username and Password **1-5**
- Password Protecting the Offline DM Menu **1-6**
- Booting the CSS on a Routine Basis **1-7**
- Logging in to the CSS **1-9**
- Using the Configuration Script **1-11**
 - Configuring Layer 3 Load Balancing **1-14**
 - Configuring Layer 5 Load Balancing **1-16**
 - Configuring Proxy Cache **1-18**
 - Configuring Transparent Cache **1-20**
- Rebooting the CSS **1-23**
- Shutting Down the CSS **1-24**
- Where to Go Next **1-25**

CHAPTER 2**Configuring CSS Basics 2-1**

- Initial Setup Quick Start **2-2**
- Changing the Administrative Username and Password **2-5**
- Creating Usernames and Passwords **2-6**
- Configuring the Ethernet Management Port **2-9**
 - Configuring an IP Address and Subnet Mask for the Ethernet Management Port **2-11**
 - Configuring Static Routes for the Ethernet Management Port **2-12**
 - Configuring a Default Gateway for the Ethernet Management Port **2-13**
 - Discarding ICMP Redirects on the Ethernet Management Port **2-13**
 - Shutting Down the Ethernet Management Port **2-15**
- Configuring an IP Route **2-16**
- Configuring the Date, Time, and Time Zone **2-17**
 - Setting the Date **2-17**
 - Setting the European Date **2-18**
 - Setting the Time **2-18**

- Setting the Time Zone **2-18**
- Configuring Daylight Saving Time **2-20**
 - Configuring DST to Occur Every Year **2-21**
 - Configuring DST for Only One Year **2-22**
 - Disabling DST on the CSS **2-23**
- Showing the Date and Time **2-23**
- Synchronizing the CSS with an SNTP Server **2-25**
 - Configuring a Primary or Secondary SNTP Server **2-26**
 - Configuring the Poll Interval for the SNTP Server **2-27**
 - Showing SNTP Configuration Information **2-28**
- Configuring a Host Name **2-29**
- Where to Go Next **2-29**

CHAPTER 3**Configuring the Domain Name Service 3-1**

- Specifying a Primary DNS Server **3-1**
- Using DNS Resolve **3-2**
- Specifying a Secondary DNS Server **3-2**
- Specifying a DNS Suffix **3-2**
- Specifying UDP Traffic on the DNS Server Port **3-3**
- Where to Go Next **3-3**

CHAPTER 4**Configuring Sticky Cookies 4-1**

- Sticky Overview **4-1**
- Advanced Load-Balancing Method Using Cookies **4-2**
 - Sticky Based on a Configured String in an HTTP Cookie Header **4-3**
 - Sticky Based on a Cookie in a URL **4-5**
 - Sticky Based on a Cookie in the HTTP Header or URL **4-6**
- Where to Go Next **4-6**

CHAPTER 5

Where to Go Next 5-1

CSS Task Topic List **5-1**

Comprehensive CSS Documentation List **5-24**

Cisco Content Services Switch Administration Guide **5-25**

Cisco Content Services Switch Routing and Bridging Configuration Guide **5-29**

Cisco Content Services Switch Content Load-Balancing Configuration Guide **5-33**

Cisco Content Services Switch Global Server Load-Balancing Configuration Guide **5-39**

Cisco Content Services Switch Redundancy Configuration Guide **5-41**

Cisco Content Services Switch Security Configuration Guide **5-43**

Cisco Content Services Switch SSL Configuration Guide **5-44**

APPENDIX A

Troubleshooting the Boot Process A-1

Diagnostic Tests for Hardware and Error Messages **A-2**

Offline DM Verification of the Boot Configuration Record and Disk **A-6**

CSS 11501 Boot and Verification **A-6**

CSS 11503 and CSS 11506 Boot and Module Verification **A-7**

INDEX



Figure 2-1

CSS Directory Access Privileges **2-8**



<i>Table 1-1</i>	Boot and Login Quick Start	1-2
<i>Table 1-2</i>	Status LEDs Boot Definitions	1-8
<i>Table 1-3</i>	Configuration Script Menu Options	1-13
<i>Table 2-1</i>	Initial Setup Quick Start	2-2
<i>Table 2-2</i>	Field Descriptions for the show clock Command	2-23
<i>Table 2-3</i>	Field Descriptions for the show snmp global Command	2-28
<i>Table 5-1</i>	Administration and Configuration Task Topic List	5-1
<i>Table 5-2</i>	Cisco Content Services Switch Administration Guide	5-25
<i>Table 5-3</i>	Cisco Content Services Switch Routing and Bridging Configuration Guide	5-29
<i>Table 5-4</i>	Cisco Content Services Switch Content Load-Balancing Configuration Guide	5-33
<i>Table 5-5</i>	Cisco Content Services Switch Global Server Load-Balancing Configuration Guide	5-39
<i>Table 5-6</i>	Cisco Content Services Switch Redundancy Configuration Guide	5-41
<i>Table 5-7</i>	Cisco Content Services Switch Security Configuration Guide	5-43
<i>Table 5-8</i>	Cisco Content Services Switch SSL Configuration Guide	5-44
<i>Table A-1</i>	Fields in the Diagnostic Monitor Error Message	A-3



Preface

This guide provides instructions for basic administration of the Cisco 11500 Series Content Services Switches (CSS). It describes how to perform tasks to get the CSS started, including logging in to the CSS. For information on managing and upgrading your CSS software, refer to the *Cisco Content Services Switch Administration Guide*. Information in this guide applies to all CSS models except where noted.

The CSS software is available in a Standard or optional Enhanced feature set. The Enhanced feature set contains all of the Standard feature set and also includes Network Address Translation (NAT) Peering, Domain Name Service (DNS), Demand-Based Content Replication (Dynamic Hot Content Overflow), Content Staging and Replication, and Network Proximity DNS. Proximity Database and Secure Management, which includes Secure Shell Host and SSL strong encryption, are optional features.

This preface contains the following major sections:

- Audience
- How to Use This Guide
- Related Documentation
- Symbols and Conventions
- Obtaining Documentation
- Documentation Feedback
- Cisco Product Security Overview
- Product Alerts and Field Notices

- Obtaining Technical Assistance
- Obtaining Additional Publications and Information

Audience

This guide is intended for the following trained and qualified service personnel who are responsible for configuring the CSS:

- Web master
- System administrator
- System operator

How to Use This Guide

This guide is organized as follows:

Chapter	Description
Chapter 1, Booting, Logging In, and Getting Started	Provides information to power on and boot the CSS for the first time, log in to the CSS, and boot the CSS on a routine basis.
Chapter 2, Configuring CSS Basics	Provides information to configure the username and password, Ethernet management port, static IP routes, and the date and time including daylight savings time (summer time) and SNTP.
Chapter 3, Configuring the Domain Name Service	Provides information to configure the Domain Name Server for hostname resolution.
Chapter 4, Configuring Sticky Cookies	Provides a CSS sticky overview and examples of configuring sticky cookies.

Chapter	Description
Chapter 5, Where to Go Next	Provides content information for the CSS documentation to help you find administration and configuration tasks.
Appendix A, Troubleshooting the Boot Process	Provides information to troubleshoot the boot process for the Cisco 11500 series CSS.

Related Documentation

In addition to this document, the CSS documentation set includes the following:

Document Title	Description
<i>Release Note for the Cisco 11500 Series Content Services Switch</i>	This release note provides information on operating considerations, caveats, and command-line interface (CLI) commands for the Cisco 11500 series CSS.
<i>Cisco 11500 Series Content Services Switch Hardware Installation Guide</i>	This guide provides information for installing, cabling, and powering the Cisco 11500 series CSS. In addition, this guide provides information about CSS specifications, cable pinouts, and hardware troubleshooting.

Document Title	Description
<i>Cisco Content Services Switch Administration Guide</i>	<p>This guide describes how to perform administrative tasks on the CSS, including upgrading your CSS software and configuring the following:</p> <ul style="list-style-type: none"> • Logging, including displaying log messages and interpreting sys.log messages • User profile and CSS parameters • SNMP • RMON • XML documents to configure the CSS • CSS scripting language • Offline Diagnostic Monitor (Offline DM) menu
<i>Cisco Content Services Switch Routing and Bridging Configuration Guide</i>	<p>This guide describes how to perform routing and bridging configuration tasks on the CSS, including:</p> <ul style="list-style-type: none"> • Management ports, interfaces, and circuits • Spanning-tree bridging • Address Resolution Protocol (ARP) • Routing Information Protocol (RIP) • Internet Protocol (IP) • Open Shortest Path First (OSPF) protocol • Cisco Discovery Protocol (CDP) • Dynamic Host Configuration Protocol (DHCP) relay agent

Document Title	Description
<i>Cisco Content Services Switch Content Load-Balancing Configuration Guide</i>	<p>This guide describes how to perform CSS content load-balancing configuration tasks, including:</p> <ul style="list-style-type: none">• Flow and port mapping• Services• Service, global, and script keepalives• Source groups• Loads for services• Server/Application State Protocol (SASP)• Dynamic Feedback Protocol (DFP)• Owners• Content rules• Sticky parameters• HTTP header load balancing• Content caching• Content replication
<i>Cisco Content Services Switch Global Server Load-Balancing Configuration Guide</i>	<p>This guide describes how to perform CSS global load-balancing configuration tasks, including:</p> <ul style="list-style-type: none">• Domain Name System (DNS)• DNS Sticky• Content Routing Agent• Client-Side Accelerator• Network proximity
<i>Cisco Content Services Switch Redundancy Configuration Guide</i>	<p>This guide describes how to perform CSS redundancy configuration tasks, including:</p> <ul style="list-style-type: none">• VIP and virtual interface redundancy• Adaptive session redundancy• Box-to-box redundancy

Document Title	Description
<i>Cisco Content Services Switch Security Configuration Guide</i>	This guide describes how to perform CSS security configuration tasks, including: <ul style="list-style-type: none"> • Controlling access to the CSS • Secure Shell Daemon protocol • Radius • TACACS+ • Firewall load balancing
<i>Cisco Content Services Switch SSL Configuration Guide</i>	This guide describes how to perform CSS SSL configuration tasks, including: <ul style="list-style-type: none"> • SSL certificate and keys • SSL termination • Back-end SSL • SSL initiation • HTTP data compression
<i>Cisco Content Services Switch Command Reference</i>	This reference provides an alphabetical list of all CLI commands including syntax, options, and related commands.

Symbols and Conventions

This guide uses the following symbols and conventions to identify different types of information.



Caution

A caution means that a specific action you take could cause a loss of data or adversely impact use of the equipment.



Warning

A warning describes an action that could cause you physical harm or damage the equipment.

**Note**

A note provides important related information, reminders, and recommendations.

Bold text indicates a command in a paragraph.

Courier text indicates text that appears on a command line, including the CLI prompt.

Courier bold text indicates commands and text you enter in a command line.

Italic text indicates the first occurrence of a new term, book title, emphasized text, and variables for which you supply values.

1. A numbered list indicates that the order of the list items is important.
 - a. An alphabetical list indicates that the order of the secondary list items is important.
- A bulleted list indicates that the order of the list topics is unimportant.
 - An indented list indicates that the order of the list subtopics is unimportant.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

<http://www.cisco.com/univercd/home/home.htm>

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

<http://www.cisco.com/go/marketplace/docstore>

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

<http://www.cisco.com/go/marketplace/docstore>

If you do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Technical Support & Documentation site area by entering your comments in the feedback form available in every online document.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to do the following:

- Report security vulnerabilities in Cisco products
- Obtain assistance with security incidents that involve Cisco products
- Register to receive security information from Cisco

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only — security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For nonemergencies — psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive Cisco Product Alerts and Cisco Field Notices by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. (To register as a Cisco.com user, go to this URL:

<http://tools.cisco.com/RPF/register/register.do>) Registered users can access the tool at this URL:

<http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en>

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

**Note**

Use the **Cisco Product Identification Tool** to locate your product serial number before submitting a request for service online or by phone. You can access this tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This tool offers three search options: by product ID or model name; by tree view; or, for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

**Tip**

Displaying and Searching on Cisco.com

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing F5.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. On the Cisco.com home page, click the **Advanced Search** link under the Search box and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended

solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411

Australia: 1 800 805 227

EMEA: +32 2 704 55 55

USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

<http://www.cisco.com/offer/subscribe>

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:

<http://www.cisco.com/go/guide>

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- Cisco Press publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:

<http://www.cisco.com/ipj>

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

<http://www.cisco.com/en/US/products/index.html>

- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:
<http://www.cisco.com/discuss/networking>
- “What’s New in Cisco Documentation” is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of “What’s New in Cisco Documentation” at this URL:
<http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm>
- World-class networking training is available from Cisco. You can view current offerings at this URL:
<http://www.cisco.com/en/US/learning/index.html>



Booting, Logging In, and Getting Started

This chapter describes how to boot the CSS for the first time and on a routine basis, and how to log in. It also covers using the configuration script, which initiates automatically when you log in *and* the CSS does not detect an existing startup-config file. Information in this chapter applies to all CSS models, except where noted.

This chapter contains the following major sections:

- Booting and Logging In Quick Start
- Booting the CSS on a Routine Basis
- Logging in to the CSS
- Using the Configuration Script
- Rebooting the CSS
- Shutting Down the CSS

Booting and Logging In Quick Start

Table 1-1 is a quick start configuration table designed to simplify the CSS boot and login process. For a complete description of each process, see the sections following Table 1-1.

Table 1-1 Boot and Login Quick Start

Task and Command Example

1. When booting the CSS for the first time, the CSS performs hardware initialization and power-on diagnostics, and then prompts you to:
 - Configure the IP address, subnet mask, and default gateway for the Ethernet management port
 - Change the default administrative login name (**admin**) and password (**system**)
 - Password-protect the Offline Diagnostic Monitor (Offline DM) menu
2. When you power up the CSS on a routine basis, the boot process:
 - Displays the software version and build number
 - Performs hardware initialization and power-on self tests
 - Provides access to the Offline DM menu
 - Prompts you to log in to the CSS
3. Log in to the CSS using the default administrative username (**admin**) and password (**system**), or the username and password assigned to you.
4. When you log in to the CSS and it does not detect an existing startup-config file, the CSS automatically initiates the configuration script. During the running of the configuration script, the CSS prompts you to enter the following information:
 - IP address and subnet mask for circuit VLAN1 (all interfaces are assigned to VLAN1 by default)
 - IP address for the default gateway
 - IP addresses for the servers
 - Virtual IP address (VIP) for the content rule

See the “Using the Configuration Script” section for details.

Booting the CSS for the First Time

Upon bootup, the CSS initially:

- Performs hardware initialization and power-on diagnostics (as described in the “Booting the CSS on a Routine Basis” section)
- Prompts you to:
 - Configure the IP address, subnet mask, and default gateway for the Ethernet management port, used for CSS configuration and Ethernet management only; this port does not route traffic
 - Change the default administrative login name (**admin**) and password (**system**)
 - Password-protect the Offline Diagnostic Monitor (Offline DM) menu

This sections includes the following procedures:

- Entering Your Software License Key
- Configuring the Ethernet Management Port
- Changing the Default Username and Password
- Password Protecting the Offline DM Menu

Entering Your Software License Key

When the CSS completes hardware initialization and power-on diagnostics, the CSS prompts you to accept the license agreement. You must accept the license agreement or you cannot log in to the CSS.

If, during the initial CSS order placement, you purchased the Enhanced feature set, the Secure Management option (which includes Secure Shell Host and SSL strong encryption), or the Proximity Database software option, locate the software Claim Certificate in the accessory kit. Follow the instructions on the Claim Certificate to obtain a license key from Cisco Systems for the additional software feature.

After you receive the software license key, use the **license** command to enter the license key. At the prompt, enter the license key. To install the Enhanced feature set license key:

1. Log in to the CSS and enter the **license** command.

```
# license
```

2. Enter the 12-digit Enhanced feature set software license key. For example:

```
Enter the Software License Key (q to quit): nnnnnnnnnnnn
```

The Enhanced feature set license key is now properly installed and the feature set is activated.

**Note**

After you enter the software license key for the Proximity Database software option, you must reboot the CSS for the license key to take effect.

Configuring the Ethernet Management Port

Once you enter a valid license key at the boot prompt, the CSS displays the following message and prompt:

```
Use the Ethernet management port IP address to access the Content
Services Switch for configuration and management only. This port does
not route traffic and is not associated with VLAN circuits.
```

```
The current address setting (0.0.0.0) disables the Ethernet Management
port.
```

```
Do you wish to configure a valid address for the Ethernet management
port [y/n]?
```

Enter one of the following:

- **y** to configure an IP address, subnet mask, and default gateway for the Ethernet management port. The CSS prompts you for an IP address, a subnet mask, then a default gateway. You must enter a valid IP address or the CSS repeats the prompt until you do.

```
Enter IP Address [0.0.0.0]:  
Enter Subnet Mask [0.0.0.0]:  
Enter Default Gateway [0.0.0.0]:
```



Note The Ethernet management port IP address must be on a different subnet from any other CSS VLAN circuit subnet. If you do not make this IP address unique, you will not be able to access the port.

- **n** to accept the default IP address (0.0.0.0), subnet mask (0.0.0.0), and gateway (0.0.0.0) and to disable the port. The CSS does not prompt you for an IP address, subnet mask, and default gateway.

The Ethernet management port default IP address of 0.0.0.0 disables the Ethernet management port. To enable the Ethernet management port, specify the **ip address** command in boot mode (see Chapter 2, Configuring CSS Basics) or use the Offline DM menu (refer to the *Cisco Content Services Switch Administration Guide*).

Changing the Default Username and Password

The CSS allows you to change the default username and password. We recommend that you change them to safeguard the CSS against unauthorized logins.

Access to this device is allowed using the default username and password. For enhanced security we recommend that you change the defaults. Do you want to change the defaults now (yes,no):

Enter one of the following:

- **yes** to change the username and password. The CSS prompts you for the following information and password confirmation.

```
Enter <administrator> username:  
Enter <administrator> password:  
Confirm <administrator> password:
```

- **no** to keep the default username and password.

To change the default username and password from the CLI, see Chapter 2, Configuring CSS Basics, for details.

Password Protecting the Offline DM Menu

The CSS prompts you to password-protect the Offline DM menu.

```
Set Password Protection for Offline Diagnostic Monitor menu (yes,no)
```



Caution

Use care when password protecting the Offline DM menu and ensure that you write down the new password. If you lose the new password, it cannot be recovered and you will be unable to access the Offline DM Main menu. The only solution, at that point, is to contact the Cisco Technical Assistance Center (TAC) at 1-800-553-2447 or 1-408-526-7209. You can also e-mail TAC at tac@cisco.com.

Enter one of the following:

- **yes** to password protect the Offline DM menu. When you password protect the Offline DM menu, you need to enter the administrative username and password each time you access the menu.

```
The administrative username and password are required to access
the Offline Diagnostic Monitor menu.
Initializing the disk.....OK
```

Refer to the *Cisco Content Services Switch Administration Guide* for information on the Offline DM menu options.

- **no** to disable password protection on the Offline DM menu.

The CSS prompts you to access the Offline DM menu.

```
Would you like to access the Offline Diagnostic Monitor? (Y <cr>)
```

Enter **y** to access the Offline DM menu. If you do not wish to access the Offline DM menu after seeing this message, wait for the CSS to boot.

Booting the CSS on a Routine Basis

When you power up a CSS, the boot process:

- Displays the software version and build number
- Performs hardware initialization and power-on self tests
- Provides access to the Offline DM menu
- Prompts you to log in to the CSS

The duration of the boot process depends on the CSS startup configuration and, with the CSS 11503 and CSS 11506, the number of modules in the chassis.

When you boot the CSS, it initializes the hardware and performs power-on self tests. The CSS displays the following messages (shown for the CSS 11503 and CSS 11506):

```
Locked boot flash.  
Validating operational boot flash, please wait...  
Operational boot flash valid. Jumping to operational boot flash.  
Copyright 2002(c), Cisco Systems, Inc.
```

```
Operational boot flash.  
Attaching interrupt handlers...Done.  
Master SCM.  
Built Jun 22 2002 @ 15:14:20  
Version x.xx Build xx
```

**Note**

After the CSS begins to boot (approximately 15 seconds) the CSS allows you to access the Offline DM menu. The Offline DM Main menu allows you to set the boot configuration, display the boot configuration, select Advanced Options, or reboot the system. Refer to the *Cisco Content Services Switch Administration Guide* for detailed information on using Offline DM.

The hardware then goes through a series of power-on self tests. The asterisks that appear indicate the completion of each test.

```
Press <ESC> to enter the Diagnostic Monitor
* * * * *
Ran 1 times, x tests. Detected 0 errors.
```

During the power-on self tests, the Status LEDs blink and change color to indicate the stages of the boot process. The left Status LED is bicolor, green or red. The right Status LED is amber.

The Ethernet connectors on the CSS 11501 and the 8- and 16-port Fast Ethernet Modules on the CSS 11503 or CSS 11506 do not contain Status LEDs. Each Ethernet connector has Link and Duplex LEDs to indicate the state of the connection.

Table 1-2 defines the boot states and the blinking patterns of the Status LEDs.

Table 1-2 Status LEDs Boot Definitions

State Sequence		LED Color	LED State
1.	The CSS powers up, scans flash, and performs a power-on self test.	Amber	Fast blink
	The CSS powers on and a self test detects an error.	Red	Solid
2.	The CSS 11501 or a module in the CSS 11503 or CSS 11506 is offline and active.	Amber	Slow blink
3.	The CSS 11501 or a module in the CSS 11503 or CSS 11506 is online and not active.	Amber	Solid
	In the CSS 11506, a passive SCM LED remains in this state and color.		

Table 1-2 Status LEDs Boot Definitions (continued)

State Sequence	LED Color	LED State
4.	Green	Solid
The CSS 11501, or a module in the CSS 11503 or CSS 11506, is on line and active.		
The CSS 11501 or a module in the CSS 11503 or CSS 11506 (except a Fast Ethernet Module) failed.	Red	Blinking
In the CSS 11503 or 11506, if: <ul style="list-style-type: none"> • A Fast Ethernet Module fails, all of the Link and Duplex LEDs blink simultaneously. • The master SCM in slot 1 detects a module failure, its Status LED is green and blinks slowly. • The master SCM in slot 1 fails, the CSS does not boot unless there is a passive SCM in slot 2. 		
5.	Green	Variable blinking
Disk activity		

If an error occurs during a power-on self-test, the console displays an error message, increments the detected error counter, and continues to the next test until the CSS completes all of the power-on self tests. See Appendix A, Troubleshooting the Boot Process, for more information on boot errors and messages.

Logging in to the CSS

After the CSS completes the boot process, it displays the login banner, copyright, and login prompt.

When a startup-config file is present, the CSS displays the message: `Press CTRL-C to abort running the startup-config`

**Note**

If the CSS does not detect an existing startup-config file, the CSS automatically initiates the configuration script (see the “Using the Configuration Script” section). The configuration script prompts you to enter configuration information. Subsequent logins to the CSS do not start the configuration script.

If you abort running the startup-config file, the CSS does not use the existing startup-config file. Aborting the use of the startup-config file enables you to log in and reconfigure the CSS to create a new running-config file. Use this feature if you misconfigure your startup-config file and the CSS becomes unusable.

When you log in from:

- A console, the CSS displays the message: `Press any key to log in.`
- A Telnet session, the message is not displayed.

The CSS prompts you to enter a username and password, as follows:

```
User Access Verification
Username:
Password
```

If you connect a console to the CSS after the CSS boots, your screen will be blank. Press **Enter** to display the username and password prompts.

To initially log in to the CSS, enter the default user name **admin** and the default password **system** as lowercase text, or enter the administrative username and password you configured during the boot process. For security, the CSS does not display the password. The default username **admin** enables you to log in with SuperUser status.

If you have not changed the default administrative username and password, we recommend that you change them to safeguard the CSS against unauthorized logins. To change the default username and password from the CLI, see Chapter 2, Configuring CSS Basics.

Using the Configuration Script

When you log in to the CSS and it does not detect an existing startup-config file, the CSS automatically initiates the configuration script. During the running of the configuration script, the CSS prompts you to enter the following information:

- IP address and subnet mask for circuit VLAN1 (all interfaces are assigned to VLAN1 by default)
- IP address for the default gateway
- IP addresses for the servers
- Virtual IP address (VIP) for the content rule

Based on your entries, the configuration script allows you to create services, owners, and content rules. For background information on configuring services, owners, and content rules, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

To accept the script default values, press the **Enter** key at the prompts shown in the configuration script. To quit the script, enter **q** at any prompt. If you quit running the script, you may proceed to Chapter 2, Configuring CSS Basics, to continue the initial setup of the CSS. For information on configuring sticky cookies on the CSS, see Chapter 4, Configuring Sticky Cookies.



Note

You may also initiate the configuration script manually by entering the **script play setup** command.

To clear an existing running-config file, use the **clear running-config** command from SuperUser mode. To clear an existing startup-config file, use the **clear startup-config** command from SuperUser mode.

The following example illustrates the configuration script including:

- **Bold** text to indicate user entry examples
- Explanations to help you use the script

```
#####
#Setup Script for the Content Services Switch#
#####

Checking for Existing Config...

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

Note: Pressing "q" after any prompt quits setup. Pressing <CR> after
any [y/n] defaults to "y".

Warning: All circuit VLAN IP addresses must be on a different subnet
than the Ethernet Mgt port IP address. The existing Ethernet Mgt port
IP address is: 10.0.4.251

Add an IP address to VLAN1: [default = 192.168.10.1] 192.168.3.6

Add an IP subnet mask to VLAN1: [default = 255.255.255.0]

Warning: The default gateway IP address must be on the same subnet as
VLAN1. VLAN1 IP address is: 192.168.3.6

Add IP address for default gateway: [default = 192.168.3.2]
192.168.3.3

Pinging the default gateway: 100% Success.

Which feature do you want to configure?

[1] Layer3 load balancing
[2] Layer5 load balancing
[3] Proxy cache
[4] Transparent cache
[5] Exit script
```

Table 1-3 describes each Configuration Script menu item.

Table 1-3 Configuration Script Menu Options

Menu Option	Function
Layer3 Load Balancing	Configure Layer 3 load balancing to enable the CSS to use a Virtual IP address (VIP) to load balance web traffic to web servers based on IP addresses.
Layer5 Load Balancing	Configure Layer 5 load balancing to enable the CSS to use a VIP address to load balance web traffic to web servers based on URLs.
Proxy Cache	Configure proxy cache to enable the CSS to use a Virtual IP address (VIP) to load balance web traffic to proxy cache servers based on domain name.
Transparent Cache	Configure transparent cache to enable the CSS to redirect cacheable HTTP traffic to transparent cache servers based on IP address and port (80).
Exit Script	Exit from the script and save the information you entered to the CSS running-config file. The CSS displays the running-config file.

Refer to the following sections for details about each item in the Configuration Script menu:

- Configuring Layer 3 Load Balancing
- Configuring Layer 5 Load Balancing
- Configuring Proxy Cache
- Configuring Transparent Cache

Configuring Layer 3 Load Balancing

A Layer 3 load-balancing configuration enables the CSS to use a Virtual IP address (VIP) to load balance web traffic to web servers based on IP addresses.

When you select Layer 3 load balancing, the script automatically:

- Creates an owner (L3_Owner)
- Creates a Layer 3 content rule (L3_Rule) and defines ArrowPoint Content Awareness (ACA) as the load balance method
- Activates the services
- Activates the content rule
- Saves the running configuration to the startup-config file

The script prompts you to configure:

- Service name (default name is Server1)
- Service IP address
- VIP for the content rule

To configure Layer 3 load balancing, enter **1** at the Configuration Script menu.

Which feature do you want to configure?

```
[1] Layer3 load balancing
[2] Layer5 load balancing
[3] Proxy cache
[4] Transparent cache
```

Enter the number for the feature you want to configure: **1**

To accept the script default values, press the **Enter** key at the prompts.

Creating Layer3 load balancing

Enter service name: [default = Server1]

Enter service IP address: [default = 192.168.10.3] **192.168.3.58**

Create another service? [y/n]? **y**

Enter service name: [default = Server2]

Enter service IP address: [default = 192.168.10.3] **192.168.3.59**

```
Create another service? [y/n]? n
```

```
Enter Virtual IP address for L3_Rule: [default = 192.168.10.4]
192.168.3.6
```

After you specify the configuration, the script automatically:

- Displays the running-config file
- Saves the running configuration to the startup-config file

```
Showing the Running Config
```

```
!Generated MAR 6 17:53:49
```

```
!***** GLOBAL *****
ip route 0.0.0.0 0.0.0.0 192.168.3.3
!***** CIRCUIT *****
circuit VLAN1
ip address 192.168.3.6 255.255.255.0
!***** SERVICE *****
service Server1
    ip address 192.168.3.58
    active
service Server2
    ip address 192.168.3.59
    active
!***** OWNER *****
owner L3_Owner
    content L3_Rule
    add service Server1
    add service Server2
    vip address 192.168.3.6
    balance aca
    active
#####
##    Setup Completed Successfully!!!    ##
#####
```

Configuring Layer 5 Load Balancing

A Layer 5 load-balancing configuration enables the CSS to use a VIP address to load balance web traffic to web servers based on URLs.

When you select Layer 5 load balancing, the script automatically:

- Creates an owner (L5_Owner)
- Creates a Layer 3 content rule (L3_Rule)
- Creates a Layer 5 content rule (L5_Rule) and defines:
 - Protocol TCP
 - Port 80
 - URL "/*"
 - Load balance method as ACA
- Activates the services
- Activates the content rule
- Saves the running configuration to the startup-config file

The script prompts you to configure:

- Service name (default name is Server1)
- VIP for the content rule

To configure Layer 5 load balancing, enter **2** at the Configuration Script menu..

Which feature do you want to configure?

```
[1] Layer3 load balancing
[2] Layer5 load balancing
[3] Proxy cache
[4] Transparent cache
```

Enter the number for the feature you want to configure: **2**

To accept the script default values, press the **Enter** key at the prompts.

Creating Layer5 load balancing

Enter service name: [default= Server1]

Enter service IP address: [default = 192.168.10.3] **192.168.3.58**

```
Create another service? [y/n]? n
```

```
Enter Virtual IP address for L5_Rule: [default = 192.168.10.4]
192.168.3.8
```

After you specify the configuration, the script automatically:

- Displays the running-config file
- Saves the running configuration to the startup-config file

```
Showing the Running Config
```

```
!Generated MAR 6 17:53:49
```

```
!***** GLOBAL *****
ip route 0.0.0.0 0.0.0.0 192.168.3.3
!***** CIRCUIT *****
circuit VLAN1
ip address 192.168.3.6 255.255.255.0
!***** SERVICE *****
service Server1
    ip address 192.168.3.58
    active
!***** OWNER *****
owner L5_Owner
content L3_Rule
    add service Server1
    vip address 192.168.3.8
    balance aca
    active
content L5_Rule
    add service Server1
    vip address 192.168.3.8
    protocol tcp
    port 80
    url "/"
    balance aca
    active
#####
##      Setup Completed Successfully!!!  ##
#####
```

Configuring Proxy Cache

A proxy cache configuration enables the CSS to use a Virtual IP address (VIP) to load balance web traffic to proxy cache servers based on domain name.

When you select Proxy Cache, the script automatically:

- Creates an owner (Proxy_Owner)
- Creates a content rule (Proxy_Rule) and defines:
 - Service type as proxy-cache
 - Protocol TCP
 - Port 8080
 - URL "/*"
 - Load balance method as domain
 - Application type HTTP
- Activates the services
- Activates the content rule

The script prompts you to configure:

- Service name (default name is Proxy_Cache1)
- VIP for the content rule

To configure a proxy cache configuration, enter **3** at the Configuration Script menu.

Which feature do you want to configure?

```
[1] Layer3 load balancing
[2] Layer5 load balancing
[3] Proxy cache
[4] Transparent cache
```

Enter the number for the feature you want to configure: **3**

To accept the script default values, press the **Enter** key at the prompts.

Creating Proxy Cache Configuration

Enter service name: [default=Proxy_Cache1]

Enter service IP address: [default = 192.168.10.3] **192.168.3.60**

```
Create another service? [y/n]? n
```

```
Enter Virtual IP address for Proxy_Rule: [default = 192.168.10.4]
192.168.3.9
```

After you specify the configuration, the script automatically:

- Displays the running-config file
- Saves the running configuration to the startup-config file

```
Showing the Running Config
!Generated MAR 6 17:53:49
!***** GLOBAL *****
ip route 0.0.0.0 0.0.0.0 192.168.3.3
!***** CIRCUIT *****
circuit VLAN1
ip address 192.168.3.6 255.255.255.0
!***** SERVICE *****
service Proxy_Cache1
    ip address 192.168.3.60
    type proxy-cache
    port 8080
    protocol tcp
    active
!***** OWNER *****
owner Proxy_Owner
content Proxy_Rule
    add service Proxy_Cache1
    vip address 192.168.3.9
    port 8080
    protocol tcp
    url "/*"
    balance domain
    application http
    active

#####
##      Setup Completed Successfully!!!  ##
#####
```

Configuring Transparent Cache

A transparent cache configuration enables the CSS to redirect cacheable HTTP traffic to transparent cache servers based on IP address and port (80). The CSS directs non-cacheable HTTP traffic to the origin servers.

When you select Transparent Cache, the script automatically:

- Creates an owner (Transparent_Owner)
- Creates a content rule (Transparent_Rule) and defines:
 - Service type as transparent-cache
 - Protocol TCP
 - Port 80
 - Extension Qualifier List (EQL) named *Cacheable* that contains the file types displayed in the sample running-config file
 - URL "/*" eql cacheable
 - Load balance method as domain
 - Failover type as bypass
 - Application type HTTP
- Activates the services
- Activates the content rule

The script enables you to:

- Configure a service name (Transparent_Cache1)
- Define whether to direct only cacheable content or all content to the cache servers

To configure a transparent cache configuration, enter **4** at the Configuration Script menu.

Which feature do you want to configure?

```
[1] Layer3 load balancing
[2] Layer5 load balancing
[3] Proxy cache
[4] Transparent cache
```

Enter the number for the feature you want to configure: **4**

To accept the script default values, press the **Enter** key at the prompts.

Creating Transparent Cache Configuration

Enter service name: [default = Transparent_Cache1]

Enter service IP address: [default = 0.0.0.0] **192.168.3.7**

Create another service? [y/n]? **n**

Transparent caching can be configured to direct only cacheable content to the cache server. Non-cacheable content is sent directly to the origin server.

The alternative is to direct all traffic to the cache server regardless of whether the content is cacheable.

Should only cacheable content be directed to the cache server? [y/n]?

Enter one of the following:

- **y** to define URL “/*” as epl-cacheable in the content rule and allow the CSS to direct only cacheable content to the cache servers.
- **n** to define URL “/*” in the content rule and allow the CSS to direct all content to the cache servers.

After you specify the configuration, the script automatically:

- Displays the running-config file
- Saves the running configuration to the startup-config file

Showing the Running Config

!Generated MAR 6 17:53:49

```
!***** GLOBAL *****
ip route 0.0.0.0 0.0.0.0 192.168.3.3
!***** CIRCUIT *****
circuit VLAN1
ip address 192.168.3.6 255.255.255.0
!***** SERVICE *****
service Transparent_Cache1
    ip address 192.168.3.7
    type transparent-cache
    port 80
    protocol tcp
    active
```

```

!***** EQL *****
eq1 Cacheable
  description "This EQL contains
    extensions of cacheable content"
  extension pdf "Acrobat"
  extension fdf "Acrobat Forms Document"
  extension au "Sound audio/basic"
  extension bmp "Bitmap Image"
  extension z "Compressed data
    application/x-compress"
  extension gif "GIF Image image/gif"
  extension html "Hypertext Markup
    Language text/html"
  extension htm
  extension js "Java script
    application/x-javascript"
  extension mocha
  extension jpeg "JPEG image image/jpeg"
  extension jpg
  extension jpe
  extension jfif
  extension pjpeg
  extension pjp
  extension mp2 "MPEG Audio audio/x-mpeg"
  extension mpa
  extension abs
  extension mpeg "MPEG Video video/mpeg"
  extension mpg
  extension mpe
  extension mpv
  extension vbs
  extension mlv
  extension pcx "PCX Image"
  extension txt "Plain text text/plain"
  extension text
  extension mov "QuickTime video/quicktime"
  extension tiff "TIFF Image image/tiff"
  extension tar "Unix Tape Archive
    application/x-tar"
  extension avi "Video for Windows
    video/x-msvideo"
  extension wav "Wave File audio/x-wav"
  extension gz "application/x-gzip"
  extension zip "ZIP file
    application/x-zip-compressed"

```

```

!***** OWNER *****
owner Transparent_Owner
content Transparent_Rule
    add service Transparent_Cache1
    port 80
    protocol tcp
    url "/*" eq1 Cacheable or url "/*"
    balance domain
    failover bypass
    application http
    active
#####
##      Setup Completed Successfully!!!      ##
#####

```

Rebooting the CSS

Use the **reboot** command to reboot the CSS. This command is available in Boot mode.

Before you enter the **reboot** command, save an existing running-config file prior to rebooting the CSS by using the **copy running-config startup-config** command from SuperUser mode. If you are not in expert mode, the CSS displays the prompts to save profile and configuration changes before it reboots.

To reboot the CSS, access Boot mode and enter the **reboot** command. For example, enter:

```

(config)# boot
(config-boot)# reboot

```

The CSS displays a prompt to verify that you want to reboot it:

```

Are you sure you want to reboot the system, [y/n]

```

Enter **y** to reboot the CSS.

**Note**

The CSS has a reboot alias that allows you to reboot it from any mode except User mode. When you enter the reboot alias, the CSS changes the current mode to Boot mode and then executes the **reboot** command.

You must enter the entire reboot alias name to execute it. The CSS does not automatically complete the reboot alias at the command line when you enter only part of its name. For example, if you enter **reb** in global configuration mode, the CSS displays an invalid command message.

Shutting Down the CSS

Use the **shutdown** command to shut down the CSS. This command shuts down all CSS processes so you can power cycle the unit safely. The **shutdown** command is available in Boot mode.

To shut down the CSS, access Boot mode and enter:

```
(config-boot)# shutdown
```

The CSS displays a prompt to verify that you want to shut it down:

```
Are you sure you want to shutdown the system, [y/n]:
```

Enter **y** to shut down the CSS.

**Note**

The CSS has a shutdown alias that allows you to shut it down from any mode except User mode. When you enter the shutdown alias, the CSS changes the current mode to Boot mode and then executes the **shutdown** command.

You must enter the entire shutdown alias name to execute it. The CSS does not automatically complete the shutdown alias at the command line when you enter only part of its name. For example, if you enter **shutd** in global configuration mode, the CSS displays an invalid command message.

Where to Go Next

Chapter 2, *Configuring CSS Basics*, describes the initial configuration procedures for the CSS, such as changing the administrative username and password, creating usernames and passwords, configuring the Ethernet management port, specifying a static IP address and subnet mask, and changing the date and time.



Configuring CSS Basics

This chapter describes the initial configuration procedures for the CSS. Information in this chapter applies to all CSS models, except where noted.

This chapter contains the following major sections:

- Initial Setup Quick Start
- Changing the Administrative Username and Password
- Creating Usernames and Passwords
- Configuring the Ethernet Management Port
- Configuring an IP Route
- Configuring the Date, Time, and Time Zone
- Synchronizing the CSS with an SNTP Server
- Configuring a Host Name

Initial Setup Quick Start

Table 2-1 is a quick start configuration table designed to help you configure the CSS quickly and easily. This table provides the following basic steps:

- Log in and access config mode
- Change the default administrative username and password
- Create additional usernames and passwords to log in to the CSS (optional)
- Access boot mode to configure an IP address and subnet mask for the Ethernet management port
- Configure a static route for destination networks that are outside the local subnet of the CSS and the Ethernet management port (optional)
- Configure a default IP route
- Enter the date, time, and time zone (optional)
- Specify a Simple Network Time Protocol (SNTP) server (optional)

Once you configure the Ethernet management port IP address, you can continue to use the console port or you can use the Ethernet management port to Telnet in to the CSS and configure it remotely.

Table 2-1 Initial Setup Quick Start

Task and Command Example

1. Log in to the CSS using the default administrative username **admin** and password **system**, or the username and password assigned to you during the boot process.

Refer to Chapter 1, Booting, Logging In, and Getting Started, for details on logging in to the CSS.

2. Access config mode.

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

3. Change the default administrative username and password.

```
(config)# username-offdm bobo password secret
```

Table 2-1 Initial Setup Quick Start (continued)**Task and Command Example**

4. Create usernames and passwords to log in to the CSS (optional). The CSS supports a maximum of 32 usernames, including the administrator and technician usernames. You can assign each user with SuperUser or User status.

```
(config)# username picard password "captain" superuser
```

5. Access boot mode to configure an IP address for the Ethernet management port. This IP address must be on a different subnet than any other CSS virtual LAN (VLAN) circuit IP subnet or you will not be able to access the port. You must reboot the CSS for the new IP address to take effect.

```
(config)# boot  
(config-boot)# ip address 172.16.6.58
```

6. Configure a subnet mask for the Ethernet management port in boot mode.

```
(config-boot)# subnet mask 255.255.255.0
```

7. Exit from boot mode to config mode.

```
(config-boot)# exit
```

8. Configure a static IP route, as required.

```
(config)# ip route 192.168.0.0 255.255.0.0 192.168.1.1
```

9. Exit from config mode to configure a date. The **clock date** command does not allow backspacing. If you enter a wrong date, reenter the command with the new information.

Enter the date in the format *mm-dd-yy*.

```
# clock date  
Enter date: [12-31-03] 12-31-03
```

To use the European format to specify the date (using the format of day, month, and year), access config mode and use the **date european-date** command to enable the **clock date** command to accept date input in the format of day, month, and year.

```
(config)# date european-date  
(config)# exit  
# clock date  
Enter date: [31-12-03] 31/12/03
```

Table 2-1 Initial Setup Quick Start (continued)**Task and Command Example**

10. Configure the time using the **clock time** command. The **clock time** command does not allow backspacing. If you enter the wrong time, reenter the command with the new information.

Enter the time in the format *hh:mm:ss*.

```
# clock time
Enter time: [15:17:33] 16:17:33
```

11. (Optional) Specify the time zone and Universal Time Coordinated (UTC) offset if you are using an SNTP server to synchronize the CSS system clock.

```
# clock timezone EST hours 3 before-UTC
```

12. (Optional) Access config mode and specify the SNTP server and the polling frequency if you are using an SNTP server to synchronize the CSS system clock.

```
# config
(config)# sntp server 192.168.19.21 version 2
(config)# sntp poll-interval 90
```

13. Save your configuration changes to the running-config file (recommended). If you do not save changes to the running-config file, all configuration changes are lost upon reboot.

```
(config)# exit
# copy running-config startup-config
```

The following running-configuration example shows the results of entering the commands in Table 2-1.

```
!***** GLOBAL *****
username picard des-password 1hbfoeqbyecllac superuser
sntp server 192.168.19.21 version 2
sntp poll-interval 90

ip route 192.168.0.0 255.255.0.0 192.168.1.1 1
```

Changing the Administrative Username and Password

During the initial log in to the CSS you enter the default user name **admin** and the default password **system** in lowercase text. For security reasons, you should change the administrative username and password. Security on your CSS can be compromised because the administrative username and password are configured to be the same for every CSS shipped from Cisco Systems.

The administrative username and password are stored in nonvolatile random access memory (NVRAM). Each time you reboot the CSS, it reads the username and password from NVRAM and reinserts them in to the user database. SuperUser status is assigned to the administrative username by default.

You can change the administrative username and password, but because the information is stored in NVRAM, you cannot permanently delete them. If you delete the administrative username using the **no username** command, the CSS deletes the username from the running-config file, but restores the username from NVRAM when you reboot the CSS.

Use the **username-offdm name password text** command to change the administrative username or password.

**Note**

You can also use the Security Options menu from the Offline DM menu (accessed during the boot process) to change the administrative username and password. Refer to the *Cisco Content Services Switch Administration Guide* for information on the Offline DM menu.

For example, to change the default administrative username and password to a different username and password, enter.

```
(config)# username-offdm bobo password secret
```

Creating Usernames and Passwords

You can assign each user that logs into the CSS with SuperUser or User status.

- **User** - Allows access to a limited set of commands that enable you to monitor and display CSS parameters, but not change them. A User prompt ends with the > symbol.
- **SuperUser** - Allows access to the full set of CLI commands, including those in User mode, that enable you to configure the CSS. A SuperUser prompt ends with the # symbol.

Use the **username** command to create usernames and passwords to log in to the CSS. The CSS supports a maximum of 32 usernames, including the administrator and technician usernames.

From SuperUser mode, you can enter global configuration mode and its subordinate configuration modes. If you do not specify **superuser** when configuring a new user, the new user has only user-level status by default.



Caution

Creating or modifying a username and password is restricted to CSS users who are identified as either administrators or technicians, and it is contingent on whether the **restrict user-database** command has been entered (refer to the *Cisco Content Services Switch Security Configuration Guide*).

The syntax for this global configuration mode command is:

```
username name [des-password|password] password {superuser}
{dir-access access}
```

The following example creates a SuperUser named *picard* with a password of *captain*.

```
(config)# username picard password "captain" superuser
```

The options and variables are as follows:

- *name* - Sets the username you want to assign or change. Enter an unquoted text string with no spaces and a maximum of 16 characters. To see a list of existing usernames, enter **username ?**.

- **des-password** - Specifies that the password you enter is the Data Encryption Standard (DES) form of the password. Use this option *only* when you are creating a script or a startup configuration file. Enter a DES-encrypted, case-sensitive, unquoted text string with no spaces from 6 to 64 characters.



Note If you specify the **des-password** option, you must know the encrypted form of the password to successfully log in to the CSS. You can find the CSS encrypted password in the Global section of the running-config. To display the running-config, use the **show running-config** command.

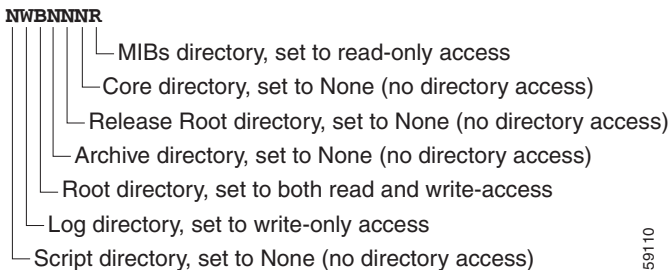
- **password** - Specifies that the password is not encrypted on your display as you enter it. However, the CSS DES-encrypts the password in the running-config for extra security. Use this option when you use the CLI to create users. Enter a case-sensitive, unquoted text string with no spaces from 6 to 16 characters.
- *password* - The text string that you enter. The CSS allows all special characters in a password except for the percent sign (%).
- **superuser** - Specifies SuperUser privileges to allow a user to access SuperUser mode. If you do not enter this option, the user can access only User mode.
- **dir-access** - (Optional) Defines the CSS directory access privileges for the username. There are access privileges assigned to the seven CSS directories, in the following order: Script, Log, Root (installed CSS software), Archive, Release Root (configuration files), Core, and MIBs. By default, users have both read- and write-access privileges (B) to all seven directories. Administrators or technicians can use the **dir-access** option to selectively implement a set of directory access privileges for each user. Changing the access level also affects the use of the CLI commands associated with directories.

To use the **dir-access** option, you must first specify the **restrict user-database** command to implement security restrictions for the CSS user database (refer to the *Cisco Content Services Switch Administration Guide*).

- *access* - Specifies directory access privileges for the username. By default, users have both read- and write-access privileges (B) to all seven directories. Enter, in order, one of the following access privilege codes for each of the seven CSS directories:
 - **R** - Read-only access to the CSS directory
 - **W** - Write-only access to the CSS directory
 - **B** - Both read- and write-access privileges to the CSS directory
 - **N** - No access privileges to the CSS directory

Figure 2-1 illustrates the directory access privileges for a username.

Figure 2-1 CSS Directory Access Privileges



For example, to define directory access for username *picard*, enter:

```
(config)# username picard password "captain" superuser NWBNNNR
```

To display a list of existing usernames, enter:

```
(config)# username ?
```

To remove an existing username, enter:

```
(config)# no username picard
```

To change a user password, reenter the **username** command and specify the new password. Remember to include SuperUser privileges if required. For example:

```
(config)# username picard password "flute" superuser
```



Caution

The **no username** command removes a user permanently. Make sure you want to perform this action because you cannot undo this command.

Configuring the Ethernet Management Port

The Ethernet management port provides a connection to the CSS that allows you to perform CSS management functions. The Ethernet management port supports management functions such as:

- Secure remote login through SSH
- Remote login through Telnet
- File transfer through active FTP
- SNMP queries
- SNTTP
- DNS
- ICMP redirects
- RADIUS
- Syslog
- CDP
- TACACs
- CSS configuration changes through XML

**Note**

When using static routes for managing the CSS from subnets beyond the management LAN, the Ethernet management port supports the previous list of management applications, except CDP, DNS, SNTTP, and TACACs. For more information on static routes, see the “Configuring Static Routes for the Ethernet Management Port” section.

The Ethernet management port also supports ping and traceroutes initiated from the CSS.

The Ethernet management port is located on the CSS 11501, CSS 11503, or CSS 11506 SCM front panels.

To access the Ethernet management port on the CSS, you must assign an IP address and a subnet mask to the port. If you want to manage the CSS from a subnet that is different from the Ethernet management port, you can configure static routes for the Ethernet management port.

If you want to use the Offline Diagnostic Monitor (Offline DM) menu to boot the CSS from an image that resides on a different subnet, you can configure a default gateway for the Ethernet management port.

Note the following considerations when configuring or using the Ethernet management port:

- Dynamic routing protocols (such as RIP and OSPF) are not supported on the Ethernet management port.
- Packet routing or forwarding is not supported between the Ethernet management port and the Ethernet interface ports.
- Access control lists (ACLs) are not supported on the Ethernet management port.
- APP sessions are not supported on the Ethernet management port.
- You cannot specify an Ethernet management port IP address that matches or overlaps an IP address, VIP range, or static route previously set for one of the Ethernet interface ports. If you attempt to specify an overlapping or matching IP address, the CSS displays an error message and stops you from completing the command entry.
- The Ethernet management port supports SNMP requests to retrieve CSS port information. The CSS Enterprise MIBs, however, do not return data for the Ethernet management port.

This section includes the following procedures:

- Configuring an IP Address and Subnet Mask for the Ethernet Management Port
- Configuring Static Routes for the Ethernet Management Port
- Configuring a Default Gateway for the Ethernet Management Port
- Discarding ICMP Redirects on the Ethernet Management Port
- Shutting Down the Ethernet Management Port

Configuring an IP Address and Subnet Mask for the Ethernet Management Port

To access the Ethernet management port on the CSS, you must assign an IP address and a subnet mask. When setting the Ethernet management port IP address, note that:

- The IP address must be on a different subnet than any other CSS VLAN circuit IP subnets. If you do not make the Ethernet management port IP address unique, you cannot access the port. Any traffic that is transmitted from or sent to the CSS circuit will fail if there is an overlap with the management port IP address.
- An IP address of 0.0.0.0 for the Ethernet management port is a legal setting and disables the management port upon reboot. If you enter **0.0.0.0**, and attempt to use the **subnet mask** command, the following message appears:
The mask cannot be set because the IP address is 0.0.0.0.

Use the **ip address** command to configure an IP address for the Ethernet management port. Use the **subnet mask** command to configure the subnet mask for the Ethernet management port. Both commands are available in boot mode. You must reboot the CSS for the new Ethernet management port IP address and subnet to take effect.

The first time that you enter an IP address for the Ethernet management port, the CSS automatically configures a default subnet mask of 255.255.255.0. If you want, you can overwrite the default subnet mask with a mask that is appropriate for your application.

For example, to specify an Ethernet management port IP address, enter:

```
(config)# boot
(config-boot)# ip address 172.16.6.58
```

For example, to specify an Ethernet management port subnet mask of 255.255.255.0, enter:

```
(config-boot)# subnet mask 255.255.255.0
```

Both the **ip address** command and the **subnet mask** command do not have a **no** form of the command. To change the IP address of the Ethernet management port, reenter the **ip address** command and enter the new IP address. To change the subnet mask, reenter the **subnet mask** command and enter the new subnet mask.

Configuring Static Routes for the Ethernet Management Port

If you want to manage the CSS from a subnet that is different from the Ethernet management port, you can configure static routes for the Ethernet management port. Static route entries consist of the destination IP network address and the IP address of the next hop router. You can configure a maximum of eight static routes for the Ethernet management port.

**Note**

When using static routes for managing the CSS from subnets beyond the management LAN, the Ethernet management port supports the management applications listed in the “Configuring the Ethernet Management Port” section except CDP, DNS, SNTP, and TACACs.

Note the following considerations when configuring a static route for the Ethernet management port:

- The CSS does not use an internal (implicit) service for the Ethernet management port to periodically poll the next hop address in a static route. The periodic polling of the next hop address with an ICMP echo (or ping) keepalive is performed only when you configure a static route for an Ethernet interface port.
- The **rip redistribute static** and **ospf redistribute static** commands do not advertise static routes configured on the Ethernet management port. These two commands only advertise static routes configured on the Ethernet interface ports.

Use the **ip management route** command to configure static routes for the Ethernet management port. This command is available in global configuration mode.

The syntax for the **ip management route** command is:

```
ip management route ip_address subnet_mask ip_address2
```

The variables are as follows:

- *ip_address* - The destination network address. Enter the IP address in dotted-decimal notation (for example, 192.168.11.0).
- *subnet_mask* - The IP subnet mask. Enter the mask as either:
 - A prefix length in classless interdomain routing (CIDR) bit-count notation (for example, /24).
 - An IP address in dotted-decimal notation (for example, 255.255.255.0).
- *ip_address2* - The next hop address for the route. Enter the IP address in dotted-decimal notation (for example, 192.168.11.0).

For example, to configure a static route for the Ethernet management port, enter:

```
(config)# ip management route 172.27.59.0 /24 172.16.6.100
```

To disable a static route for the Ethernet management port, enter:

```
(config)# no ip management route 172.27.59.0 /24 172.16.6.100
```

Configuring a Default Gateway for the Ethernet Management Port

The Ethernet management port allows you to boot the CSS from the Offline DM menu when the boot image resides on a different subnet. Use the **gateway address** command to configure a default gateway for the Ethernet management port. This command is available in boot mode.

To specify a default gateway for the Ethernet management port for use in Offline DM, enter:

```
(config)# boot
(config-boot)# gateway address 172.16.6.110
```

To disable the default gateway and set it to an IP address of 0.0.0.0, use the **no** form of the **gateway address** command. For example:

```
config-boot)# no gateway address
```

A default gateway of 0.0.0.0 for the Ethernet management port does not appear in the **show boot-config** command output for the CSS boot configuration.

Discarding ICMP Redirects on the Ethernet Management Port

By default, the Ethernet management port accepts all incoming ICMP redirects. If you do not configure static routes for the management port, the CSS disregards any ICMP redirect packets. However, when you configure static routes for the management port, the CSS incorporates the ICMP redirects to the port as an entry in the routing table.

To enhance security on the CSS when you configure static routes on the management port, we strongly recommend that you configure the CSS management port to discard ICMP redirects.



Note

The Ethernet management port never transmits an ICMP redirect. If you remove a static route when the management port is configured to accept ICMP redirect packets, the CSS removes from the routing table the router entry created by the ICMP redirects associated with the static route.

To configure the CSS to discard ICMP redirect packets on the Ethernet management port, enter:

```
(config)# ip management no-icmp-redirect
```

To reset the default behavior of accepting ICMP redirect packets on the Ethernet management port, enter:

```
(config)# no ip management no-icmp-redirect
```

To view whether the management port accepts or discards ICMP redirect packets, use the **show ip configuration** command to display the IP Management Port ICMP redirect field. When the port accepts ICMP redirects, the field entry displays enable. When the port discards ICMP redirects, the field entry displays disable.

Shutting Down the Ethernet Management Port

To shut down the Ethernet management port, use the **admin-shutdown** or **shut** command.

For example:

- To shut down the Ethernet management port on the CSS 11501 with the **admin-shutdown** command, enter:

```
(config-if[Ethernet-Mgt])# admin-shutdown
```

- To shut down the Ethernet management port on the CSS 11501 with the **shut** command, enter:

```
(config-if[Ethernet-Mgt])# shut
```

When you use the **shut** command, the CSS changes the **shut** command to the **admin-shutdown** command in the running configuration.

Configuring an IP Route

To establish IP connectivity to the CSS, a static IP route is required to connect the CSS to the next hop router. A static route consists of a destination network address and mask and the next hop to reach the destination. You can also specify a default static route (using 0.0.0.0 as the destination network address and a valid next hop address) to direct frames for which no other destination is listed in the routing table. Default static routes are useful for forwarding otherwise unroutable packets by the CSS.

When you configure a static IP route, the CSS periodically polls the next hop router with an internal ICMP keepalive service to ensure the router is functioning properly. If the router fails, the CSS removes any entries from the routing table that point to the failed router and stops sending traffic to the failed router. When the router recovers, the CSS:

- Becomes aware of the router
- Reenters applicable routes in the routing table

To configure a static IP route, use the **ip route** command and specify one of the following:

- An IP address and prefix length; for example, 192.168.1.0 /24
- An IP address and a subnet mask; for example, 192.168.1.0 255.255.255.0

The syntax for the **ip route** command is:

```
ip route ip_address subnet mask ip_address2
```

The variables are as follows:

- *ip_address* - The destination network address. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1).
- *subnet_mask* - The IP subnet mask. Enter the mask as either:
 - A prefix length in CIDR bit-count notation (for example, /24)
 - An IP address in dotted-decimal notation (for example, 255.255.255.0)
- *ip_address2* - The next hop address for the route. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1).

For example, to configure a static IP route to destination network address *192.168.0.0/16* and a next hop address of *192.168.1.1*, enter:

```
(config)# ip route 192.168.0.0 /16 192.168.1.1
```

For example, to configure a default IP route using a destination address of *0.0.0.0/0* and a next hop address of *192.167.1.1*, enter:

```
(config)# ip route 0.0.0.0 /0 192.167.1.1
```

Refer to the *Cisco Content Services Switch Routing and Bridging Configuration Guide* for complete information on configuring IP routes.

Configuring the Date, Time, and Time Zone

To set the date, time, or time zone for the CSS, use the **clock** command. When you enter this command, the CSS displays the current date and time.

The **clock** command does not allow backspacing. If you enter the wrong date, time, or time zone, you must reenter the command with the new information.

This section includes the following topics:

- Setting the Date
- Setting the European Date
- Setting the Time
- Setting the Time Zone
- Configuring Daylight Saving Time
- Showing the Date and Time

Setting the Date

Use the **clock date** command to set the date. A prompt appears to show the current date in the correct format to use. Enter the month, day, and year as integers with dash characters separating them. For example, enter June 15th 2003 as 06-15-03.

Enter the new date in the format *mm-dd-yy* as shown:

```
# clock date
Enter date: [12-31-03] 12-31-03
```

Setting the European Date

Use the **date european-date** global configuration mode command to specify the date in the European format of day, month, and year. This command enables the **clock date** command to accept the date in day, month, and year, separated by slashes (/).

Enter the new date in the format *dd/mm/yy* as shown:

```
(config)# date european-date
(config)# exit
# clock date
Enter date: [31-12-03] 31/12/03
```

To reset the format for the **clock date** command to the default of month, day, and year, enter:

```
(config)# no date european-date
```

Setting the Time

Use the **clock time** command to set the time. This command sets the time in military-time (24-hour) format. A prompt appears to show the current time in the correct format to use. Enter the hour, minutes, and seconds as integers, separated by colons.

Enter the new time in the format *hh:mm:ss* as shown:

```
# clock time
Enter time: [15:12:38] 16:12:38
```

Setting the Time Zone

Use the **clock timezone** command to specify a time zone for the CSS, which synchronizes the CSS system clock with an SNTP server. The time stored in the CSS is the local time. The SNTP server calculates the Universal Time Coordinated (UTC, also known as Greenwich Mean Time) time by offsetting the time zone from the local time. If required, you can apply a negative offset to the UTC (for example, -05:-23:+00) or a positive offset to the UTC (for example, +12:+00:+00).

Use the **no** form of the **clock timezone** command to reset the time zone information to 00:00:00, and also to set the clock to the new time without the time zone offset.

**Note**

The use of the **clock timezone** command assumes you are using the CSS with an SNTP server to synchronize the CSS system UTC time to that of a designated SNTP server. Without a configured SNTP server, the time zone information is not used. See the “Synchronizing the CSS with an SNTP Server” section for details.

The syntax for the **clock timezone** command is:

```
clock timezone name hours hours {before-UTC|after-UTC} {minute  
minutes {before-UTC|after-UTC}
```

The options and variables are as follows:

- **timezone** *name* - The name of the time zone. Enter a name with a maximum of 32 characters and no spaces.
- **hours** *hours* - The hours of offset for the time zone. Enter a number from 0 to 12. Use with the **before-UTC** option or **after-UTC** option to set the offset to either a negative or positive number.
- **before-UTC** - The offset for UTC as a negative number. For example, if the hour offset is 12, **before-UTC** sets the offset to -12.
- **after-UTC** - The offset for UTC as a positive number (the default offset).
- **minute** *minutes* - The minutes of offset for the time zone. Enter a number from 0 to 59. Use with the **before-UTC** option or **after-UTC** option to set the offset to either a positive or negative number.

For example, to enter the new time zone for Eastern Standard Time (EST) with a -3 hour offset:

```
# clock timezone EST hours 3 before-UTC
```

To set the time zone offset back to 00:00:00 (and also set the clock to the new time without the time zone offset):

```
# no clock timezone
```

Configuring Daylight Saving Time

By default, the CSS does not automatically change its clock for daylight saving time (DST). You can configure the CSS clock to automatically change to accommodate DST and its different policies in countries and territories worldwide. In many places in the world, DST is also known as Summer Time.

The DST feature on the CSS allows you to configure the date to begin and end DST, the time of day, and the number of minutes to offset the time. The DST feature is compatible with the CSS SNTP feature, but also works without having SNTP configured. A CSS configured with both SNTP and DST relies on SNTP to obtain the Coordinated Universal Time (UTC), and the CSS clock timezone information to provide the proper offset from UTC.



Note

Commands that are scheduled in the command scheduler may be affected by the time change when DST begins and ends. If a command is scheduled for execution at the same time period when the clock moves forward on the start of DST, then the CSS does not execute this command. However, when the time reverts back at the conclusion of the DST period and a command is scheduled for execution at this time, then the CSS executes the command twice.

To configure the CSS clock for DST, use the **clock summer-time** command in SuperUser mode. Through this command, you can configure DST to occur every year or for a single year occurrence on the CSS. You can also configure the number of minutes to offset the time. See the following sections to configure DST on the CSS:

- Configuring DST to Occur Every Year
- Configuring DST for Only One Year
- Disabling DST on the CSS

To view the DST configuration or whether DST is disabled on the CSS, use the **show clock** command. For more information, see the “Showing the Date and Time” section.



Note

The CSS stores DST configuration information in NVRAM.

Configuring DST to Occur Every Year

To configure DST to occur every year on the CSS, use the **recurring** option with the **clock summer-time** command. When you use the **recurring** keyword without any other options, the CSS uses the United States (US) standard for DST with a 60 minute offset. US DST starts at 2 a.m. on the first Sunday of April and reverts to standard time at 2 a.m. on the last Sunday of October. The syntax is:

```
clock summer-time name recurring
```

The *name* variable is a three-character name for the time zone that appears when you use the **show clock** command during DST (for example, EDT, CDT, PDT).

For example to configure a zone named EDT to signify eastern daylight time using the default US standard DST every year, enter:

```
# clock summer-time EDT recurring
```

When you display this configuration using the **show clock** command, the Summer Time field displays 1 Sunday April 2:00 last Sunday October 2:00 60.

If you want to configure the CSS DST to occur every year on a different date or time other than that of the US standard, you must enter the start and stop dates and time for DST in the following syntax:

```
clock summer-time zone recurring start_week start_day start_month  
hh:mm end_week end_day end_month hh:mm {offset}
```

The options are:

- *zone* - The three-character name to designate the time zone.
- *start_week* - The week of the month to begin DST. Enter a number from 1 to 4, or **last**.
- *start_day* - The day of the week to begin DST. Enter a day from Sunday to Saturday.
- *start_month* - The month to begin DST. Enter a month from January to December.
- *hh:mm* - The military format of time in hours and minutes. For example, to enter 2 a.m., enter 02:00. For 2 p.m., enter 14:00.
- *end_week* - The week of the month to end DST. Enter a number from 1 to 4, or **last**.

- *end_day* - The day of the week to end DST. Enter a day from Sunday to Saturday.
- *end_month* - The month to end DST. Enter a month from January to December.
- (Optional) *offset* - The number of minutes added to the time for DST. By default, the offset is 60. Enter a number from 1 to 240.

For example, to configure DST in time zone EDT to start on the first Sunday in June at 2 a.m. and end on the last Sunday in October at 2 a.m., enter:

```
# clock summer-time EDT recurring 1 Sunday June 02:00 last Sunday
October 02:00
```

Configuring DST for Only One Year

To configure DST to occur for only one year on the CSS, use the **date** keyword with the **clock summer-time** command in the following syntax:

```
clock summer-time zone date dateStart monthStart yearStart hh:mm
dateEnd monthEnd yearEnd hh:mm {offset}
```

- *zone* - The three-character name to designate the time zone.
- *dateStart* - The day of the month to begin DST. Enter a number from 1 to 31.
- *monthStart* - The month to begin DST. Enter a month from January to December.
- *yearStart* - The year to begin DST. Enter a value from 2000 to 2079.
- *hh:mm* - The military format of time in hours and minutes. For 2 a.m., enter 02:00. For 2 p.m., enter 14:00.
- *dateEnd* - The day of the month to end DST. Enter a number from 1 to 31.
- *monthEnd* - The month to end DST. Enter a month from January to December.
- *yearEnd* - The year to end DST. Enter a value from 2000 to 2079.
- (Optional) *offset* - The number of minutes added to the time for DST. By default, the offset is 60. Enter a number from 1 to 240.

For example, to configure DST in zone PDT to start on October 2, 2005 at 2 a.m. and end on May 2, 2006 at 2 a.m., enter:

```
# clock summer-time PDT date 2 October 2005 02:00 2 May 2006 02:00
```

Disabling DST on the CSS

To disable DST on the CSS, the default behavior, use the **no clock summer-time** command. For example, enter:

```
# no clock summer-time
```

Showing the Date and Time

Use the **show clock** command to display the current date and time. For example:

```
# show clock
```

Table 2-2 describes the fields in the **show clock** command output.

Table 2-2 Field Descriptions for the **show clock** Command

Field	Description
Date	<p>Configured date in the format of month, day, and year (mm-dd-yyyy); for example, the date June 15th 2005 appears as 06-15-2005.</p> <p>If you use the date european-date command, the format is day, month, and year (dd-mm-yyyy). For example, the date June 15th 2005 appears as 15-06-2005.</p>
Time	<p>Configured time in the format of hour, minute, and second (hh:mm:ss); for example, 16:23:45.</p> <p>If you configure an SNTP server, the show clock command displays the time adjusted with the time zone offset. The show clock command displays the UTC time from the SNTP server. If you configure a time zone, the show clock command displays the time adjusted with the time zone offset. For example, if the UTC time from the server is 16:30:43 and you configure a time zone negative offset of 5 hours and 30 minutes (-05:-30:+00), the displayed time becomes 11:00:43.</p>

Table 2-2 *Field Descriptions for the show clock Command (continued)*

Field	Description
TimeZone	<p>The configured name of the time zone and the time offset from an SNTP server. When daylight savings time (DST) is configured, the configured DST timezone name is displayed during DST.</p> <p>An offset with all zeros (00:00:00) indicates that no offset was configured for the time zone. A negative symbol (-) indicates a negative offset to the UTC (for example, -05:-23:+00). A positive symbol (+) indicates a positive offset to the UTC (for example, +12:+00:+00).</p> <p>When DST is configured, this field also provides information in brackets that displays the DST recurring or date configuration settings. During DST, the configured name for the time zone, and the start date and time for standard time are displayed. When standard time is in effect, the configured name for the DST time zone, and its start date and time are displayed.</p>
Summer Time	The three-letter configured name of the time zone when you configure DST. Disabled indicates that the CSS is not configured for DST.
Change	The number of minutes added to the time for DST. By default, the offset is 60.
Added	The current DST configuration when the clock transitions to DST.
Removed	The current DST configuration when the clock transitions to standard time.

Synchronizing the CSS with an SNTP Server

The Simple Network Time Protocol (SNTP) enables you to synchronize the computer system clocks on the Internet to that of a designated SNTP server. SNTP is a simplified, client-only version of the Network Time Protocol (NTP) that enables the CSS time-of-day to be synchronized with any SNTP server. Use the `sntp` command to configure SNTP on the CSS.

Accurate time-of-day is provided by synchronizing to the UTC time, which provides time within 100 milliseconds of the accurate time. You can configure information about the local time zone so the time appears correctly relative to the local time zone. You can configure two SNTP servers (primary and secondary) in case one server is unavailable. The CSS can receive the time from both servers but uses only the time of the primary server. If the primary server is unavailable, the CSS uses the time of the secondary server.

**Note**

The CSS cannot be used to provide time services to other devices.

Before you synchronize the CSS with an SNTP server, make sure you configure the proper time zone for the CSS (for example, to EST). Also make sure the time difference between the CSS internal clock and the SNTP server clock is less than 24 hours. Otherwise, the CSS will not synchronize its clock with the SNTP server. To configure the time on the CSS, see the “Configuring the Date, Time, and Time Zone” section for details.

For detailed information on configuring the SNTP server, consult the documentation provided with the server.

This section includes the following topics:

- Configuring a Primary or Secondary SNTP Server
- Configuring the Poll Interval for the SNTP Server
- Showing SNTP Configuration Information

Configuring a Primary or Secondary SNTP Server

The CSS can receive the time from an SNTP server. You can configure up to two SNTP servers on the CSS. The primary server is the main server from which the CSS receives the time. You can configure an additional server, a secondary server, that acts as a backup server if the primary SNTP server is unavailable.

For the CSS to receive the time from an SNTP server, you must configure the IP address for the server through the **sntp** command. You can configure a primary, or secondary server, or both. You can also configure the version of SNTP that the server is using. The syntax for this command is:

```
sntp primary-server | secondary-server ip_address {version number}
```

The keywords, options, and variables are:

- **primary-server** - Configures the server as the primary SNTP server.
- **secondary-server** - Configures the server as the secondary SNTP server.
- *ip_address* - The IP address for the SNTP server. Enter an IP address in dotted-decimal notation (for example, 192.168.1.0).
- **version number** - (Optional) Configures the version number of the SNTP server. The valid *number* entries are 1 to 4. The default is 1.

For example., to configure a primary SNTP server running version 3, enter:

```
(config)# sntp primary-server 192.168.19.21 version 3
```

To remove a primary SNTP server, enter:

```
(config)# no sntp primary-server
```

To configure a secondary SNTP server running version 3, enter:

```
(config)# sntp secondary-server 192.168.19.22 version 3
```

To remove a secondary SNTP server, enter:

```
(config)# no sntp secondary-server
```

Configuring the Poll Interval for the SNTP Server

Continuous polling is critical for the CSS to obtain time from the SNTP server and ensure the local time matches the “real time” of the server. The poll interval is the time in seconds between successive SNTP request messages to the server. By default, this interval is 64 seconds. To configure the poll interval for SNTP request message, use the following command:

```
sntp [primary-server-poll-interval | secondary-server-poll-interval]  
seconds
```

The keywords and variable are:

- **primary-server-poll-interval** - Configures the poll interval for the primary SNTP server.
- **secondary-server-poll-interval** - Configures the poll interval for the secondary SNTP server.
- *seconds* - The poll interval in seconds between successive SNTP request messages to the server. Enter a value from 16 to 16284 seconds. The default is 64 seconds

For example, to specify a poll-interval of 90 seconds for the primary SNTP server, enter:

```
(config)# sntp primary-server-poll-interval 90
```

To reset the poll-interval for the primary SNTP server to the default setting of 64 seconds, enter:

```
(config)# no sntp primary-server-poll-interval
```

Showing SNTP Configuration Information

To display the SNTP configuration information on the CSS, enter the **show sntp global** command. For example:

```
(config)# show sntp global
```

Table 2-3 describes the fields in the **show sntp global** command output.

Table 2-3 *Field Descriptions for the show sntp global Command*

Field	Description
Server	Whether the server is configured as a primary or secondary server.
Server Address	The IP address for the SNTP server. This field also indicate whether the server is configured as a primary or secondary server.
Version	The version number of the server. The default is 1.
Poll Interval	The time in seconds between SNTP request messages. The range is 16 to 16284. The default is 64.
TimeSinceLastUpdate	The time in seconds since the last server reply.
Server Status	The operating status of the SNTP server, UP or DOWN. After the CSS fails to connect to the SNTP server three consecutive times, the CSS marks the SNTP state as DOWN.

Configuring a Host Name

The Host table is the static mapping of mnemonic host names to IP addresses, which is analogous to the ARP table. Use the **host** command to manage entries in the Host table of the CSS.

The syntax for this global configuration mode command is:

```
host host_name ip_address
```

The variables are as follows:

- *host_name* - The name of the host. Enter an unquoted text string with no spaces and a length from 1 to 16 characters.
- *ip_address* - The address associated with the host name. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1).

To add a host to the Host table, the host name must not exist in the Host table. To change a current host address, remove the host name and then add it again to the Host table with the new address.

For example:

```
(config)# host CSS11501-LML 192.168.3.6
```

To remove the existing host from the Host table, enter:

```
(config)# no host CSS11501-LML
```

To display a list of host names, enter:

```
(config)# show running-config global
```

Where to Go Next

Chapter 3, Configuring the Domain Name Service, provides information to configure the Domain Name Service (DNS), the facility that translates host names such as myhost.mydomain.com to IP addresses.



Configuring the Domain Name Service

This chapter provides information to configure the Domain Name Service (DNS), the facility that translates host names such as `myhost.mydomain.com` to IP addresses such as `192.168.11.1`. This chapter contains the following major sections:

- Specifying a Primary DNS Server
- Using DNS Resolve
- Specifying a Secondary DNS Server
- Specifying a DNS Suffix
- Specifying UDP Traffic on the DNS Server Port

Use the **show running-config global** command to display DNS configurations (refer to the *Cisco Content Services Switch Administration Guide*).

Specifying a Primary DNS Server

To specify the primary DNS server, use the **dns primary** command. Enter the IP address in dotted-decimal notation (for example, `192.168.11.1`) of the DNS server you want to specify as the primary DNS server.

For example:

```
(config)# dns primary 192.168.11.1
```

To remove the primary DNS server, enter:

```
(config)# no dns primary
```

Using DNS Resolve

To resolve a host name by querying the DNS server, use the **dns resolve** command. Enter the host name you want to resolve in mnemonic host-name format (for example, myhost.mydomain.com).

For example:

```
(config)# dns resolve fred.arrowpoint.com
```

Specifying a Secondary DNS Server

When a primary DNS server fails, the CSS uses the secondary DNS server to resolve host names to IP addresses. Use the **dns secondary** command to specify a secondary DNS server. Enter the IP address of the secondary DNS server in dotted-decimal notation (for example, 192.168.11.1).

```
(config)# dns secondary 192.168.3.6
```

You can specify a maximum of two secondary servers. To specify each additional server, repeat the **dns secondary** command. The order in which you enter the IP addresses is the order in which they are used when the primary DNS server fails.

To remove a secondary DNS server, specify the **no** version of the command followed by the IP address of the DNS server you wish to remove. For example:

```
(config)# no dns secondary 192.168.3.6
```

Specifying a DNS Suffix

To specify the default suffix to use when querying the DNS facility, use the **dns suffix** command. Enter the default suffix as an unquoted text string with no spaces and a maximum of 64 characters.

For example:

```
(config)# dns suffix arrowpoint.com
```

To remove the default DNS suffix, enter:

```
(config)# no dns suffix
```

Specifying UDP Traffic on the DNS Server Port

By default, the CSS sets up flows using FCBs for DNS requests and responses. For DNS UDP traffic on port 53, use the **dnsflow** command to determine whether the CSS uses flow control blocks (FCBs) for DNS requests and responses. This command provides the following options:

- **enable** (default) - This command has been removed from the CLI. Use the **flow-state** command instead. For details about the **flow-state** command, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.
- **disable** - This command has been deprecated (obsoleted). This option maps to the **flow-state 53 udp flow-disable nat-enable** command. For details about the **flow-state** command, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

Where to Go Next

Chapter 4, Configuring Sticky Cookies, provides information to configure CSS sticky using cookies.



Configuring Sticky Cookies

This chapter provides information on CSS sticky using cookies.

- Sticky Overview
- Advanced Load-Balancing Method Using Cookies

For detailed information on services, sticky parameters and their uses, and Layer 3, Layer 4, and Layer 5 sticky, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

Sticky Overview

When customers visit an e-commerce site, they usually start out by browsing the site, the Internet equivalent of window shopping. Depending on the application, the site may require that the customer become “stuck” to one server once the connection is established, or the application may not require this until the customer starts to build a shopping cart.

In either case, once the customer adds items to the shopping cart, it is important that all of the customer’s requests get directed to the same server so that all the items are contained in one shopping cart on one server. An instance of a customer's shopping cart is typically local to a particular Web server and is not duplicated across multiple servers.

Stickiness is the association between a client and a server that the CSS maintains during a session. Stickiness enables transactions over the Web because the client must remain on the same server for the entire session. Depending on the content rule, the CSS “sticks” a client to an appropriate server after the CSS has determined which load-balancing method to use.

If the CSS determines that a client is already stuck to a particular service, then the CSS places the client request on that service, regardless of the load balancing criteria specified by the matched content rule. If the CSS determines that the client is not stuck to a particular service, it applies normal load balancing to the content request.

Client *cookies* uniquely identify clients to the services providing content. A cookie is a small data structure used by a server to deliver data to a Web client and request that the client store the information. In certain applications, the client returns the information to the server to maintain the state between the client and the server.

When the CSS examines a request for content and determines through content rule matching that the content is sticky, it examines any cookie or URL present in the content request. The CSS uses this information to place the content request on the appropriate server.

Advanced Load-Balancing Method Using Cookies

A content rule is “sticky” when additional sessions from the same user or client are sent to the same service as the first connection, overriding normal load balancing. By default, the advanced balancing method is disabled.

Use the **advanced-balance** command to specify an advanced load-balancing method for a content rule that includes stickiness. The **advanced-balance** command options (**cookies**, **cookieurl**, and **url**) use strings for sticking clients to servers. These options are beneficial when the sticky table limit is too small for your application requirements because the string methods do not use the sticky table.

The following sections provide configuration information for:

- Sticky Based on a Configured String in an HTTP Cookie Header, using the **advance-balanced cookies** command
- Sticky Based on a Cookie in a URL, using the **advance-balanced url** command
- Sticky Based on a Cookie in the HTTP Header or URL, using the **advance-balanced cookieurl** command

For information on additional advanced load-balancing methods including arrowpoint cookies, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

Sticky Based on a Configured String in an HTTP Cookie Header

If the server returns a cookie that is static and uniquely identifies itself, use the **advanced-balance cookies** command. This command enables the content rule to stick a client to a server based on the configured string found in the HTTP cookie header. A content rule with a sticky configuration set to **advanced-balance cookies** requires all clients to enable cookies on their browser.

In the following configuration, the CSS looks for the cookie in the Cookie: field of the HTTP header:

1. The CSS looks for the configured string prefix, which is the cookie name. In this example, the string prefix in the content rule is MyCookie=.
2. If the CSS finds the prefix, then it looks for the value that matches one of the string values configured in one of the services. For example, the string value for service test 1 is server1. The CSS begins searching for the prefix and value at the beginning of the cookie field in the header and searches the entire field until the end of the field.

If the HTTP header spans multiple packets, the CSS searches up to 5 packets by default; however, you can configure the CSS to search up to 20 packets (refer to the global **spanning-packets** command for more details).

- If the CSS cannot find the string prefix or match the cookie value with one of the service string values, then the CSS load balances the request according to the configured balance method (roundrobin by default). For more details on what action the CSS takes when it cannot locate the cookie header or the specified cookie string, see the content rule mode **sticky-no-cookie-found-action** command.

configure

```

!***** GLOBAL *****
ip route 0.0.0.0 0.0.0.0 10.86.191.174 1

!***** INTERFACE *****
interface 3/2
  bridge vlan 2

!***** CIRCUIT *****
circuit VLAN1
  description "client vlan"

  ip address 10.86.191.161 255.255.255.240

circuit VLAN2
  description "server vlan"

  ip address 10.1.1.254 255.255.0.0

!The string value configured in the service must match the value of
the cookie for a particular server.
!***** SERVICE *****
service test1
  ip address 10.1.1.1
  string server1
  active

service test2
  ip address 10.1.1.2
  string server2
  active

service test3
  ip address 10.1.1.3
  string server3
  active

```

```

service test4
  ip address 10.1.1.4
  string server4
  active

!The string prefix must match the cookie name. We recommend that you
include the '=' as part of the string prefix.
!***** OWNER *****

owner test

content stickyCookie
  advanced-balance cookies
  string prefix "MyCookie="
  add service test1
  add service test2
  add service test3
  add service test4
  port 80
  protocol tcp
active

```

Sticky Based on a Cookie in a URL

If the cookie is present in the URL instead of the cookie field of the HTTP header, use the **advanced-balance url** command. Some client applications do not accept cookies. When a site depends upon the information in the cookie, administrators sometimes modify the server application so that it appends the cookie data to the parameters section of the URL. The parameters typically follow a “?” at the end of the main data section of the URL.

In this configuration, the CSS functions in a similar manner as when using the **advanced-balance cookies** command; however, the CSS looks in the URL after the “?” for the cookie.

Using the full configuration of the “Sticky Based on a Configured String in an HTTP Cookie Header” section, the only difference is the **advanced-balance url** command in the content rule.

```

!***** OWNER *****
owner test

content stickyCookie
  advanced-balance url

```

```

string prefix "MyCookie="
add service test1
add service test2
add service test3
add service test4
port 80
protocol tcp
active

```

Sticky Based on a Cookie in the HTTP Header or URL

If the cookie could be in either the cookie field of the HTTP header or the URL, use the **advanced-balance cookieurl** command.

In this configuration, the CSS searches for the cookie first in the cookie field of the HTTP header. If the cookie field does not exist, then the CSS looks for the cookie in the URL. This command is intended for applications where some clients cannot accept cookies but others can.

Using the full configuration of the “Sticky Based on a Configured String in an HTTP Cookie Header” section, the only difference is the **advanced-balance cookieurl** command in the content rule.

```

!***** OWNER *****
owner test

content stickyCookie
  advanced-balance cookieurl
  string prefix "MyCookie="
  add service test1
  add service test2
  add service test3
  add service test4
  port 80
  protocol tcp
active

```

Where to Go Next

Chapter 5, Installing the CiscoView Device Manager on the CSS, provides information about installing the CSS Manager, a browser-based graphical user interface, to perform switch and load balancing configuration tasks.



Where to Go Next

This chapter provides information on where to go next to administer and configure the CSS. The chapter consists of the following major sections:

- **CSS Task Topic List** - Provides a list of administrative and configuration task topics in alphabetical order and the location of the topic in the CSS guides.
- **Comprehensive CSS Documentation List** - Provides detailed outlines for each of the CSS administration, configuration, and user guides.

CSS Task Topic List

Table 5-1 provides a list of CSS administrative and configuration task topics in alphabetical order and the location of the topics in the CSS documentation. For more concise lists of topics, refer to the index of each document.

Table 5-1 Administration and Configuration Task Topic List

Task Topic	Guide and Chapter
Absolute load configuration with quick start	CSS Content Load-Balancing Configuration Guide Chapter 6, Configuring Loads for Services
ACA load-balancing algorithm configuration	CSS Content Load-Balancing Configuration Guide Chapter 6, Configuring Loads for Services
Accelerated domains configuration	CSS Global Server Load-Balancing Configuration Guide Chapter 4, Configuring a Client-Side Accelerator

Table 5-1 Administration and Configuration Task Topic List (continued)

Task Topic	Guide and Chapter
Access Control Lists (ACLs) configuration with quick start	CSS Security Configuration Guide Chapter 1, Controlling CSS Access
Access FTP, demand-based content replication and publishing and subscribing	CSS Content Load-Balancing Configuration Guide Chapter 14, Configuring Content Replication
Access to the CSS configuration	CSS Security Configuration Guide Chapter 1, Controlling CSS Access
Access to the CiscoView Device Manager	CSS Getting Started Guide Chapter 5, Installing the CiscoView Device Manager on the CSS
ACLs with source groups configuration	CSS Content Load-Balancing Configuration Guide Chapter 5, Source Groups for Services
Adaptive Session Redundancy (ASR) configuration with quick start, and show command	CSS Redundancy Configuration Guide Chapter 2, Configuring Adaptive Session Redundancy
Address Resolution Protocol (ARP) configuration with quick start, and show command	CSS Routing and Bridging Configuration Guide Chapter 4, Configuring the Address Resolution Protocol
ADI, unpack and remove an ArrowPoint Distribution Image (ADI) to a CSS disk.	CSS Administration Guide Chapter 1, Managing the Software
Administrative access to the CSS configuration	CSS Security Configuration Guide Chapter 1, Controlling CSS Access
Administrative username and password configuration	CSS Administration Guide Appendix B, Using the Offline Diagnostic Monitor Menu
Administrative username and password configuration	CSS Security Configuration Guide Chapter 1, Controlling CSS Access
Advanced load-balancing method for sticky content configuration	CSS Content Load-Balancing Configuration Guide Chapter 11, Configuring Sticky Parameters for Content Rules

Table 5-1 Administration and Configuration Task Topic List (continued)

Task Topic	Guide and Chapter
Advertise a route through RIP on the CSS configuration	CSS Routing and Bridging Configuration Guide Chapter 5, Configuring Routing Information Protocol
Application Peering Protocol (APP) configuration, and show command	CSS Global Server Load-Balancing Configuration Guide Chapter 1, Configuring the CSS as a Domain Name System Server
Application Peering Protocol-User Datagram Protocol (APP-UDP) configuration	CSS Global Server Load-Balancing Configuration Guide Chapter 5, Configuring Network Proximity
Application type configuration	CSS Content Load-Balancing Configuration Guide Chapter 10, Configuring Content Rules
Archive file configuration	CSS Administration Guide Chapter 1, Managing the Software
ARP configuration with quick start, and show command	CSS Routing and Bridging Configuration Guide Chapter 4, Configuring the Address Resolution Protocol
ArrowPoint Content Awareness (ACA) load-balancing algorithm configuration	CSS Content Load-Balancing Configuration Guide Chapter 6, Configuring Loads for Services
ArrowPoint cookies configuration	CSS Content Load-Balancing Configuration Guide Chapter 11, Configuring Sticky Parameters for Content Rules
ASR configuration with quick start, and show command	CSS Redundancy Configuration Guide Chapter 2, Configuring Adaptive Session Redundancy
Back-end SSL configuration	CSS SSL Configuration Guide Chapter 5, Configuring Back-End SSL
Back-end SSL proxy list quick start	CSS SSL Configuration Guide Chapter 2, SSL Configuration Quick Starts
Backup CSS as a master temporarily	CSS Redundancy Configuration Guide Chapter 3, Configuring Box-to-Box Redundancy

Table 5-1 Administration and Configuration Task Topic List (continued)

Task Topic	Guide and Chapter
Banner (login) configuration	CSS Administration Guide Chapter 3, Configuring User Profiles
Boot configuration	CSS Administration Guide Appendix B, Using the Offline Diagnostic Monitor Menu
Boot configuration with quick start and show command	CSS Administration Guide Chapter 2, Specifying the CSS Boot Configuration
Box-to-box redundancy configuration	CSS Redundancy Configuration Guide Chapter 3, Configuring Box-to-Box Redundancy
BPDU guard configuration	CSS Routing and Bridging Configuration Guide Chapter 1, Configuring Interfaces and Circuits
Bridge interface to a VLAN circuit configuration	CSS Routing and Bridging Configuration Guide Chapter 1, Configuring Interfaces and Circuits
Bypass cache configuration	CSS Content Load-Balancing Configuration Guide Chapter 13, Configuring Caching
Bypass content rules on caches configuration	CSS Content Load-Balancing Configuration Guide Chapter 3, Configuring Services
CA certificates for server authentication configuration	CSS SSL Configuration Guide Chapter 6, Configuring SSL Initiation
Cable redundant CSS configuration	CSS Redundancy Configuration Guide Chapter 3, Configuring Box-to-Box Redundancy
Caching configuration with quick start	CSS Content Load-Balancing Configuration Guide Chapter 13, Configuring Caching
CDP configuration with quick start, and show command	CSS Routing and Bridging Configuration Guide Chapter 7, Configuring the Cisco Discovery Protocol
Certificates and keys (SSL) configuration and verification	CSS SSL Configuration Guide Chapter 3, Configuring SSL Certificates and Keys

Table 5-1 Administration and Configuration Task Topic List (continued)

Task Topic	Guide and Chapter
Circuits Virtual LAN (VLAN) configuration, and show command	CSS Routing and Bridging Configuration Guide Chapter 1, Configuring Interfaces and Circuits
Cisco Discovery Protocol (CDP) configuration with quick start, and show command	CSS Routing and Bridging Configuration Guide Chapter 7, Configuring the Cisco Discovery Protocol
CLI prompt configuration	CSS Administration Guide Chapter 3, Configuring User Profiles
Client authentication configuration	CSS SSL Configuration Guide Chapter 4, Configuring SSL Termination
Client certificate and keys configuration	CSS SSL Configuration Guide Chapter 6, Configuring SSL Initiation
Client-Side Accelerator (CSA) configuration with quick start, and show command	CSS Global Server Load-Balancing Configuration Guide Chapter 4, Configuring a Client-Side Accelerator
Command history buffer configuration	CSS Administration Guide Chapter 3, Configuring User Profiles
Command scheduler configuration	CSS Administration Guide Chapter 8, Using the CSS Scripting Language.
Compression, HTTP response data	CSS SSL Configuration Guide Chapter 9, Configuring HTTP Compression
Configuration changes, saved for subsequent CSS reboots.	CSS Administration Guide Chapter 1, Managing the Software
Configuration synchronization configuration	CSS Redundancy Configuration Guide Chapter 3, Configuring Box-to-Box Redundancy
Consistent weight range among services (DFP) configuration	CSS Content Load-Balancing Configuration Guide Chapter 8, Configuring Dynamic Feedback Protocol for Server Load Balancing

Table 5-1 Administration and Configuration Task Topic List (continued)

Task Topic	Guide and Chapter
Console authentication configuration	CSS Security Configuration Guide Chapter 1, Controlling CSS Access
Content API configuration	CSS Administration Guide Chapter 7, Using an XML Document to Configure the CSS
Content Routing Agent (CRA) configuration with quick start, and show command	CSS Global Server Load-Balancing Configuration Guide Chapter 3, Configuring a CSS as a Content Routing Agent
Content rule overview	CSS Content Load-Balancing Configuration Guide Chapter 1, Content Load-Balancing Overview
Content rule-based DNS configuration with quick start and show command	CSS Global Server Load-Balancing Configuration Guide Chapter 1, Configuring the CSS as a Domain Name System Server
Content rules configuration with quick start, and show command	CSS Content Load-Balancing Configuration Guide Chapter 10, Configuring Content Rules
Content staging and replication configuration with quick start	CSS Content Load-Balancing Configuration Guide Chapter 14, Configuring Content Replication
Cookies for advanced load-balancing configuration	CSS Content Load-Balancing Configuration Guide Chapter 11, Configuring Sticky Parameters for Content Rules
Copy files from FTP server configuration	CSS Administration Guide Chapter 1, Managing the Software
Core dumps configuration	CSS Administration Guide Chapter 1, Managing the Software
CRA configuration with quick start, and show command	CSS Global Server Load-Balancing Configuration Guide Chapter 3, Configuring a CSS as a Content Routing Agent
Critical phy configuration with quick start	CSS Redundancy Configuration Guide Chapter 1, Configuring VIP and Virtual Interface Redundancy

Table 5-1 Administration and Configuration Task Topic List (continued)

Task Topic	Guide and Chapter
Critical services configuration	CSS Redundancy Configuration Guide Chapter 3, Configuring Box-to-Box Redundancy
CRL record show command	CSS SSL Configuration Guide Chapter 7, Displaying SSL Configuration Information and Statistics
Crossover cable pinouts for box-to-box redundancy	CSS Redundancy Configuration Guide Chapter 3, Configuring Box-to-Box Redundancy
CSA configuration with quick start, and show command	CSS Global Server Load-Balancing Configuration Guide Chapter 4, Configuring a Client-Side Accelerator
Clock configuration	CSS Getting Started Guide Chapter 2, Configuring CSS Basics
Daylight savings time	CSS Getting Started Guide Chapter 2, Configuring CSS Basics
Demand-based content replication configuration with quick start	CSS Content Load-Balancing Configuration Guide Chapter 14, Configuring Content Replication
Denial of Service (DoS) configuration using SNMP	CSS Administration Guide Chapter 5, Configuring Simple Network Management Protocol (SNMP)
Destination service for source group configuration	CSS Content Load-Balancing Configuration Guide Chapter 5, Source Groups for Services
DFP agent configuration, and show command	CSS Content Load-Balancing Configuration Guide Chapter 8, Configuring Dynamic Feedback Protocol for Server Load Balancing
DHCP Relay Agent configuration with quick start, and show command	CSS Routing and Bridging Configuration Guide Chapter 8, Configuring the DHCP Relay Agent

Table 5-1 Administration and Configuration Task Topic List (continued)

Task Topic	Guide and Chapter
Disk configuration	CSS Administration Guide Chapter 1, Managing the Software
	CSS Administration Guide Appendix B, Using the Offline Diagnostic Monitor Menu
DNS configuration to a zone-based DNS content rule based configuration, conversion	CSS Global Server Load-Balancing Configuration Guide Chapter 2, Configuring the DNS Sticky Feature
DNS peering and DNS server configuration including DNS record	CSS Global Server Load-Balancing Configuration Guide Chapter 1, Configuring the CSS as a Domain Name System Server
DNS server forwarder	CSS Global Server Load-Balancing Configuration Guide Chapter 4, Configuring a Client-Side Accelerator
DNS Sticky configuration with quick start, and show command	CSS Global Server Load-Balancing Configuration Guide Chapter 2, Configuring the DNS Sticky Feature
DNS-based content rule configuration	CSS Global Server Load-Balancing Configuration Guide Chapter 1, Configuring the CSS as a Domain Name System Server
Domain cache configuration	CSS Global Server Load-Balancing Configuration Guide Chapter 4, Configuring a Client-Side Accelerator
Domain name content rule	CSS Content Load-Balancing Configuration Guide Chapter 10, Configuring Content Rules
Domain Name System (DNS) Sticky feature, see DNS sticky	CSS Global Server Load-Balancing Configuration Guide Chapter 2, Configuring the DNS Sticky Feature
Domain qualifier list (DQL) and virtual web hosting including a quick start	CSS Content Load-Balancing Configuration Guide Chapter 10, Configuring Content Rules
Domain record configuration, DNS server	CSS Global Server Load-Balancing Configuration Guide Chapter 1, Configuring the CSS as a Domain Name System Server

Table 5-1 Administration and Configuration Task Topic List (continued)

Task Topic	Guide and Chapter
Domain records configuration, network proximity	CSS Global Server Load-Balancing Configuration Guide Chapter 5, Configuring Network Proximity
Double-wildcard caching rule configuration	CSS Content Load-Balancing Configuration Guide Chapter 13, Configuring Caching
DQL configuration including a quick start	CSS Content Load-Balancing Configuration Guide Chapter 10, Configuring Content Rules
Dynamic Feedback Protocol (DFP) agent configuration, and show command	CSS Content Load-Balancing Configuration Guide Chapter 8, Configuring Dynamic Feedback Protocol for Server Load Balancing
ECMP configuration	CSS Routing and Bridging Configuration Guide Chapter 6, Configuring the Internet Protocol
E-commerce sticky configuration	CSS Content Load-Balancing Configuration Guide Chapter 11, Configuring Sticky Parameters for Content Rules
Ethernet management port configuration	CSS Getting Started Guide Chapter 2, Configuring CSS Basics
Ethernet interface configuration	CSS Routing and Bridging Configuration Guide Chapter 1, Configuring Interfaces and Circuits
Expert mode configuration	CSS Administration Guide Chapter 3, Configuring User Profiles
Extension qualifier lists (EQL) configuration	CSS Content Load-Balancing Configuration Guide Chapter 10, Configuring Content Rules
Failover handling configuration	CSS Content Load-Balancing Configuration Guide Chapter 10, Configuring Content Rules
File storage locations configuration	CSS Administration Guide Chapter 1, Managing the Software

Table 5-1 Administration and Configuration Task Topic List (continued)

Task Topic	Guide and Chapter
Firewall IP route configuration	CSS Routing and Bridging Configuration Guide Chapter 6, Configuring the Internet Protocol
Firewall Load Balancing (FWLB) configuration, and show command	CSS Security Configuration Guide Chapter 5, Configuring Firewall Load Balancing
Flow and port mapping configuration including inactivity timeouts and flow-state table, and show command	CSS Content Load-Balancing Configuration Guide Chapter 2, Configuring Flow and Port Mapping Parameters
Flow on the CSS overview	CSS Content Load-Balancing Configuration Guide Chapter 1, Content Load-Balancing Overview
Forward IP subnet broadcast addressed frames configuration	CSS Routing and Bridging Configuration Guide Chapter 6, Configuring the Internet Protocol
Fragmented IP packets flow processing configuration	CSS Content Load-Balancing Configuration Guide Chapter 2, Configuring Flow and Port Mapping Parameters
FTP access for demand-based content replication and publishing and subscribing	CSS Content Load-Balancing Configuration Guide Chapter 14, Configuring Content Replication
FTP connections through source groups configuration	CSS Content Load-Balancing Configuration Guide Chapter 5, Source Groups for Services
FTP record configuration	CSS Administration Guide Chapter 1, Managing the Software
FTP reserved control port reclamation configuration	CSS Content Load-Balancing Configuration Guide Chapter 2, Configuring Flow and Port Mapping Parameters
FWLB with VIP and virtual interface redundancy configuration	CSS Security Configuration Guide Chapter 5, Configuring Firewall Load Balancing
Global keepalives configuration with quick start	CSS Content Load-Balancing Configuration Guide Chapter 4, Configuring Service, Global, and Script Keepalives

Table 5-1 Administration and Configuration Task Topic List (continued)

Task Topic	Guide and Chapter
Global service loads show command	CSS Content Load-Balancing Configuration Guide Chapter 6, Configuring Loads for Services
Global sticky database configuration with quick start, and show command	CSS Global Server Load-Balancing Configuration Guide Chapter 2, Configuring the DNS Sticky Feature
Graceful shutdown of an overloaded service configuration	CSS Content Load-Balancing Configuration Guide Chapter 3, Configuring Services
Hash algorithms for content rules configuration	CSS Content Load-Balancing Configuration Guide Chapter 10, Configuring Content Rules
Header field group configuration with quick start, and show command	CSS Content Load-Balancing Configuration Guide Chapter 12, Configuring HTTP Header Load Balancing
Hot list configuration	CSS Content Load-Balancing Configuration Guide Chapter 10, Configuring Content Rules
HTTP compression	CSS SSL Configuration Guide Chapter 9, Configuring HTTP Compression
HTTP encrypted keepalives	CSS Content Load-Balancing Configuration Guide Chapter 4, Configuring Service, Global, and Script Keepalives CSS SSL Configuration Guide Chapter 5, Configuring Back-End SSL
HTTP method parsing	CSS Content Load-Balancing Configuration Guide Chapter 10, Configuring Content Rules
Hot list configuration	CSS Content Load-Balancing Configuration Guide Chapter 10, Configuring Content Rules
HTTP redirection configuration	CSS Content Load-Balancing Configuration Guide Chapter 10, Configuring Content Rules
Implicit service for the static route next hop configuration	CSS Routing and Bridging Configuration Guide Chapter 6, Configuring the Internet Protocol

Table 5-1 Administration and Configuration Task Topic List (continued)

Task Topic	Guide and Chapter
Interface configuration, and show command	CSS Routing and Bridging Configuration Guide Chapter 1, Configuring Interfaces and Circuits
Internet Protocol configuration with quick start, and show command	CSS Routing and Bridging Configuration Guide Chapter 6, Configuring the Internet Protocol
Inter-Switch Communications (ISC) redundant services configuration	CSS Redundancy Configuration Guide Chapter 2, Configuring Adaptive Session Redundancy
IP equal-cost multipath (ECMP) selection algorithm and the preferred reverse egress path configuration	CSS Routing and Bridging Configuration Guide Chapter 6, Configuring the Internet Protocol
IP fragmentation configuration	CSS Content Load-Balancing Configuration Guide Chapter 2, Configuring Flow and Port Mapping Parameters
IP source, static, and record route configuration	CSS Routing and Bridging Configuration Guide Chapter 6, Configuring the Internet Protocol
Kal-ap-vip client and agent configuration	CSS Global Server Load-Balancing Configuration Guide Chapter 1, Configuring the CSS as a Domain Name System Server
Keepalives configuration, and show command	CSS Content Load-Balancing Configuration Guide Chapter 4, Configuring Service, Global, and Script Keepalives
Load configuration (absolute and relative)	CSS Content Load-Balancing Configuration Guide Chapter 6, Configuring Loads for Services
Load-balancing algorithm for content rule configuration	CSS Content Load-Balancing Configuration Guide Chapter 10, Configuring Content Rules
Location cookie configuration	CSS Content Load-Balancing Configuration Guide Chapter 11, Configuring Sticky Parameters for Content Rules
Logging configuration, and show command	CSS Administration Guide Chapter 4, Using the CSS Logging Features

Table 5-1 Administration and Configuration Task Topic List (continued)

Task Topic	Guide and Chapter
Maximum segment size (MSS) for TCP data configuration	CSS Content Load-Balancing Configuration Guide Chapter 2, Configuring Flow and Port Mapping Parameters
MIBs, overview	CSS Administration Guide Chapter 5, Configuring Simple Network Management Protocol (SNMP)
MIBs, update	CSS Administration Guide Appendix A, Upgrading Your CSS Software
NAT peering configuration with quick start	CSS Content Load-Balancing Configuration Guide Chapter 13, Configuring Caching
Network Address Translation (NAT) for the transparent cache service type configuration	CSS Content Load-Balancing Configuration Guide Chapter 3, Configuring Services
Network Address Translation (NAT) source group configuration	CSS Content Load-Balancing Configuration Guide Chapter 5, Source Groups for Services
Network boot drive configuration	CSS Administration Guide Chapter 2, Specifying the CSS Boot Configuration
Network proximity configuration	CSS Global Server Load-Balancing Configuration Guide Chapter 5, Configuring Network Proximity
Network Qualifier Lists (NQL) for ACLs configuration	CSS Security Configuration Guide Chapter 1, Controlling CSS Access
noflow port mapping configuration	CSS Content Load-Balancing Configuration Guide Chapter 2, Configuring Flow and Port Mapping Parameters
Offline Diagnostic Monitor Menu	CSS Administration Guide Appendix B, Using the Offline Diagnostic Monitor Menu
Opportunistic Layer 3 forwarding configuration	CSS Routing and Bridging Configuration Guide Chapter 6, Configuring the Internet Protocol

Table 5-1 Administration and Configuration Task Topic List (continued)

Task Topic	Guide and Chapter
OSPF configuration with quick start, and show command	CSS Routing and Bridging Configuration Guide Chapter 3, Configuring Open Shortest Path First (OSPF)
Owner configuration, and show command	CSS Content Load-Balancing Configuration Guide Chapter 9, Configuring Owners
Owner overview	CSS Content Load-Balancing Configuration Guide Chapter 1, Content Load-Balancing Overview
Passive SCM configuration	CSS Administration Guide Chapter 2, Specifying the CSS Boot Configuration
Permanent TCP and UDP port connection configuration	CSS Content Load-Balancing Configuration Guide Chapter 2, Configuring Flow and Port Mapping Parameters
Persistence configuration	CSS Content Load-Balancing Configuration Guide Chapter 10, Configuring Content Rules
Physical link configuration list	CSS Redundancy Configuration Guide Chapter 3, Configuring Box-to-Box Redundancy
Port Fast configuration	CSS Routing and Bridging Configuration Guide Chapter 1, Configuring Interfaces and Circuits
Port mapping configuration (source groups)	CSS Content Load-Balancing Configuration Guide Chapter 5, Source Groups for Services
Port mapping configuration, and show command (global and noflow)	CSS Content Load-Balancing Configuration Guide Chapter 2, Configuring Flow and Port Mapping Parameters
Primary boot record configuration	CSS Administration Guide Chapter 2, Specifying the CSS Boot Configuration
Primary sorry server configuration	CSS Content Load-Balancing Configuration Guide Chapter 10, Configuring Content Rules
Processing of SSL flows by the SSL module example	CSS SSL Configuration Guide Chapter 8, Examples of CSS SSL Configurations

Table 5-1 Administration and Configuration Task Topic List (continued)

Task Topic	Guide and Chapter
Proximity domain name server (PDNS) configuration, and show command	CSS Global Server Load-Balancing Configuration Guide Chapter 5, Configuring Network Proximity
Proxy cache configuration	CSS Content Load-Balancing Configuration Guide Chapter 13, Configuring Caching
Publishing and subscribing services configuration, and show command	CSS Content Load-Balancing Configuration Guide Chapter 14, Configuring Content Replication
Publishing service, associate an FTP access mechanism with a service	CSS Content Load-Balancing Configuration Guide Chapter 3, Configuring Services
RADIUS configuration with quick start including authentication and authorization	CSS Security Configuration Guide Chapter 3, Configuring the CSS as a Client of a RADIUS Server
Reboot the CSS	CSS Administration Guide Appendix B, Using the Offline Diagnostic Monitor Menu
Reclaim of reserved Telnet and FTP control ports configuration	CSS Content Load-Balancing Configuration Guide Chapter 2, Configuring Flow and Port Mapping Parameters
Redirection requests for content configuration	CSS Content Load-Balancing Configuration Guide Chapter 10, Configuring Content Rules
Redundancy configuration (ASR)	CSS Redundancy Configuration Guide Chapter 2, Configuring Adaptive Session Redundancy
Redundancy configuration (box-to-box)	CSS Redundancy Configuration Guide Chapter 3, Configuring Box-to-Box Redundancy
Redundancy configuration (VIP and virtual interface)	CSS Redundancy Configuration Guide Chapter 1, Configuring VIP and Virtual Interface Redundancy
Relative load configuration with quick start, and show command	CSS Content Load-Balancing Configuration Guide Chapter 6, Configuring Loads for Services

Table 5-1 Administration and Configuration Task Topic List (continued)

Task Topic	Guide and Chapter
Remapping configuration	CSS Content Load-Balancing Configuration Guide Chapter 10, Configuring Content Rules
Remote user access to the CSS including virtual and console authentication	CSS Security Configuration Guide Chapter 1, Controlling CSS Access
Replication and staging configuration with quick start	CSS Content Load-Balancing Configuration Guide Chapter 14, Configuring Content Replication
Reporter mode configuration	CSS Redundancy Configuration Guide Chapter 1, Configuring VIP and Virtual Interface Redundancy
Resolve domain names using the Internet through source groups configuration	CSS Content Load-Balancing Configuration Guide Chapter 5, Source Groups for Services
Restore archived files	CSS Administration Guide Chapter 1, Managing the Software
Restrict access to the CiscoView Device Manager	CSS Getting Started Guide Chapter 5, Installing the CiscoView Device Manager on the CSS
Reverse proxy caching configuration	CSS Content Load-Balancing Configuration Guide Chapter 13, Configuring Caching
RIP for an IP interface configuration	CSS Routing and Bridging Configuration Guide Chapter 1, Configuring Interfaces and Circuits
RMON configuration with quick start, and show command	CSS Administration Guide Chapter 6, Configuring Remote Monitoring (RMON)
Router-Discovery Protocol configuration	CSS Routing and Bridging Configuration Guide Chapter 1, Configuring Interfaces and Circuits
Routing Information Protocol (RIP) configuration with quick start, and show command	CSS Routing and Bridging Configuration Guide Chapter 5, Configuring Routing Information Protocol

Table 5-1 Administration and Configuration Task Topic List (continued)

Task Topic	Guide and Chapter
RSA certificate and key generation and import quick start	CSS SSL Configuration Guide Chapter 2, SSL Configuration Quick Starts
SASP configuration	CSS Content Load-Balancing Configuration Guide Chapter 7, Configuring Server/Application State Protocol for Server Load Balancing
Save configuration changes for subsequent CSS reboots	CSS Administration Guide Chapter 1, Managing the Software
Script keepalives configuration	CSS Content Load-Balancing Configuration Guide Chapter 4, Configuring Service, Global, and Script Keepalives
Scripts configuration, and show command	CSS Administration Guide Chapter 8, Using the CSS Scripting Language.
Secure URL rewrite configuration	CSS SSL Configuration Guide Chapter 4, Configuring SSL Termination
Server/Application State Protocol (SASP) configuration	CSS Content Load-Balancing Configuration Guide Chapter 7, Configuring Server/Application State Protocol for Server Load Balancing
Serverdown failover for sticky configuration	CSS Content Load-Balancing Configuration Guide Chapter 11, Configuring Sticky Parameters for Content Rules
Service configuration with quick start, and show command	CSS Content Load-Balancing Configuration Guide Chapter 3, Configuring Services
Service in CSS ping response decision configuration	CSS Content Load-Balancing Configuration Guide Chapter 10, Configuring Content Rules
Service keepalive configuration	CSS Content Load-Balancing Configuration Guide Chapter 4, Configuring Service, Global, and Script Keepalives

Table 5-1 Administration and Configuration Task Topic List (continued)

Task Topic	Guide and Chapter
Service loads configuration	CSS Content Load-Balancing Configuration Guide Chapter 6, Configuring Loads for Services
Service overview	CSS Content Load-Balancing Configuration Guide Chapter 1, Content Load-Balancing Overview
Service redirection configuration	CSS Content Load-Balancing Configuration Guide Chapter 10, Configuring Content Rules
Service source group configuration	CSS Content Load-Balancing Configuration Guide Chapter 5, Source Groups for Services
Service weight configuration through content rule	CSS Content Load-Balancing Configuration Guide Chapter 10, Configuring Content Rules
Session configuration (global)	CSS Administration Guide Chapter 3, Configuring User Profiles
Session Initiation Protocol load balancing configuration	CSS Content Load-Balancing Configuration Guide Chapter 11, Configuring Sticky Parameters for Content Rules
Shutdown the interfaces	CSS Routing and Bridging Configuration Guide Chapter 1, Configuring Interfaces and Circuits
SIP configuration with quick start	CSS Content Load-Balancing Configuration Guide Chapter 11, Configuring Sticky Parameters for Content Rules
Site certificate configuration	CSS SSL Configuration Guide Chapter 3, Configuring SSL Certificates and Keys
SNMP configuration	CSS Administration Guide Chapter 5, Configuring Simple Network Management Protocol (SNMP)
SNTP configuration	CSS Getting Started Guide Chapter 2, Configuring CSS Basics

Table 5-1 Administration and Configuration Task Topic List (continued)

Task Topic	Guide and Chapter
Sorry server, primary and secondary configuration	CSS Content Load-Balancing Configuration Guide Chapter 10, Configuring Content Rules
Source group configuration with quick start, and show command	CSS Content Load-Balancing Configuration Guide Chapter 5, Source Groups for Services
Spanned packets for content rule configuration	CSS Content Load-Balancing Configuration Guide Chapter 10, Configuring Content Rules
Spanning-tree bridging configuration	CSS Routing and Bridging Configuration Guide Chapter 1, Configuring Interfaces and Circuits
Spanning-tree bridging for the CSS configuration with quick start, and show command	CSS Routing and Bridging Configuration Guide Chapter 2, Configuring Spanning-Tree Bridging for the CSS
SSH configuration, and show command	CSS Security Configuration Guide Chapter 2, Configuring the Secure Shell Daemon Protocol
SSL certificates and keys configuration	CSS SSL Configuration Guide Chapter 3, Configuring SSL Certificates and Keys
SSL client authentication configuration	CSS SSL Configuration Guide Chapter 4, Configuring SSL Termination
SSL flows show command	CSS SSL Configuration Guide Chapter 7, Displaying SSL Configuration Information and Statistics
SSL full proxy configuration example	CSS SSL Configuration Guide Chapter 8, Examples of CSS SSL Configurations
SSL HTTP header insertion configuration	CSS SSL Configuration Guide Chapter 4, Configuring SSL Termination
SSL initiation configuration	CSS SSL Configuration Guide Chapter 6, Configuring SSL Initiation

Table 5-1 Administration and Configuration Task Topic List (continued)

Task Topic	Guide and Chapter
SSL initiation configuration example	CSS SSL Configuration Guide Chapter 8, Examples of CSS SSL Configurations
SSL initiation proxy list quick start	CSS SSL Configuration Guide Chapter 2, SSL Configuration Quick Starts
SSL proxy configuration show command	CSS SSL Configuration Guide Chapter 7, Displaying SSL Configuration Information and Statistics
SSL termination configuration	CSS SSL Configuration Guide Chapter 4, Configuring SSL Termination
SSL termination quick start	CSS SSL Configuration Guide Chapter 2, SSL Configuration Quick Starts
SSL transparent proxy configuration with one SSL module, two SSL module, or HTTP and back-end SSL servers example	CSS SSL Configuration Guide Chapter 8, Examples of CSS SSL Configurations
SSL unclean shutdown (disable Close Notify alert)	CSS SSL Configuration Guide Chapter 4, Configuring SSL Termination
SSL URL rewrite and SSL module statistics show command	CSS SSL Configuration Guide Chapter 7, Displaying SSL Configuration Information and Statistics
SSL, overview	CSS SSL Configuration Guide Chapter 1, Overview of CSS SSL
SSL-Layer 4 fallback configuration	CSS Content Load-Balancing Configuration Guide Chapter 11, Configuring Sticky Parameters for Content Rules
Stateless redundancy failover configuration	CSS Redundancy Configuration Guide Chapter 3, Configuring Box-to-Box Redundancy

Table 5-1 Administration and Configuration Task Topic List (continued)

Task Topic	Guide and Chapter
Sticky configuration, and show command	CSS Content Load-Balancing Configuration Guide Chapter 11, Configuring Sticky Parameters for Content Rules
Subscriber service configuration and show command	CSS Content Load-Balancing Configuration Guide Chapter 14, Configuring Content Replication
Switched Port Analyzer feature	CSS Routing and Bridging Configuration Guide Chapter 1, Configuring Interfaces and Circuits
Synchronize redundant configuration	CSS Redundancy Configuration Guide Chapter 3, Configuring Box-to-Box Redundancy
TACACS+ configuration including authentication and authorization, quick start, and show command	CSS Security Configuration Guide Chapter 4, Configuring the CSS as a Client of a TACACS+ Server
TCP and UDP traffic handled by the CSS overview (3-way handshake)	CSS Content Load-Balancing Configuration Guide Chapter 1, Content Load-Balancing Overview
TCP flow reset reject configuration	CSS Content Load-Balancing Configuration Guide Chapter 10, Configuring Content Rules
TCP reset if a VIP is unavailable configuration	CSS Content Load-Balancing Configuration Guide Chapter 2, Configuring Flow and Port Mapping Parameters
Telnet access configuration	CSS Security Configuration Guide Chapter 1, Controlling CSS Access
Terminal configuration	CSS Administration Guide Chapter 3, Configuring User Profiles
Trap configuration and logs	CSS Administration Guide Chapter 5, Configuring Simple Network Management Protocol (SNMP)
Troubleshoot SSL initiation	CSS SSL Configuration Guide Chapter 6, Configuring SSL Initiation

Table 5-1 Administration and Configuration Task Topic List (continued)

Task Topic	Guide and Chapter
UDP traffic handled by the CSS overview	CSS Content Load-Balancing Configuration Guide Chapter 1, Content Load-Balancing Overview
Unconditional bridging configuration	CSS Routing and Bridging Configuration Guide Chapter 6, Configuring the Internet Protocol
Uniform Resource Locator (URL) for content rule configuration	CSS Content Load-Balancing Configuration Guide Chapter 10, Configuring Content Rules
Uniform Resource Locator qualifier list (URQL) configuration with quick start	CSS Content Load-Balancing Configuration Guide Chapter 10, Configuring Content Rules
Upgrade the CSS software	CSS Administration Guide Appendix A, Upgrading Your CSS Software
User profile configuration with quick start	CSS Administration Guide Chapter 3, Configuring User Profiles
Usernames and password configuration	CSS Security Configuration Guide Chapter 1, Controlling CSS Access
VIP and virtual interface redundancy configuration with quick start	CSS Redundancy Configuration Guide Chapter 1, Configuring VIP and Virtual Interface Redundancy
Virtual authentication configuration	CSS Security Configuration Guide Chapter 1, Controlling CSS Access
Virtual SSL servers for the SSL termination configuration	CSS SSL Configuration Guide Chapter 4, Configuring SSL Termination
Virtual web hosting configuration	CSS Content Load-Balancing Configuration Guide Chapter 10, Configuring Content Rules
VLAN trunking configuration	CSS Routing and Bridging Configuration Guide Chapter 1, Configuring Interfaces and Circuits

Table 5-1 Administration and Configuration Task Topic List (continued)

Task Topic	Guide and Chapter
VRID peering configuration	CSS Redundancy Configuration Guide Chapter 1, Configuring VIP and Virtual Interface Redundancy
Wireless users for E-commerce applications configuration	CSS Content Load-Balancing Configuration Guide Chapter 11, Configuring Sticky Parameters for Content Rules
XML access to the CSS	CSS Security Configuration Guide Chapter 1, Controlling CSS Access
XML configuration	CSS Administration Guide Chapter 7, Using an XML Document to Configure the CSS
Zone-based DNS on a CSS configuration with quick start	CSS Global Server Load-Balancing Configuration Guide Chapter 1, Configuring the CSS as a Domain Name System Server

Comprehensive CSS Documentation List

This section contains information for the following CSS documentation:

- Cisco Content Services Switch Administration Guide
- Cisco Content Services Switch Routing and Bridging Configuration Guide
- Cisco Content Services Switch Content Load-Balancing Configuration Guide
- Cisco Content Services Switch Global Server Load-Balancing Configuration Guide
- Cisco Content Services Switch Redundancy Configuration Guide
- Cisco Content Services Switch Security Configuration Guide
- Cisco Content Services Switch SSL Configuration Guide

For information on CSS CLI commands, refer to the *Cisco Content Services Switch Command Reference*. This reference provides an alphabetical list of all CLI commands including syntax, options, and related commands.

Cisco Content Services Switch Administration Guide

This guide describes how to perform administrative tasks on the CSS, including managing and upgrading your CSS software. Table 5-2 lists the chapters and appendices in this guide, and a description of their contents and tasks.

Table 5-2 Cisco Content Services Switch Administration Guide

Chapter	Contents/Tasks
Chapter 1, Managing the Software	<ul style="list-style-type: none"> • Overview of CSS system software • Creating an FTP record to access an FTP server from the CSS and how to copy files from the server • Saving configuration changes for subsequent CSS reboots. • Configuring file storage locations for a two-disk 11500 series CSS. These tasks include formatting a disk, defining which disk is the boot disk and where to save the log files and core dumps, and copying files between the disks. • Unpacking and removing an ArrowPoint Distribution Image (ADI) to a CSS disk. • Archiving files to the CSS archive directory and then restoring them. • Enabling and handling core dumps. • Displaying the system information for the CSS.
Chapter 2, Specifying the CSS Boot Configuration	<ul style="list-style-type: none"> • Boot setup quick start. • Accessing boot configuration mode and its commands. • Configuring a primary location from which the CSS accesses the boot image • Configuring a secondary location from which the CSS accesses the boot image when the primary boot configuration fails. • Configuring the individual components of the boot configuration record on the passive SCM installed in a CSS 11506 chassis. A passive module is a standby module in case of an active module failure. • Booting the CSS from a network drive. • Displaying the boot configuration.

Table 5-2 Cisco Content Services Switch Administration Guide (continued)

Chapter	Contents/Tasks
Chapter 3, Configuring User Profiles	<ul style="list-style-type: none"> • Overview of user-profiles • User profile configuration quick start. • Configuring how to control the output to the system terminal screen including length of time that a session can be idle before the CSS terminates it, the number of output lines that the CLI displays, the --More-- prompt at the bottom of the terminal screen, how the CSS displays subnet masks, and the total amount of time a session can be logged in before the CSS terminates it. • Globally setting the total amount of time all console, Telnet, SSH or FTP sessions can be active before the CSS terminates them. • Configuring expert mode to turn the CSS confirmation capability on or off. • Changing the CLI prompt. • Modifying the size of the history buffer that stores the most recent CLI commands that you enter. • Configuring the banner that appears when you log in to the CSS. • Copy the running profile from the CSS to the default-profile file, an FTP server, a TFTP server, or your user-profile file.
Chapter 4, Using the CSS Logging Features	<ul style="list-style-type: none"> • Enable logging • Setting up the log buffer • Determining where to send the activity information • Displaying and interpreting log messages
Chapter 5, Configuring Simple Network Management Protocol (SNMP)	<ul style="list-style-type: none"> • Overview of SNMP and the MIB. • Preparing SNMP on the CSS. • Defining the CSS as an SNMP agent. This section includes a quick start. • Configuring special enterprise traps to notify the trap host of Denial of Service (DoS) attacks on your system. This section includes a quick start. • Managing SNMP on the CSS. • SNMP traps and MIB object lists.

Table 5-2 Cisco Content Services Switch Administration Guide (continued)

Chapter	Contents/Tasks
Chapter 6, Configuring Remote Monitoring (RMON)	<ul style="list-style-type: none"> • Configuring an RMOM event, alarm, and history with applicable quick starts • Displaying RMON statistics and history data, and alarm event notifications
Chapter 7, Using an XML Document to Configure the CSS	<ul style="list-style-type: none"> • Creating XML code • Allowing the transfer of XML configuration files on the CSS • Parsing the XML code • Publishing the XML code to the CSS • Testing the output of the XML code
Chapter 8, Using the CSS Scripting Language.	<ul style="list-style-type: none"> • Playing a script • Using the command scheduler to configure the scheduled execution of any CLI commands, including playing scripts • Using the echo command to control what appears on the screen during script execution • Using commented lines to document your script with comments. • Using variables to construct commands, command aliases, and scripts • Using logical and relational operators and branch commands • Using arrays to hold subvalues (elements) within its memory space • Capturing user input in a variable • Passing command line arguments as quoted text to a script • Using functions to organize your scripts into subroutines or modules • Using the grep command to search for specified data • Using socket command allowing ASCII or hexadecimal send and receive functionality • Script examples

Table 5-2 Cisco Content Services Switch Administration Guide (continued)

Chapter	Contents/Tasks
Appendix A, Upgrading Your CSS Software	<ul style="list-style-type: none"> • Downloading the new CSS software and creating an FTP server record • Using the upgrade script to automatically or interactive upgrade the CSS software • Manually upgrading the CSS software through CLI commands • Updating MIBs
Appendix B, Using the Offline Diagnostic Monitor Menu	<ul style="list-style-type: none"> • Setting the boot configuration: <ul style="list-style-type: none"> – Configure a primary and secondary location from which the CSS accesses the boot image. – Configure an IP address for the CSS – Configure a subnet mask – Configure a default gateway • Showing the boot configuration. • Selecting Advanced Options to: <ul style="list-style-type: none"> – Delete a software version from the disk – Set a password for the Offline DM Main menu – Set an administrative username and password – Reformat the disk and perform a check disk – Configure disks • Rebooting the CSS.

Cisco Content Services Switch Routing and Bridging Configuration Guide

This guide describes how to perform routing and bridging configuration tasks on the CSS. Table 5-3 lists the chapters in this guide, and a description of their contents and tasks.

Table 5-3 Cisco Content Services Switch Routing and Bridging Configuration Guide

Chapter	Contents/Tasks
Chapter 1, Configuring Interfaces and Circuits	<ul style="list-style-type: none"> • Overview of interfaces and circuit. • An interfaces and Virtual LAN (VLAN) circuits quick start. • Configuring a Ethernet interfaces including setting the maximum idle time, bridging it to a VLAN circuit, specifying VLAN trunking, configuring spanning-tree bridging and Port Fast, displaying the interfaces configuration, and shutting down the interfaces. • Configuring VLAN circuits including configuring a circuit IP interface, configuring Router-Discovery Protocol Settings for a Circuit, and displaying circuit and IP interface information. • Configuring RIP for an IP interface including a default route, the receive and send versions, and packet logging, and displaying the configurations. • Configuring the Switched Port Analyzer feature to mirror (copy) traffic passing through one CSS port (Fast Ethernet or Gigabit Ethernet) to another designated port of the same type and on the same CSS module for analysis. Instructions to verify the configuration are also provided.
Chapter 2, Configuring Spanning-Tree Bridging for the CSS	<ul style="list-style-type: none"> • Spanning-tree protocol (STP) quick start • Configuring aging, forward and hello time, priority and max-age • Disabling spanning-tree • Displaying the bridge configuration

Table 5-3 Cisco Content Services Switch Routing and Bridging Configuration Guide (continued)

Chapter	Contents/Tasks
Chapter 3, Configuring Open Shortest Path First (OSPF)	<ul style="list-style-type: none"> • Overview of OSPF • An OSPF configuration quick start • Configuring OSPF on the CSS • Configuring OSPF on a CSS IP interface • Displaying OSPF information
Chapter 4, Configuring the Address Resolution Protocol	<ul style="list-style-type: none"> • Address Resolution Protocol (ARP) configuration quick start • Configuring ARP timeout and wait period • Updating and clearing ARP parameters • Displaying ARP information
Chapter 5, Configuring Routing Information Protocol	<ul style="list-style-type: none"> • Routing Information Protocol (RIP) configuration quick start • Advertising a route through RIP on the CSS. • Advertising routes from other protocols through RIP • Setting the maximum number of routes that RIP can insert into the routing table • Displaying RIP configurations

Table 5-3 Cisco Content Services Switch Routing and Bridging Configuration Guide (continued)

Chapter	Contents/Tasks
Chapter 6, Configuring the Internet Protocol	<ul style="list-style-type: none">• Internet Protocol (IP) configuration quick start.• Configuring an IP route. You can configure a static route, a default static IP route, a blackhole route (where the CSS drops any packets addressed to the route), or a firewall IP route.• Disabling an implicit service for the static route next hop, to forward traffic to the next hop even when the next hop is unavailable.• Configuring an IP source route to enable the CSS to process frames with information that overrides the default routing.• Configuring the IP record route to enable the CSS to process frames with the IP address of each router along a path.• Configuring box-to-box redundancy between two identically configured CSSs.• Configuring IP equal-cost multipath (ECMP) selection algorithm and the preferred reverse egress path.• Forwarding IP subnet broadcast addressed frames.• Configuring IP unconditional bridging to always make a bridging decision on the received packets.• Configuring IP opportunistic Layer 3 forwarding to enable opportunistic Layer 3 forwarding and allow the CSS to make Layer 3 forwarding decisions even if the Layer 2 packet destination MAC address does not belong to the CSS.• Displaying IP configuration information.

Table 5-3 Cisco Content Services Switch Routing and Bridging Configuration Guide (continued)

Chapter	Contents/Tasks
Chapter 7, Configuring the Cisco Discovery Protocol	<ul style="list-style-type: none"> • Cisco Discovery Protocol (CDP) configuration quick start • Enabling CDP • Setting the hold time that a receiving device retains the CDP information sent by the CSS (time-to-live information) before discarding this information • Setting the transmission rate to specify the frequency at which the CSS transmits CDP packets to all receiving CDP-compatible devices • Displaying CDP information
Chapter 8, Configuring the DHCP Relay Agent	<ul style="list-style-type: none"> • Dynamic Host Configuration Protocol (DHCP) configuration quick start • Adding a DHCP destination on a circuit so that the initial DHCP broadcast request from the CSS is sent to all of the configured destinations • Enabling and disabling DHCP on the circuit • Defining the hops field value for forwarding DHCP messages • Displaying the DHCP relay configuration

Cisco Content Services Switch Content Load-Balancing Configuration Guide

This guide provides instructions to configure content load balancing on the CSS including the configuration of keepalives, source groups, loads, DFP, content rules, and content replication. Table 5-4 lists the chapters in this guide, and a description of their contents and tasks.

Table 5-4 Cisco Content Services Switch Content Load-Balancing Configuration Guide

Chapter	Contents/Tasks
Chapter 1, Content Load-Balancing Overview	<ul style="list-style-type: none"> • Provides information to assist you in understanding what happens when load balancing occurs on the CSS by providing information about the relationship of service, owner, and content rules, and describes how the CSS handles TCP and UDP traffic
Chapter 2, Configuring Flow and Port Mapping Parameters	<ul style="list-style-type: none"> • Configuring flow parameters to create permanent TCP and UDP ports, configuring how often the CSS scans flows from reserved Telnet and FTP control ports to reclaim them, changing the maximum segment size (MSS), and displaying the statistics on currently allocated flows • Configuring flow inactivity timeouts on content rules and source groups and displaying the timeout statistics • Configuring flow processing for fragmented IP packets allowing the CSS to process the IP fragments in the flow path, defining the maximum and minimum fragment size, and displaying and resetting the IP fragment statistics • Configuring a CSS to send a TCP reset if a VIP is unavailable • Configuring the flow-state table to alter the flow characteristics and NAT state of TCP and UDP ports and displaying the table • Configuring CSS port mapping to globally control the range of port numbers a CSS uses to perform port address translation (PAT) on TCP and UDP source ports, and display port mapping statistics

Table 5-4 Cisco Content Services Switch Content Load-Balancing Configuration Guide (continued)

Chapter	Contents/Tasks
Chapter 3, Configuring Services	<ul style="list-style-type: none"> • A service configuration quick start • Configuring an IP Address, port, protocol, domain name, HTTP redirect string and cookie, weight service type, access, and maximum TCP connections • Associating an FTP access mechanism with a service when a service offers publishing services • Bypassing content rules on caches to prevent the CSS from applying content rules to requests originating from a proxy or transparent-cache service type • Enabling destination Network Address Translation (NAT) for the transparent-cache service type • Bypassing a cache farm and establishing a connection with the origin server to retrieve noncacheable content • Activating and suspending services • Showing service information and clearing statistics
Chapter 4, Configuring Service, Global, and Script Keepalives	<ul style="list-style-type: none"> • Overview of keepalives • Configuring service keepalives • Configuring global keepalives and a quick start • Configuring keepalive attributes for service and global keepalives including frequency, retry period, maximum failures, type, TCP keepalive with graceful socket close, port number, method, HTTP response code, URI, and hash value • Displaying keepalive information • Using script keepalives with services

Table 5-4 Cisco Content Services Switch Content Load-Balancing Configuration Guide (continued)

Chapter	Contents/Tasks
Chapter 5, Source Groups for Services	<ul style="list-style-type: none"> • Overview of source groups and port mapping • A source group configuration quick start • Configuring a VIP address, service, and destination service • Activating and suspending a source group • Configuring port mapping including a starting port, number of ports in a port-map range, and a VIP address range, and disabling port mapping • Configuring source groups with ACLs, for FTP connections, and to allow servers to resolve domain names using the Internet • Displaying source group information and clearing counters
Chapter 6, Configuring Loads for Services	<ul style="list-style-type: none"> • Overview of service loads • A relative load configuration quick start • Configuring relative loads including global load reporting, load step, load threshold, and teardown and ageout timers. • Displaying global service loads • An absolute load configuration quick start • Configuring the absolute load calculation method including modifying and optimizing the absolute load scale, and setting the load variance • Displaying relative load statistics and absolute load calculation ranges • Using ArrowPoint Content Awareness (ACA) load-balancing algorithm to balance traffic between a group of servers based on load and weight
Chapter 7, Configuring Server/Application State Protocol for Server Load Balancing	<ul style="list-style-type: none"> • Overview of Server/Application State Protocol (SASP) • Configuring an SASP agent, and enabling SASP on the CSS • Displaying SASP information, including configured SASP agents and supported services

Table 5-4 Cisco Content Services Switch Content Load-Balancing Configuration Guide (continued)

Chapter	Contents/Tasks
Chapter 8, Configuring Dynamic Feedback Protocol for Server Load Balancing	<ul style="list-style-type: none"> • Overview of Dynamic Feedback Protocol (DFP) • Configuring a DFP agent to listen for DFP connections on a particular IP address and TCP port combination on a server, and to enable the DFP manager on the CSS • Maintaining a consistent weight range among services • Displaying DFP information, including configured DFP agents and supported services
Chapter 9, Configuring Owners	<ul style="list-style-type: none"> • Configuring owner attributes such as a DNS balance type, address, billing information, case sensitivity, DNS type • Removing an owner • Displaying owner information
Chapter 10, Configuring Content Rules	<ul style="list-style-type: none"> • Overview of content rules. • Content rule configuration quick start. • Assigning a content rule to an owner. • Configuring the virtual IP (VIP) address. • Configuring a domain name content rule. • Configuring a domain qualifier list (DQL) and virtual web hosting (VWH) including a quick start. • Adding a service to a content rule. This section includes specifying a service weight, adding a primary and secondary sorry server, and adding a DNS name to a content rule. • Activating, suspending, and removing a content rule. • Configuring a port, load-balancing algorithm, DNS balance type, hot lists, extension qualifier lists (EQL), Uniform Resource Locator qualifier list (URQL) and quick start, Uniform Resource Locator (URL), spanned packets, load threshold, services in CSS ping response decision, TCP flow reset reject, persistence, remapping and redirection, failover handling, and application type. • Displaying content rule information and clearing counters.

Table 5-4 Cisco Content Services Switch Content Load-Balancing Configuration Guide (continued)

Chapter	Contents/Tasks
Chapter 11, Configuring Sticky Parameters for Content Rules	<ul style="list-style-type: none"> • Overview of sticky • Configuring sticky on the CSS • Specifying an advanced load-balancing method for sticky content • Configuring SSL-Layer 4 fallback • Configuring sticky serverdown failover • Configuring a sticky subnet mask, inactivity timeout, sticky contents for SSL, string range, string operation, ASCII conversion, multiple string matches, end of string characters, string prefix, and string process and skip length • Configuring sticky parameters for E-commerce and other Internet applications including arrowpoint and location cookies, wireless users for E-commerce applications, and Session Initiation Protocol (SIP) load balancing • Displaying sticky attributes, tables, and connection statistics
Chapter 12, Configuring HTTP Header Load Balancing	<ul style="list-style-type: none"> • Overview of HTTP header load balancing • HTTP header load-balancing configuration quick start • Creating a header-field group, configuring a header-field entry, and associating a header-field group to a content rule • HTTP header load-balancing configuration examples • Displaying header-field groups

Table 5-4 Cisco Content Services Switch Content Load-Balancing Configuration Guide (continued)

Chapter	Contents/Tasks
Chapter 13, Configuring Caching	<ul style="list-style-type: none"> • Overview of caching • Caching configuration quick start • Configuring caching content rules, including specifying a service and failover type, load-balancing algorithm, double-wildcard caching rule, bypass caches, and NATing for the transparent cache service type • Configuring NAT peering and quick start
Chapter 14, Configuring Content Replication	<ul style="list-style-type: none"> • Demand-based content replication quick start • Configuring demand-based content replication including hot lists, service type, maximum age, pieces of content, and disk space for replicated objects on services, and FTP access • Content staging and replication quick start • Configuring content staging and replication including publishing and subscribing services, FTP access, and publisher content replication • Displaying content

Cisco Content Services Switch Global Server Load-Balancing Configuration Guide

This guide describes how to perform CSS global load-balancing configuration tasks. Table 5-5 lists the chapters in this guide, and a description of their contents and tasks.

Table 5-5 Cisco Content Services Switch Global Server Load-Balancing Configuration Guide

Chapter	Contents/Tasks
Chapter 1, Configuring the CSS as a Domain Name System Server	<ul style="list-style-type: none"> • Overviews of CSS DNS feature and Application Peering Protocol (APP). • Configuring APP including the maximum frame size, TCP port, session, and the issuing of CLI commands (including playing scripts) to remote CSS peers over an APP session. • Displaying APP information. • Zone-based DNS quick start. • Configuring zone-based DNS on a CSS including a DNS server, buffer count, DNS forwarder server, responder task count, zones, domain records, and kal-ap-vip client and agent. • Configuring content rule-based DNS and quick start. This section includes configuring DNS exchange policy for the owner, DNS peering and server, and adding and removing a DNS name from a content rule. • Displaying DNS information for a CSS configured as a DNS server including zone, record and peering information.
Chapter 2, Configuring the DNS Sticky Feature	<ul style="list-style-type: none"> • Overview of CSS Domain Name System (DNS) Sticky feature • DNS sticky with or without global server load balancing (GSLB), and network proximity quick starts • Converting your content rule-based DNS configuration to a zone-based DNS configuration • Configuring DNS sticky parameters • Displaying DNS sticky information

Table 5-5 Cisco Content Services Switch Global Server Load-Balancing Configuration Guide (continued)

Chapter	Contents/Tasks
Chapter 3, Configuring a CSS as a Content Routing Agent	<ul style="list-style-type: none"> • Overview of CRA • A CRA quick start • Configuring CRA parameters including enabling the CRA, and configuring the CPU load threshold, domain records, and alias for an existing client domain • Displaying and clearing CRA statistics
Chapter 4, Configuring a Client-Side Accelerator	<ul style="list-style-type: none"> • Overview of CSA and configuration examples • A CSA quick start • Configuring CSA parameters including enabling CSA functionality and configuring domain cache, DNS server forwarder, and accelerated domains • Displaying CSA information
Chapter 5, Configuring Network Proximity	<ul style="list-style-type: none"> • Overviews on network proximity and configuring a proximity database on a CSS 11150 and a proximity domain name server (PDNS) as an authoritative DNS server that uses information from the Proximity Database (PDB) to resolve DNS requests • Configuring Application Peering Protocol-User Datagram Protocol (APP-UDP) to exchange proximity information between a PDB and a PDNS, and between a PDNS and services and APP • Configuring domain records • Enabling PDNS and proximity lookup cache • Displaying PDNS information

Cisco Content Services Switch Redundancy Configuration Guide

This guide describes how to perform CSS redundancy configuration tasks.

Table 5-6 lists the chapters in this guide, and a description of their contents and tasks.

Table 5-6 Cisco Content Services Switch Redundancy Configuration Guide

Chapter	Contents/Tasks
Chapter 1, Configuring VIP and Virtual Interface Redundancy	<ul style="list-style-type: none"> • Overviews of CSS redundancy and VIP and virtual interface redundancy • A VIP and virtual interface redundancy quick start • Configuring VIP and virtual interface redundancy including the circuit IP interface, virtual router, redundant VIP and virtual interface, VRID peering and quick start, critical service, critical physical interface and quick start, and synchronizing a VIP redundancy configuration • Displaying VIP and virtual interface redundancy information
Chapter 2, Configuring Adaptive Session Redundancy	<ul style="list-style-type: none"> • Overview of CSS redundancy • ASR quick start • Configuring ASR, including Inter-Switch Communications (ISC); redundant services, content rules, and source groups; and synchronizing ASR configurations • Displaying ASR information

Table 5-6 Cisco Content Services Switch Redundancy Configuration Guide (continued)

Chapter	Contents/Tasks
Chapter 3, Configuring Box-to-Box Redundancy	<ul style="list-style-type: none"> • Overview of CSS redundancy and redundancy protocol • Redundancy configuration quick start • Cabling redundant CSSs • Configuring redundancy including IP redundancy, redundant circuits, redundancy protocol, and VRRP backup timer • Synchronizing a redundant configuration • Configuring a backup CSS as a master temporarily • Configuring multiple redundant uplink services • Adding an interface to the physical link configuration list • Configuring stateless redundancy failover • Displaying redundant configurations

Cisco Content Services Switch Security Configuration Guide

This guide describes how to perform CSS security configuration tasks. Table 5-7 lists the chapters in this guide, and a description of their contents and tasks.

Table 5-7 Cisco Content Services Switch Security Configuration Guide

Chapter	Contents/Tasks
Chapter 1, Controlling CSS Access	<ul style="list-style-type: none"> • Changing the administrative username and password • Creating usernames and passwords • Controlling remote user access to the CSS including virtual and console authentication • Controlling administrative access to the CSS • Controlling network traffic through Access Control Lists (ACLs), including an overview, quick start, configuring clauses, applying the ACL to a circuit, and enabling ACLs • Configuring Network Qualifier Lists for ACLs
Chapter 2, Configuring the Secure Shell Daemon Protocol	<ul style="list-style-type: none"> • Enabling SSH • Configuring SSH access, SSHD on the CSS, and Telnet access when using SSHD • Displaying SSHD configurations
Chapter 3, Configuring the CSS as a Client of a RADIUS Server	<ul style="list-style-type: none"> • RADIUS configuration quick start • Configuring a RADIUS server for use with the CSS including authentication and authorization settings • Configuring primary and secondary RADIUS servers, timeout interval, retransmits, and dead-time interval • Displaying RADIUS server configuration information

Table 5-7 Cisco Content Services Switch Security Configuration Guide (continued)

Chapter	Contents/Tasks
Chapter 4, Configuring the CSS as a Client of a TACACS+ Server	<ul style="list-style-type: none"> • TACACS+ configuration quick start • Configuring TACACS+ server user accounts for use with the CSS, including authentication and authorization settings • Configuring global TACACS+ attributes, including timeout period, encryption key, and keepalive frequency • Defining a TACACS+ server • Setting TACACS+ authorization and accounting to control specific CSS commands • Displaying TACACS+ server information
Chapter 5, Configuring Firewall Load Balancing	<ul style="list-style-type: none"> • Configuring Firewall Load Balancing (FWLB) including keepalive timeout, IP static route, OSPF and RIP to advertise firewall routes • Configuring FWLB with VIP and virtual interface redundancy • Displaying firewall information including flow summaries and routes

Cisco Content Services Switch SSL Configuration Guide

This guide provides instructions for configuring the SSL features and HTTP data compression on the CSS. Table 5-8 lists the chapters in this guide, and a description of their contents and tasks.

Table 5-8 Cisco Content Services Switch SSL Configuration Guide

Chapter	Contents/Tasks
Chapter 1, Overview of CSS SSL	<ul style="list-style-type: none"> • Overviews of SSL cryptography and the CSS SSL features including SSL termination, client authentication, back-end SSL, and SSL initiation
Chapter 2, SSL Configuration Quick Starts	<ul style="list-style-type: none"> • Generating RSA certificates and keys and importing quick starts • SSL termination, back-end SSL, and SSL initiation proxy lists quick starts • Configuring services and content rules for SSL termination, back-end SSL server, and SSL initiation quick starts

Table 5-8 Cisco Content Services Switch SSL Configuration Guide (continued)

Chapter	Contents/Tasks
Chapter 3, Configuring SSL Certificates and Keys	<ul style="list-style-type: none"> • Overview of SSL certificates and keys • Generating certificates and private keys including RSA and DSA key pairs, Diffie-Hellman key parameters, and self-signed certificate • Preparing a global site certificate • Importing and exporting certificates and private keys, including configuring the FTP record, and transferring certificate and keys to the CSS • Associating certificates and private key files with names including an imported or generated certificate, RSA and DSA key pair, and Diffie-Hellman parameters • Verifying a certificate against a key pair • Removing certificates and private keys from the CSS
Chapter 4, Configuring SSL Termination	<ul style="list-style-type: none"> • Overview of SSL termination • Creating an SSL proxy list • Configuring virtual SSL servers for the SSL proxy list, including a VIP address and port; certificate, key and cipher suites for server authentication; client authentication; HTTP header insertion; SSL or TLS version; secure URL rewrite; session cache timeout and handshake negotiation; delay time for SSL queued data; client and server side connection timeouts; and Nagle algorithm and TCP buffering for SSL TCP connections • Activating and suspending the proxy list • Configuring a service and a content rule for SSL termination

Table 5-8 Cisco Content Services Switch SSL Configuration Guide (continued)

Chapter	Contents/Tasks
Chapter 5, Configuring Back-End SSL	<ul style="list-style-type: none"> • Overview of back-end SSL • Creating an SSL proxy list • Configuring back-end SSL server in the proxy list, including a VIP address and port, server IP address and port, SSL version, cipher suites, session cache timeouts and handshake renegotiation, client and server side connection timeouts, and Nagle algorithm and TCP buffering for SSL TCP connections • Activating and suspending the proxy list • Configuring a service and content rule for back-end SSL
Chapter 6, Configuring SSL Initiation	<ul style="list-style-type: none"> • Overview of SSL initiation • Creating an SSL initiation proxy list • Configuring a back-end SSL initiation server in the proxy list including the IP address and port for the SSL initiation server, server IP address and port, SSL version, cipher suites, session cache timeouts and handshake renegotiation, client and server side connection timeouts, Nagle algorithm and TCP buffering for SSL TCP connections, client certificate and keys, and CA certificates for server authentication • Activating and suspending the proxy list • Configuring a service and content rule for SSL initiation • Troubleshooting SSL initiation
Chapter 7, Displaying SSL Configuration Information and Statistics	<ul style="list-style-type: none"> • Displaying certificates and key pairs • Displaying SSL proxy configurations • Displaying CRL record configurations • Displaying SSL URL rewrite and SSL module statistics • Displaying SSL flows

Table 5-8 Cisco Content Services Switch SSL Configuration Guide (continued)

Chapter	Contents/Tasks
Chapter 8, Examples of CSS SSL Configurations	<ul style="list-style-type: none">• Processing of SSL flows by the SSL module• SSL transparent proxy configuration with one SSL module, two SSL module, or HTTP and back-end SSL servers• SSL full proxy configuration• SSL initiation configuration
Chapter 9, Configuring HTTP Compression	<ul style="list-style-type: none">• CSS compression overview• Compression-only service quickstart• Configuring compression on the CSS• Configuring TCP options for a compression only service• Displaying compression information



Troubleshooting the Boot Process

There are three phases in the boot process during which the Cisco 11500 series CSS runs power-on self tests on the hardware and checks the boot configuration. During any of these phases, the CSS reports problems through error messages.

- With the CSS 11501, the internal motherboard boots all components in the chassis and verifies that each component is properly functioning.
- With the CSS 11503 and CSS 11506, the SCM boots each module in the chassis and verifies that the module is functioning properly.

This appendix contains the following major sections:

- Diagnostic Tests for Hardware and Error Messages
- Offline DM Verification of the Boot Configuration Record and Disk
- CSS 11501 Boot and Verification
- CSS 11503 and CSS 11506 Boot and Module Verification

If the suggestions in this appendix do not help to resolve your booting problem, contact the Cisco Technical Assistance Center (TAC).

For details about powering on and booting the CSS, including the various boot states and the Status LEDs, refer to Chapter 1, Booting, Logging In, and Getting Started.

Diagnostic Tests for Hardware and Error Messages

At the beginning of the boot process, the Cisco 11500 series CSS performs diagnostic tests on the hardware. When the CSS powers up, it first displays a series of messages (see the Chapter 1, Booting, Logging In, and Getting Started) and then the hardware goes through a series of power-on self tests.

If an error occurs during a test, the console displays an error message, increments the detected error counter, and continues to the next test until the CSS completes all of the power-on self tests. The error messages appear in the following format:

```
>>>>>>>>FAILURE_START
>
>From: Slot Slot_number, CPU Cpu_number
>Level: Failure_level
>Type: Failure_type
>Major Error ID: Maj_Error_id
>Minor Error ID: Min_Error_id
>Test Ref #: Test_reference
>Test: 'Test_name'
>Details:
>
>Failure_details
>
>>>>>>>>FAILURE_END
```

Table A-1 lists the fields in the error message and describes their meanings. This information may be useful when in contact with TAC about a specific error message.

Table A-1 *Fields in the Diagnostic Monitor Error Message*

Field	Description
<i>Slot_number</i>	The slot number reporting the error.
<i>Cpu_number</i>	The CPU number reporting the error. This field is 1 for boards with a single MIPS CPU.
<i>Failure_level</i>	There are three types of failure levels: <ul style="list-style-type: none">• Board - The CSS 11501 motherboard or a specific module in the CSS 11503 or CSS 11506. If the CSS completes the boot process, but a component or module has failed, the CSS also generates a boot log message.• Backplane - An EEPROM failure is a catastrophic failure. Contact TAC for technical assistance.• Chassis - A fan failure has occurred. After the boot process has completed, a log message appears with information on which fan has failed. For information on troubleshooting a fan failure, see the <i>Cisco 11500 Series Content Services Switch Hardware Installation Guide</i>.

Table A-1 *Fields in the Diagnostic Monitor Error Message (continued)*

Field	Description
<i>Failure_type</i>	<p>One of four types of failure, Hardware/Fatal, Hardware/Non-Fatal, Software/Fatal, and Software/Non-Fatal.</p> <ul style="list-style-type: none"> • Fatal errors indicate that a CSS 11501 component or a specific module in the CSS 11503 or CSS 11506 cannot perform its intended function. • Non-Fatal errors indicate that a CSS 11501 component or a specific module in the CSS 11503 or CSS 11506 is capable of performing its intended function despite the errors, but you should repair the problem as soon as possible. <p>In the case of fatal and non-fatal errors with the CSS 11501, contact TAC for technical assistance.</p> <p>In the case of fatal and non-fatal errors with the CSS 11503 or CSS 11506:</p> <ol style="list-style-type: none"> 1. Power down the CSS when the CSS completes the boot process. 2. Reseat the failed module. 3. Power up the CSS. <p>If reseating the module does not correct the failure, contact the TAC for technical assistance.</p>
<i>Maj_Error_id</i>	The single reference number that points to a particular sub-function in the CSS 11501 chassis or a specific module in the CSS 11503 or CSS 11506.
<i>Min_Error_id</i>	The sub-reference number that points to a particular verification step within the sub-function.
<i>Test_reference</i>	The test number associated with a particular test.

Table A-1 *Fields in the Diagnostic Monitor Error Message (continued)*

Field	Description
<i>Test_name</i>	Provides the name of the test reporting the error. For example: Uart Interrupt Test PHY Reset Test
<i>Failure_details</i>	Provides information about the error. For example: PHY Reset Register failed to clear. Addr: 0x12345678 Expected: 0x0 Actual:0xf

After the CSS performs the diagnostics, it boots the Offline DM as indicated by the following message:

```
Booting OffDm @ 0xbfd70000
```

See the “Offline DM Verification of the Boot Configuration Record and Disk” section for the Offline DM verification of the boot configuration record and disk drive.

If the Booting OffDm message does not appear, a CSS 11501 component failure or an SCM failure may have occurred; such a failure would not allow a software download to start.

If this problem occurs for a CSS 11501, contact Cisco Technical Assistance Center (TAC) for technical assistance.

If this problem occurs for a CSS 11503 or CSS 11506:

1. Power down the CSS.
2. Reseat the SCM.
3. Power up the CSS.

If reseating the module does not correct the failure, contact TAC for technical assistance.

Offline DM Verification of the Boot Configuration Record and Disk

During the Offline DM verification phase, the CSS checks the configuration record and initializes the disk. If the CSS detects any errors in the configuration record, a failed message appears along with information on the configuration parameter in question. The problems may include a misconfigured IP and subnet address, or there is no primary or secondary boot record. The CSS does not continue the boot process until the problem is resolved.

If a failed message occurs:

1. Enter the Offline DM menu and display your current configuration record. Refer to the *Cisco Content Services Switch Administration Guide* for detailed information on using Offline DM.
2. Reconfigure the CSS boot record configuration.
3. Reboot the CSS.

**Note**

If a MAC address error occurs, contact TAC for technical assistance.

After the CSS confirms a valid configuration record, it initializes the disk in slot 0. If the disk cannot initialize, the CSS indicates that it has failed. If an initialization problem occurs:

1. Enter the Offline DM menu.
2. Select the option **3** from the Disk Options menu.
3. Perform a check disk on the disk in slot 0. If necessary, reformat the disk.
4. Reboot the CSS. If the failure is not resolved, contact TAC for technical assistance.

CSS 11501 Boot and Verification

After the CSS 11501 completes the Offline DM boot process, the CSS displays the login banner and starts the Online Diagnostic Monitor (OnDM). During OnDM, the CSS 11501 downloads software to each component and verifies that each component is functioning.

If there is a component failure, the CSS 11501 attempts the boot process three times. If the boot is unsuccessful, the CSS generates the following log message and saves the message in the boot.log file:

```
CHMGR: Slot slot/subslot had diagnostic failures - NOT STARTING UP
```

If this problem occurs for a CSS 11501, contact TAC for technical assistance.

CSS 11503 and CSS 11506 Boot and Module Verification

After the CSS 11503 or CSS 11506 completes the Offline DM boot process, the CSS displays the main banner and starts the Online Diagnostic Monitor (OnDM). During OnDM, the SCM downloads software to each of the modules and boots the modules. The SCM verifies that each module is functioning.

If there is a module failure, the SCM attempts to boot the module three times. If the SCM is unsuccessful, the CSS generates the following log message and saves the message in the boot.log file:

```
CHMGR: Slot slot/subslot had diagnostic failures - NOT STARTING UP
```

The SCM disables the slot and no longer recognizes it. If you use the **show chassis** command, the slot does not appear. If a module failure occurs:

1. Power down the CSS.
2. Reseat the module.
3. Power on the CSS.

If reseating the module does not correct the failure, replace the module.

For additional information on troubleshooting the modules during normal CSS operation, see the *Cisco 11500 Series Content Services Switch Hardware Installation Guide*.



INDEX

A

administrative password
 changing **2-5**
administrative task topics **5-1**
administrative username
 changing **2-5**
assigning
 IP address for management port **2-11**
 subnet mask for management port **2-9**
audience **xii**

B

boot process
 entering license key **1-3**
 hardware initialization **1-7**

C

caution
 creating/modifying username or
 password **2-6**
 Ethernet Management port subnet
 address **2-11**
 existing username, removing **2-8**

 symbol overview **xvi**
changing
 administrative password **2-5**
 administrative username **2-5**
 user directory access privileges **2-7**
 user password **2-8**
changing the default username and
 password **1-5**
CLI
 conventions **xvii**
 Ethernet management port usage **2-9**
 expert mode **2-17**
 User commands versus SuperUser
 commands **2-6**
configuration quick start
 initial CSS configuration **1-2, 2-2**
configuration scripts **1-2, 1-11**
configuration task topics **5-1**
configuring
 Ethernet management port **1-4**
 Layer 3 load balancing **1-14**
 Layer 5 load balancing **1-16**
 proxy cache **1-18**
 SNTP server operation **2-25**
 time, date, and timezone **2-17**
 transparent cache **1-13, 1-20**

user name and password **2-6**

Content Services Switch

assigning a subnet mask **2-9, 2-11**

controlling remote access to **2-17**

host name, configuring **2-29**

logging in **1-9**

rebooting **1-23**

shutdown **1-24**

cookies

advanced-balance **4-2**

client **4-2**

CSS. See Content Services Switch

D

date, configuring **2-17, 2-18**

daylight saving time (DST), configuring **2-20**

default gateway for management port **2-13**

default IP route, configuring **2-16**

directory access privileges (username) **2-7**

displaying

username **2-8**

DNS

configuring for CSS **3-1, 5-1**

primary server for CSS, configuring **3-1**

resolve for CSS, configuring **3-2**

secondary server for CSS, configuring **3-2**

specifying suffix **3-2**

documentation

audience **xii**

chapter contents **xii**

related **xiii**

set **xiii**

symbols and conventions **xvi**

E

e-commerce

using stickiness **4-1**

Ethernet management port

configuring **1-4**

ICMP redirects, discarding **2-13**

IP address and subnet mask, configuring **2-11**

overview **2-9**

shutting down **2-15**

static routes, defining **2-12**

european date, configuring **2-18**

G

gateway, default for Management port **2-13**

H

hardware initialization **1-7**

I

- ICMP redirects, discarding on the management port **2-13**
- IP address
 - Ethernet management port, configuring for **2-11**
 - management port **2-9**

L

- Layer 3 load balancing, configuring **1-14**
- Layer 5 load balancing, configuring **1-16**
- LEDs
 - CSS 11501 boot patterns **1-8**
 - CSS 11503 and 11506 module boot patterns **1-8**
- license key, entering **1-3**
- logging
 - into the CSS **1-9**

M

- management port, assigning an IP address and subnet mask **2-11**

O

- Offline Diagnostic Monitor menu
 - setting password protection **1-6**

P

- password
 - administrative, changing **2-5**
 - administrative password, changing **2-5**
 - user, configuring **2-6**
 - user password, changing **2-8**
- password-protecting the OffDM menu **1-6**
- PAT **5-33**
- port address translation. See PAT
- proxy cache, configuring **1-18**

Q

- quick start
 - initial CSS configuration **1-2, 2-2**

R

- rebooting the CSS **1-23**
- removing
 - user name **2-8**
- running-config example
 - initial setup **2-4**

S

- showing
 - Sntp configuration **2-28**

shutting down the CSS **1-24**

SNTP

overview **2-25**

server, configuring **2-26**

showing SNTP information **2-28**

software

build number **1-2, 1-7**

version **1-2, 1-7**

version number **1-2, 1-7**

static IP route, configuring **2-16**

static routes, configuring **2-12**

sticky content

specifying an advanced load balancing
method **4-2**

user password

changing **2-8**

configuring **2-6**

W

warning

symbol overview **xvi**

T

tasklist topics **5-1**

time, configuring for CSS **2-17**

timezone, configuring for CSS **2-17**

transparent cache, configuring **1-13, 1-20**

U

username

configuring **2-6**

directory access privileges **2-7**

displaying **2-8**

removing **2-8**