



Cisco Internet Streamer CDS 2.4 Command Reference

September 2009

Americas 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: 408 527-0883

Text Part Number: OL-19453-02

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.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo 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. (0903R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Cisco Internet Streamer CDS 2.4 Command Reference
© 2004–2009 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface **xi**

Document Revision History	xi
Document Organization	xi
Audience	xii
Conventions	xii
Related Documentation	xiii
Obtaining Documentation and Submitting a Service Request	xiii

CHAPTER 1

Command-Line Interface Command Summary **1-1**

Using CDS Device Modes	1-1
Using Command-Line Processing	1-1
Using Command Modes	1-2
Using EXEC Mode	1-3
Using Global Configuration Mode	1-3
Using Interface Configuration Mode	1-4
Using Other Configuration Modes	1-4
Checking the Command Syntax	1-4
System Help	1-6
Saving Configuration Changes	1-6

CHAPTER 2

Internet Streamer CDS Release 2.4 Software Commands **2-1**

access-lists	2-15
acquirer (EXEC)	2-17
acquirer (global configuration)	2-19
acquisition-distribution	2-21
alarm overload-detect	2-22
asset	2-24
authentication	2-25
authsvr	2-30
bandwidth (global configuration)	2-31
bandwidth (interface configuration)	2-34
banner	2-35

bitrate	2-38
cache	2-41
capability	2-42
cd	2-43
cdnfs	2-44
cdsm	2-46
clear	2-49
clock (EXEC)	2-53
clock (global configuration)	2-55
cms (EXEC)	2-58
cms (global configuration)	2-62
configure	2-65
copy	2-66
cpfile	2-69
debug	2-70
delfile	2-77
deltree	2-78
device	2-79
dir	2-81
direct-server-return	2-82
disable	2-83
disk (EXEC)	2-84
disk (global configuration)	2-88
distribution	2-90
dnslookup	2-93
enable	2-94
end	2-95
exec-timeout	2-96
exit	2-97
external-ip	2-98
find-pattern	2-100
flash-media-streaming	2-102
help	2-105
hostname	2-106
http	2-107

[icap](#) 2-112

[icap service](#) 2-115

[install](#) 2-119

[interface](#) 2-120

[ip](#) 2-122

[ip access-list](#) 2-130

[ipv6](#) 2-138

[kernel kdb](#) 2-139

[line](#) 2-140

[lls](#) 2-141

[logging](#) 2-142

[ls](#) 2-146

[mkdir](#) 2-147

[mkfile](#) 2-148

[movie-streamer](#) 2-149

[mtu](#) 2-153

[no \(global configuration\)](#) 2-154

[no \(interface configuration\)](#) 2-156

[ntp](#) 2-157

[ntpdate](#) 2-159

[ping](#) 2-160

[ping6](#) 2-161

[port-channel](#) 2-162

[primary-interface](#) 2-163

[pwd](#) 2-165

[qos](#) 2-166

[radius-server](#) 2-168

[rcp](#) 2-172

[rea](#) 2-173

[reload](#) 2-174

[rename](#) 2-175

[restore](#) 2-176

[rmdir](#) 2-179

[rtsp](#) 2-180

[rule](#) 2-183

script	2-192
service-router	2-193
setup	2-197
show access-lists	2-198
show acquirer	2-199
show alarms	2-201
show arp	2-204
show authentication	2-205
show authsvr	2-206
show bandwidth	2-207
show banner	2-209
show bitrate	2-210
show cache	2-211
show capability	2-212
show cdnfs	2-213
show clock	2-214
show cms	2-217
show content	2-219
show debugging	2-220
show device-mode	2-221
show direct-server-return	2-223
show disks	2-224
show distribution	2-227
show flash	2-237
show flash-media-streaming	2-238
show ftp	2-240
show hardware	2-241
show hosts	2-244
show http	2-245
show icap	2-247
show interface	2-249
show inventory	2-252
show ip access-list	2-254
show ip routes	2-256
show ldap	2-257

show logging	2-259
show movie-streamer	2-261
show ntp	2-262
show processes	2-264
show programs	2-266
show qos	2-272
show radius-server	2-273
show rea	2-275
show rcp	2-276
show rtsp	2-277
show rule	2-278
show running-config	2-280
show service-router	2-283
show services	2-287
show snmp	2-289
show ssh	2-293
show standby	2-294
show startup-config	2-295
show statistics access-lists 300	2-297
show statistics acquirer	2-298
show statistics authentication	2-300
show statistics cdnfs	2-301
show statistics distribution	3-303
show statistics flash-media-streaming	3-306
show statistics http	3-308
show statistics icap	3-312
show statistics icmp	3-315
show statistics ip	3-321
show statistics movie-streamer	3-323
show statistics netstat	3-326
show statistics qos	3-327
show statistics radius	3-328
show statistics replication	3-329
show statistics service-router	3-331
show statistics services	3-332

show statistics snmp	3-333
show statistics tacacs	3-335
show statistics tcp	3-336
show statistics transaction-logs	3-345
show statistics udp	3-347
show statistics wmt	3-348
show tacacs	3-353
show tech-support	3-355
show telnet	3-361
show transaction-logging	3-362
show url-signature	3-366
show user	3-367
show users	3-368
show version	3-369
show wmt	3-370
shutdown (interface configuration)	3-376
shutdown (EXEC)	3-377
snmp-server community	3-381
snmp-server contact	3-382
snmp-server enable traps	3-383
snmp-server group	3-385
snmp-server host	3-387
snmp-server location	3-389
snmp-server notify inform	3-390
snmp-server user	3-392
snmp-server view	3-394
sshd	3-396
sysreport	3-398
tacacs	3-399
tcpdump	3-403
telnet	3-408
telnet enable	3-409
terminal	3-410
test-url	3-411
traceroute	3-415

[traceroute6](#) 3-418
[transaction-log force](#) 3-419
[transaction-logs](#) 3-421
[type](#) 3-438
[type-tail](#) 3-440
[undebug](#) 3-443
[url-signature](#) 3-444
[username](#) 3-448
[whoami](#) 3-451
[wmt](#) 3-452
[write](#) 3-466

APPENDIX A**Acronyms** A-1

APPENDIX B**Standard Time Zones** B-1

INDEX



Preface

This preface describes the objectives and organization of this guide and contains the following sections:

- [Document Revision History, page xi](#)
- [Document Organization, page xi](#)
- [Audience, page xii](#)
- [Conventions, page xii](#)
- [Related Documentation, page xiii](#)
- [Obtaining Documentation and Submitting a Service Request, page xiii](#)

Document Revision History

The Document Revision History table below records technical changes to this document.

Document Version	Date	Change Summary
OL-19453-02	September 1, 2009	Added new command keywords for URL Signing and Cross-domain Support for the 2.4.3 release.
OL-19453-01	June 15, 2009	This is the first version of this document.

Document Organization

Chapter	Description
Chapter 1, “Command-Line Interface Command Summary”	This chapter describes how to use the Content Delivery System (CDS) command-line interface (CLI) to configure software features.
Chapter 2, “Internet Streamer CDS Release 2.4 Software Commands”	This chapter provides a complete list of Cisco Internet Streamer commands listed alphabetically.

Chapter	Description
Appendix A, “Acronyms”	This chapter lists the abbreviations and acronyms used in this guide.
Appendix B, “Standard Time Zones”	This chapter lists all the standard time zones that you can configure on a Content Delivery Engine (CDE) and the offset from Coordinated Universal Time (UTC) for each standard time zone.

Audience

This guide is for the networking professional using Cisco Internet Streamer CDS Release 2.4. Before using this guide, you should have experience working with the Cisco Internet Streamer CDS. Before using this guide, you should have experience working with the concepts and terminology of Ethernet and local area networking.

Conventions

This publication uses these conventions to convey instructions and information:

Command descriptions use these conventions:

- Commands and keywords are in **boldface** text.
- Arguments for which you supply values are in *italic*.
- Square brackets ([]) means optional elements.
- Braces ({ }) group required choices, and vertical bars (|) separate the alternative elements.
- Braces and vertical bars within square brackets ([{ | }]) mean a required choice within an optional element.

Interactive examples use these conventions:

- Terminal sessions and system displays are in `screen` font.
- Information you enter is in **boldface screen** font.
- Nonprinting characters, such as passwords or tabs, are in angle brackets (< >).

Notes, cautions, and warnings use these conventions and symbols:



Note

Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this manual.



Caution

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

Related Documentation

These documents provide complete information about the CDS and are available from Cisco.com:

- *Cisco Internet Streamer CDS 2.4 Software Configuration Guide*
- *Cisco Internet Streamer CDS 2.4 Alarms and Error Messages Guide*
- *Cisco Content Delivery Engine 100/200/300/400 Hardware Installation Guide*
- *Cisco Content Delivery Engine 205/220/420 Hardware Installation Guide*
- *Regulatory Compliance and Safety Information for the Cisco Content Delivery Engines*
- *Cisco Content Delivery System 2.x Documentation Roadmap*
- *Cisco Internet Streamer CDS 2.4 Quick Start Guide*
- *Cisco Internet Streamer CDS 2.4 API Guide*
- *Release Notes for Cisco Internet Streamer CDS 2.4*
- *Cisco Internet Streamer CDS 2.x Product Documentation*

You can access the software documents at the following URL:

http://www.cisco.com/en/US/products/ps7127/tsd_products_support_series_home.html

You can access the hardware documents at the following URL:

http://www.cisco.com/en/US/products/ps7126/tsd_products_support_series_home.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.



CHAPTER 1

Command-Line Interface Command Summary

This chapter provides an overview of how to use the Cisco Internet Streamer Content Delivery System (CDS) software command-line interface (CLI), including an explanation of CLI command modes, CDS devices modes, and tables that summarize the purpose of the commands in each mode. The chapter includes the following sections:

- [Using CDS Device Modes, page 1-1](#)
- [Using Command-Line Processing, page 1-1](#)
- [Using Command Modes, page 1-2](#)
- [Checking the Command Syntax, page 1-4](#)
- [System Help, page 1-6](#)
- [Saving Configuration Changes, page 1-6](#)



Note

The CLI can be accessed through the console port or Telnet.

Using CDS Device Modes

In the Cisco Internet Streamer CDS software, the device mode determines whether the CDS device is functioning as a Service Engine (SE), CDS Manager (CDSM), or Service Router (SR). The commands available from a specific CLI mode are determined by the CDS device mode in effect. Use the **device mode** global configuration command to change the current device mode to another configuration. Use the **show device-mode EXEC** command to display the current device configuration.

To determine if a specific command is available for a specific device type, see [Table 2-1](#) in [Chapter 2](#), “Internet Streamer CDS Release 2.4 Software Commands.”

Using Command-Line Processing

Cisco Internet Streamer CDS software commands are not case sensitive. You can abbreviate commands and parameters as long as they contain enough letters to be different from any other currently available commands or parameters.

You can scroll through the last 20 commands stored in the history buffer and enter or edit the command at the prompt (see [Table 1-1](#)).

Table 1-1 *Command-Line Processing Keystroke Combinations*

Keystroke Combinations	Function
Ctrl-A	Jumps to the first character of the command line.
Ctrl-B or the Left Arrow key	Moves the cursor back one character.
Ctrl-C	Escapes and terminates prompts and tasks.
Ctrl-D	Deletes the character at the cursor.
Ctrl-E	Jumps to the end of the current command line.
Ctrl-F or the Right Arrow key	Moves the cursor forward one character.
Ctrl-K	Deletes from the cursor to the end of the command line.
Ctrl-L	Repeats the current command line on a new line.
Ctrl-N or the Down Arrow key	Enters the next command line in the history buffer.
Ctrl-P or the Up Arrow key	Enters the previous command line in the history buffer.
Ctrl-T	Transposes the character at the cursor with the character to the left of the cursor.
Ctrl-U; Ctrl-X	Deletes from the cursor to the beginning of the command line.
Ctrl-W	Deletes the last word typed.
Esc-B	Moves the cursor back one word.
Esc-D	Deletes from the cursor to the end of the word.
Esc-F	Moves the cursor forward one word.
Delete key or Backspace key	Erases a mistake when entering a command; re-enter the command after using this key.

Using Command Modes

The CLI for Cisco Internet Streamer CDS Release 2.4 software is similar to the CLI for the Cisco IOS software. Both the Cisco IOS software and the CDS CLI are organized into different command and configuration modes. Each mode provides access to a specific set of commands. This section describes the command modes provided by Cisco Internet Streamer CDS Release 2.4 software CLI and includes the following topics:

- [Using EXEC Mode, page 1-3](#)
- [Using Global Configuration Mode, page 1-3](#)
- [Using Interface Configuration Mode, page 1-4](#)
- [Using Other Configuration Modes, page 1-4](#)

Using EXEC Mode

Use the EXEC mode for setting, viewing, and testing system operations. The EXEC mode is divided into two access levels, user and privileged. Use the **enable** and **disable** commands to switch between the two levels.

Access to the user-level EXEC command line requires a valid password. The user-level EXEC commands are a subset of the privileged-level EXEC commands. The user-level EXEC prompt is the host name followed by a right angle bracket (>). The prompt for the privileged-level EXEC command line is the pound sign (#). To execute an EXEC command, enter the command at the EXEC system prompt and press the **Return** key. In the following example, a user accesses the privileged-level EXEC command line from the user level.

```
ServiceEngine>enable
ServiceEngine#
```

Use the **Delete** or **Backspace** key sequences to edit commands when you enter commands at the EXEC prompt.

As a shortcut, you can abbreviate commands to the fewest letters that make them unique. For example, the letters **sho** can be entered for the **show** command.

Certain EXEC commands display multiple screens with the following prompt at the bottom of the screen:

```
--More--
```

Press the **Spacebar** to continue the output, or press **Return** to display the next line. Press any other key to return to the prompt. Also, at the --More-- prompt, you can enter a **?** to display the help message.

To leave EXEC mode, use the **exit** command at the system prompt:

```
ServiceEngine#exit
```

The EXEC commands are entered in EXEC mode.

Using Global Configuration Mode

Use global configuration mode for setting, viewing, and testing the configuration of Internet Streamer CDS software features for the entire device. To enter this mode, enter the **configure** command from privileged EXEC mode. You must be in global configuration mode to enter global configuration commands.

```
ServiceEngine#configure
ServiceEngine(config)#
```

To exit global configuration mode, use the **end** global configuration command:

```
ServiceEngine(config)#end
```

You can also exit global configuration mode by entering the **exit** command or by pressing **Ctrl-Z**.

Global configuration commands are entered in global configuration mode.

Using Interface Configuration Mode

Use the interface configuration mode for setting, viewing, and testing the configuration of Internet Streamer CDS software features on a specific interface. To enter this mode, enter the **interface** command from the global configuration mode. The following example demonstrates how to enter interface configuration mode:

```
ServiceEngine#configure
ServiceEngine(config)#interface ?
GigabitEthernet Select a gigabit ethernet interface to configure
PortChannel      Ethernet Channel of interfaces
Standby          Standby groups
```

To exit interface configuration mode, enter **exit** to return to global configuration mode:

```
ServiceEngine(config-if)#exit
ServiceEngine(config)#
```

The interface configuration commands are entered in interface configuration mode.

Using Other Configuration Modes

The CLI provides a number of other configuration modes that make it easier to configure specific features, including the configuration modes described in [Table 1-2](#).

Table 1-2 *Commands Used to Access Configuration Modes for Specific Features*

Configuration Mode	Command to Enter from Global Configuration Mode
Standard ACL configuration mode	ip access-list standard
Extended ACL configuration mode	ip access-list extended
ICAP service configuration mode	icap service

To work with these configuration modes, enter the appropriate command from the global configuration mode prompt. The CLI enters a new configuration mode where all subsequent commands apply to the current entry. To return to global configuration mode, enter the **exit** command.

For further information about these configuration modes and the commands permitted in each one, see [Chapter 2, “Internet Streamer CDS Release 2.4 Software Commands.”](#)

Checking the Command Syntax

The user interface provides error isolation in the form of an error indicator, a caret symbol (^). The ^ symbol appears at the point in the command string where you have entered an incorrect command, keyword, or argument.

In the following example, suppose you want to set the clock. Use context-sensitive help to check the syntax for setting the clock.

An example of a mistake is as follows:

```
ServiceEngine#clock ?
read-calendar    Read the calendar and update system clock
set              Set the time and date
update-calendar  Update the calendar with system clock
```

The help output shows that the **set** keyword is required. Check the syntax for entering the time.

```
ServiceEngine#clock set ?
<0-23>: Current Time (hh:mm:ss)
```

Enter the current time in a 24-hour format with hours, minutes, and seconds separated by colons.

```
ServiceEngine#clock set 13:32:00
% Incomplete command.
```

The system indicates that you need to provide additional arguments to complete the command. Press the **Up Arrow** to automatically repeat the previous command entry. Then add a space and question mark (?) to display the additional arguments.

```
ServiceEngine#clock set 13:32:00 ?
<1-31> Day of the month
January Month of the year
February
March
. . .
```

Enter the day and month as prompted and use the question mark for additional instructions.

```
ServiceEngine#clock set 13:32:00 12 April ?
<1993-2035> Year
```

Now you can complete the command entry by entering the year.

```
ServiceEngine#clock set 13:32:00 12 April 00
                                     ^
%Invalid input detected at '^' marker.
ServiceEngine#
```

The caret symbol (^) and help response indicate an error with the 00 entry. To display the correct syntax, press **Ctrl-P** or the **Up Arrow**. You can also re-enter the command string, and then enter a space character, a question mark, and press **Enter**.

```
ServiceEngine#clock set 13:32:00 12 April ?
<1993-2035> Year
ServiceEngine#clock set 13:32:00 12 April
```

Enter the year using the correct syntax and press **Return** to execute the command.

```
ServiceEngine#clock set 13:32:00 12 April 2009
Sun Aor 12 13:32:00 UTC 2009
Restarting acquisition and distribution
ServiceEngine#
```

System Help

You can obtain help when you enter commands by using the following methods:

- For a brief description of the context-sensitive help system, enter **help**.
- To list all commands for a command mode, enter a question mark (?) at the system prompt.
- To obtain a list of commands that start with a particular character set, enter an abbreviated command immediately followed by a question mark (?).

```
ServiceEngine#cl?  
clear clock
```

- To list the command keywords or arguments, enter a space and a question mark (?) after the command.

```
ServiceEngine#clock ?  
read-calendar Read the calendar and update system clock  
set           Set the time and date  
update-calendarUpdate the calendar with system clock
```

Saving Configuration Changes

To avoid losing new configurations, save them to NVRAM using the **copy** or **write** commands, as shown in the following examples:

```
ServiceEngine#copy running-config startup-config
```

or

```
ServiceEngine#write
```

See the command description for the **copy running-config startup-config** command for more information on “running” and “saved” configuration modes.

2

Internet Streamer CDS Release 2.4 Software Commands

This chapter contains an alphabetical listing of all the commands in Cisco Internet Streamer CDS Release 2.4 software. The Internet Streamer CDS software CLI is organized into the following command modes:

- EXEC mode—For setting, viewing, and testing system operations. It is divided into two access levels, user and privileged. To use the privileged access level, enter the **enable** command at the user access level prompt and then enter the privileged EXEC password when you see the password prompt.
- Global configuration mode—For setting, viewing, and testing the configuration of Internet Streamer CDS software features for the entire device. To use this mode, enter the **configure** command from privileged EXEC mode.
- Interface configuration mode—For setting, viewing, and testing the configuration of a specific interface. To use this mode, enter the **interface** command from global configuration mode.
- Other configuration modes—A number of configuration modes are available from the global configuration mode for managing specific features. The commands used to access these modes are marked with a footnote in [Table 2-1](#).

See [Chapter 1, “Using Command Modes,”](#) for a complete discussion of using CLI command modes.

[Table 2-1](#) summarizes the Internet Streamer CDS commands and indicates the command mode for each command. The commands used to access configuration modes are marked with a footnote in [Table 2-1](#). The same command may have different effects when entered in a different command mode, and for this reason, they are listed and documented separately. In [Table 2-1](#), when the first occurrence is entered in EXEC mode, the second occurrence is entered in global configuration mode. When the first occurrence is entered in global configuration mode, the second occurrence is entered in interface configuration mode.

The Internet Streamer CDS software device mode determines whether the Internet Streamer CDS device is functioning as a Service Engine (SE), CDS Manager (CDSM), or Service Router (SR). The commands available from a specific CLI mode are determined by the Internet Streamer CDS device mode in effect. [Table 2-1](#) also indicates the device mode for each command. *All* indicates that the command is available for every device mode.



Note

When viewing this guide online, click the name of the command in the left column of the table to jump to the command page, which provides the command syntax, examples, and usage guidelines.



Note

See [Appendix A, “Acronyms”](#) for an expansion of all acronyms used in this publication.

Table 2-1 CLI Commands

Command	Description	CLI Mode	Device Mode
access-lists	Configures the access control list entries.	Global configuration	SE
acquirer (EXEC)	Configures the content acquirer.	Privileged-level EXEC	SE
acquirer (global configuration)	Enables authentication when the acquirer obtains content through a proxy server.	Global configuration	SE
acquisition-distribution	Starts and stops the acquisition and distribution database cleanup process and the content acquisition and distribution process.	Privileged-level EXEC	SE
alarm overload-detect	Configures the detection of alarm overload.	Global configuration	All
asset	Configures the CISCO-ENTITY-ASSET-MIB.	Global configuration	All
authentication	Configures the authentication parameters.	Global configuration	All
authsvr	Enables and configures the Authorization server.	Global configuration	SE
bandwidth (global configuration)	Sets the allowable bandwidth usage and its duration for the Movie Streamer and WMT streaming media.	Global configuration	SE
bandwidth (interface configuration)	Sets the specified interface bandwidth to 10, 100, or 1000 Mbps.	Interface configuration	All
banner	Configures the EXEC, login, and message-of-the-day (MOTD) banners.	Global configuration	All
bitrate	Configures the maximum pacing bit rate for the Movie Streamer and configures WMT bit-rate settings.	Global configuration	SE
cache	Specifies the cache commands.	Global configuration	SE
capability	Modifies the capability configuration.	Global configuration	SE
cd	Changes the directory.	User-level EXEC & privileged-level EXEC	All
cdnfs	Manages the Internet Streamer CDS network file system (cdnfs).	Privileged-level EXEC	SE
cdsm	Configures the CDSM IP address and primary or standby role settings.	Global configuration	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
clear	Clears the HTTP object cache, the hardware interface, statistics, archive working transaction logs, and other settings.	Privileged-level EXEC	All
clock (exec)	Manages the system clock.	Privileged-level EXEC	All
clock (global configuration)	Sets the summer daylight saving time of day and time zone.	Global configuration	All
cms (EXEC)	Configures the Centralized Management System (CMS) embedded database parameters.	Privileged-level EXEC	All
cms (global configuration)	Schedules the maintenance and enables the Centralized Management System on a given node.	Global configuration	All
configure¹	Enters configuration mode from privileged EXEC mode.	Privileged-level EXEC	All
copy	Copies the configuration or image files to and from the CD-ROM, flash memory, disk, or remote hosts.	Privileged-level EXEC	All
cpfile	Copies a file.	User-level EXEC & privileged-level EXEC	All
debug	Configures the debugging options.	Privileged-level EXEC	All
delfile	Deletes a file.	User-level EXEC & privileged-level EXEC	All
deltree	Deletes a directory and its subdirectories.	User-level EXEC & privileged-level EXEC	All
device	Configures the mode of operation on a device.	Global configuration	All
dir	Displays the files in a long list format.	User-level EXEC & privileged-level EXEC	All
direct-server-return	Enable a VIP for direct server return.	Global configuration	SE, SR
disable	Turns off the privileged EXEC commands.	Privileged-level EXEC	All
disk (EXEC)	Allocates the disks among the cdnfs and sysfs file systems.	Privileged-level EXEC	All
disk (global configuration)	Configures how the disk errors should be handled.	Global configuration	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
distribution	Reschedules and refreshes the content redistribution through multicast for all delivery services or a specified delivery service ID or name.	Privileged-level EXEC	SE, SR
dnslookup	Resolves a host or domain name to an IP address.	User-level EXEC & privileged-level EXEC	
enable ¹	Accesses the privileged EXEC commands.	User-level EXEC & privileged-level EXEC	All
end	Exits configuration and privileged EXEC modes.	Global configuration	All
exec-timeout	Configures the length of time that an inactive Telnet or Secure Shell (SSH) session remains open.	Global configuration	All
exit	Exits from interface, global configuration, or privileged EXEC modes.	All	All
external-ip	Configures up to a maximum of eight external IP addresses.	Global configuration	All
find-pattern	Searches for a particular pattern in a file.	Privileged-level EXEC	All
flash-media-streaming	Enables and configures Flash Media Streaming.	Global configuration	SE, SR
help	Obtains online help for the command-line interface.	Global configuration and user-level EXEC	All
hostname	Configures the device network name.	Global configuration	All
http	Configures the HTTP-related parameters.	Global configuration	SE, SR
icap	Enables the Internet Content Adaptation Protocol for supporting third-party software applications and plug-ins.	Global configuration	SE
icap service ¹	Configures ICAP service configurations. Provides access to the ICAP service configuration mode.	Global configuration	SE
install	Installs a new version of the caching application.	Privileged-level EXEC	All
interface ¹	Configures a Gigabit Ethernet or port-channel interface. Provides access to interface configuration mode.	Global configuration	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
ip	Configures the Internet Protocol.	Global configuration	All
ip access-list¹	Creates and modifies the access lists for controlling access to interfaces or applications. Provides access to ACL configuration mode.	Global configuration	SE
ipv6	Specifies the default gateway's IPv6 address.	Global configuration	SE
kernel kdb	Enables the kernel debugger configuration mode.	Global configuration	All
line	Specifies the terminal line settings.	Global configuration	All
lls	Displays the files in a long list format.	User-level EXEC & privileged-level EXEC	All
logging	Configures system logging (syslog).	Global configuration	All
ls	Lists the files and subdirectories in a directory.	User-level EXEC & privileged-level EXEC	All
mkdir	Makes a directory.	User-level EXEC & privileged-level EXEC	All
mkfile	Makes a file (for testing).	User-level EXEC & privileged-level EXEC	All
movie-streamer	Enables and configures the Movie Streamer server.	Global configuration	SE
mtu	Sets the interface maximum transmission unit packet size.	interface configuration	All
no (global configuration)	Negates a global configuration command or sets its defaults.	Global configuration	All
no (interface configuration)	Negates an interface command or sets its defaults.	interface configuration	All
ntp	Configures the Network Time Protocol server.	Global configuration	All
ntpdate	Sets the NTP software clock.	Privileged-level EXEC	All
ping	Sends the echo packets.	User-level EXEC & privileged-level EXEC	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
ping6	Pings the IPv6 address.	User-level EXEC & privileged-level EXEC	SE
port-channel	Configures the port-channel load-balancing options.	Global configuration	All
primary-interface	Configures a primary interface for the Internet Streamer CDS network to be a Gigabit Ethernet or port-channel interface.	Global configuration	All
pwd	Displays the present working directory.	User-level EXEC & privileged-level EXEC	All
qos	Globally enables QoS functionality on the device.	Global configuration	SE
radius-server	Configures the RADIUS authentication.	Global configuration	All
rcp	Enables RCP.	Global configuration	All
rea	Initiates the remote execution agent.	User-level EXEC & privileged-level EXEC	SE
reload	Halts a device and performs a cold restart.	Privileged-level EXEC	All
rename	Renames a file.	User-level EXEC & privileged-level EXEC	All
restore	Restores a device to its manufactured default status.	Privileged-level EXEC	All
rmdir	Removes a directory.	User-level EXEC & privileged-level EXEC	All
rtsp	Configures the Real-Time Streaming Protocol-related parameters.	Global configuration	SE
rule	Sets the rules by which the SE filters HTTP, HTTPS, and RTSP traffic.	Global configuration	SE
script	Checks the errors in a script or executes a script.	Privileged-level EXEC	All
service-router	Configures service routing.	Global configuration	SE, SR
setup	Configures the basic configuration settings and a set of commonly used caching services.	Privileged-level EXEC	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
show	Displays the running system information.	User-level EXEC & privileged-level EXEC	All
show access-lists	Displays the access control list configuration.	User-level EXEC & privileged-level EXEC	SE
show acquirer	Displays the acquirer delivery service information and progress for a specified delivery service number or name.	User-level EXEC & privileged-level EXEC	SE
show alarms	Displays information on various types of alarms, their status, and history.	Privileged-level EXEC	All
show arp	Displays the Address Resolution Protocol entries.	User-level EXEC & privileged-level EXEC	All
show authentication	Displays the authentication configuration.	User-level EXEC & privileged-level EXEC	All
show authsvr	Displays the Authorization Server status.	User-level EXEC & privileged-level EXEC	SE
show bandwidth	Displays the bandwidth allocated to a particular device.	User-level EXEC & privileged-level EXEC	SE, SR
show banner	Displays information on various types of banners.	User-level EXEC & privileged-level EXEC	All
show bitrate	Displays the SE bit-rate configuration.	User-level EXEC & privileged-level EXEC	SE, SR
show cache	Displays a list of cached contents.	User-level EXEC & privileged-level EXEC	SE
show capability	Displays information for the Cap-X profile ID.	User-level EXEC & privileged-level EXEC	SE
show cdnfs	Displays the Internet Streamer CDS network file system information.	User-level EXEC & privileged-level EXEC	SE, CDSM
show clock	Displays the system clock.	User-level EXEC & privileged-level EXEC	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
<code>show cms</code>	Displays the Centralized Management System protocol, embedded database content, maintenance status, and other information.	User-level EXEC & privileged-level EXEC	All
<code>show content</code>	Displays all content entries in the CDS.	User-level EXEC & privileged-level EXEC	SE
<code>show debugging</code>	Displays the state of each debugging option the state of each debugging option.	User-level EXEC & privileged-level EXEC	All
<code>show device-mode</code>	Displays the configured or current mode of a CDSM, SE, or SR device.	User-level EXEC & privileged-level EXEC	All
<code>show direct-server-return</code>	Displays the Direct Server return information.	User-level EXEC & privileged-level EXEC	SE, SR
<code>show disks</code>	Displays the disk configurations.	User-level EXEC & privileged-level EXEC	All
<code>show distribution</code>	Displays the distribution information for a specified delivery service.	User-level EXEC & privileged-level EXEC	SE
<code>show flash</code>	Displays the flash memory information.	User-level EXEC & privileged-level EXEC	All
<code>show flash-media-streaming</code>	Displays the Flash Media Streaming information.	User-level EXEC & privileged-level EXEC	SE, SR
<code>show ftp</code>	Displays the caching configuration of the File Transfer Protocol (FTP).	User-level EXEC & privileged-level EXEC	All
<code>show hardware</code>	Displays the system hardware information.	User-level EXEC & privileged-level EXEC	All
<code>show hosts</code>	Displays the IP domain name, name servers, IP addresses, and host table.	User-level EXEC & privileged-level EXEC	All
<code>show http</code>	Displays the HTTP-related caching configuration.	User-level EXEC & privileged-level EXEC	SE
<code>show icap</code>	Displays the ICAP configurations.	User-level EXEC & privileged-level EXEC	SE

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
show interface	Displays the hardware interface information.	User-level EXEC & privileged-level EXEC	All
show inventory	Displays the system inventory information.	User-level EXEC & privileged-level EXEC	All
show ip access-list	Displays the information about access lists that are defined and applied to specific interfaces or applications.	User-level EXEC & privileged-level EXEC	SE
show ip routes	Displays the IP routing table.	User-level EXEC & privileged-level EXEC	All
show ldap	Displays the LDAP parameters.	User-level EXEC & privileged-level EXEC	SE
show logging	Displays the system logging configuration.	User-level EXEC & privileged-level EXEC	All
show movie-streamer	Displays the Movie Streamer configuration.	User-level EXEC & privileged-level EXEC	SE
show ntp	Displays the Network Time Protocol configuration status.	User-level EXEC & privileged-level EXEC	All
show processes	Displays the process status.	User-level EXEC & privileged-level EXEC	All
show programs	Displays the scheduled programs.	User-level EXEC & privileged-level EXEC	SE
show qos	Displays QoS information.	User-level EXEC & privileged-level EXEC	SE
show radius-server	Displays the RADIUS server information.	User-level EXEC & privileged-level EXEC	All
show rea	Displays the REA information.	User-level EXEC & privileged-level EXEC	SE
show rcp	Displays RCP information	User-level EXEC & privileged-level EXEC	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
<code>show rtsp</code>	Displays the RTSP configurations.	User-level EXEC & privileged-level EXEC	SE
<code>show rule</code>	Displays the Rules Template configuration information.	User-level EXEC & privileged-level EXEC	SE
<code>show running-config</code>	Displays the current operating configuration.	User-level EXEC & privileged-level EXEC	All
<code>show service-router</code>	Displays the service router configuration.	User-level EXEC & privileged-level EXEC	All
<code>show services</code>	Displays the services-related information.	User-level EXEC & privileged-level EXEC	All
<code>show snmp</code>	Displays the SNMP parameters.	User-level EXEC & privileged-level EXEC	All
<code>show ssh</code>	Displays the Secure Shell status and configuration.	User-level EXEC & privileged-level EXEC	All
<code>show standby</code>	Displays the information related to the standby interface.	User-level EXEC & privileged-level EXEC	All
<code>show startup-config</code>	Displays the startup configuration.	User-level EXEC & privileged-level EXEC	All
<code>show statistics access-lists 300</code>	Displays the access control list statistics.	User-level EXEC & privileged-level EXEC	SE
<code>show statistics acquirer</code>	Displays the SE acquirer delivery service statistics.	User-level EXEC & privileged-level EXEC	SE
<code>show statistics authentication</code>	Displays the authentication statistics.	User-level EXEC & privileged-level EXEC	SE
<code>show statistics cdnfs</code>	Displays the SE Internet Streamer CDS network file system statistics.	User-level EXEC & privileged-level EXEC	SE, CDSM
<code>show statistics distribution</code>	Displays the simplified statistics for content distribution components.	User-level EXEC & privileged-level EXEC	SE

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
show statistics flash-media-streaming	Displays the statistics for Flash Media Streaming.	User-level EXEC & privileged-level EXEC	SE
show statistics http	Displays the Hypertext Transfer Protocol statistics.	User-level EXEC & privileged-level EXEC	SE, SR
show statistics icap	Displays the ICAP-related statistics.	User-level EXEC & privileged-level EXEC	SE
show statistics icmp	Displays the Internet Control Message Protocol statistics.	User-level EXEC & privileged-level EXEC	All
show statistics ip	Displays the Internet Protocol statistics.	User-level EXEC & privileged-level EXEC	All
show statistics movie-streamer	Displays statistics for the Movie Streamer.	User-level EXEC & privileged-level EXEC	SE
show statistics netstat	Displays the Internet socket connection statistics.	User-level EXEC & privileged-level EXEC	All
show statistics qos	Displays statistics for the QoS policy service.	User-level EXEC & privileged-level EXEC	SE
show statistics radius	Displays the RADIUS authentication statistics.	User-level EXEC & privileged-level EXEC	All
show statistics replication	Displays the delivery service replication status and related statistical data.	User-level EXEC & privileged-level EXEC	SE, CDSM
show statistics service-router	Displays the Service Router statistics.	User-level EXEC & privileged-level EXEC	SR
show statistics services	Displays the services statistics.	User-level EXEC & privileged-level EXEC	All
show statistics snmp	Displays the SNMP statistics.	User-level EXEC & privileged-level EXEC	All
show statistics tacacs	Displays the Service Engine TACACS+ authentication and authorization statistics.	User-level EXEC & privileged-level EXEC	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
<code>show statistics tcp</code>	Displays the Transmission Control Protocol statistics.	User-level EXEC & privileged-level EXEC	All
<code>show statistics transaction-logs</code>	Displays the transaction log export statistics.	User-level EXEC & privileged-level EXEC	SE
<code>show statistics udp</code>	Displays the User Datagram Protocol statistics.	User-level EXEC & privileged-level EXEC	All
<code>show statistics wmt</code>	Displays the Windows Media Technologies statistics.	User-level EXEC & privileged-level EXEC	SE
<code>show tacacs</code>	Displays TACACS+ authentication protocol configuration information.	User-level EXEC & privileged-level EXEC	All
<code>show tech-support</code>	Displays the system information for Cisco technical support.	User-level EXEC & privileged-level EXEC	All
<code>show telnet</code>	Displays the Telnet services configuration.	User-level EXEC & privileged-level EXEC	All
<code>show transaction-logging</code>	Displays the transaction logging information.	User-level EXEC & privileged-level EXEC	SE
<code>show url-signature</code>	Displays the URL signature information.	User-level EXEC & privileged-level EXEC	SE
<code>show user</code>	Displays the user identification number and username information.	User-level EXEC & privileged-level EXEC	All
<code>show users</code>	Displays the specified users.	User-level EXEC & privileged-level EXEC	All
<code>show version</code>	Displays the software version.	User-level EXEC & privileged-level EXEC	All
<code>show wmt</code>	Displays the WMT configuration.	User-level EXEC & privileged-level EXEC	SE
<code>shutdown (interface configuration)</code>	Shuts down the specified interface.	interface configuration	All
<code>shutdown (EXEC)</code>	Shuts down the device (stops all applications and operating system).	Privileged-level EXEC	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
snmp-server community	Configures the community access string to permit access to the SNMP.	Global configuration	All
snmp-server contact	Specifies the text for the MIB object sysContact.	Global configuration	All
snmp-server enable traps	Enables the SNMP traps.	Global configuration	All
snmp-server group	Defines a user security model group.	Global configuration	All
snmp-server host	Specifies the hosts to receive SNMP traps.	Global configuration	All
snmp-server location	Specifies the path for the MIB object sysLocation.	Global configuration	All
snmp-server notify inform	Configures the SNMP inform request.	Global configuration	All
snmp-server user	Defines a user who can access the SNMP engine.	Global configuration	All
snmp-server view	Defines a Version 2 SNMP (SNMPv2) MIB view.	Global configuration	All
sshd	Configures the SSH service parameters.	Global configuration	All
sysreport	Saves the sysreport onto a user-specified file.	Privileged-level EXEC	SE
tacacs	Configures TACACS+ server parameters.	Global configuration	All
tcpdump	Dumps the TCP traffic on the network.	Privileged-level EXEC	All
telnet	Starts the Telnet client.	User-level EXEC & privileged-level EXEC	All
telnet enable	Enables the Telnet services.	Global configuration	All
terminal	Sets the terminal output commands.	User-level EXEC & privileged-level EXEC	All
test-url	Tests the accessibility of a URL using FTP, HTTP, or HTTPS.	User-level EXEC & privileged-level EXEC	SE, SR
traceroute	Traces the route to a remote host.	User-level EXEC & privileged-level EXEC	All
traceroute6	Traces the route to a remote IPv6-enabled host.	User-level EXEC & privileged-level EXEC	SE, SR

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
transaction-log force	Forces archiving of the working log file to make a transaction log file.	Privileged-level EXEC	All
transaction-logs	Configures and enables the transaction logging parameters.	Global configuration	SE
type	Displays a file.	User-level EXEC & privileged-level EXEC	All
type-tail	Displays the last several lines of a file.	User-level EXEC & privileged-level EXEC	All
undebg	Disables the debugging functions (see also debug).	Privileged-level EXEC	All
url-signature	Configures the url signature,	Global configuration	SE
username	Establishes the username authentication.	Global configuration	All
whoami	Displays the current user's name.	User-level EXEC & privileged-level EXEC	All
wmt	Configures the WMT.	Global configuration	SE
write	Writes or erases the startup configurations to NVRAM or to a terminal session, or writes the MIB persistence configuration to disk.	Privileged-level EXEC	All

1. Commands used to access configuration modes.

access-lists

To configure access control list entries, use the **access-lists** global configuration command. To remove access control list entries, use the **no** form of this command.

```
access-lists {300 {deny groupname {any [position number] | groupname [position number]}} |
               {permit groupname {any [position number] | groupname [position number]}} | enable}

no access-lists {300 {deny groupname {any [position number] | groupname [position number]}} |
                 {permit groupname {any [position number] | groupname [position number]}} | enable}
```

Syntax Description		
300		Specifies the group name-based access control list (ACL).
deny		Specifies the rejection action.
groupname		Defines which groups are granted or denied access to content that is served by this SE.
any		Specifies any group name.
position		(Optional) Specifies the position of the access control list record within the access list.
<i>number</i>		Position number within the access control list (1–4294967294).
<i>groupname</i>		Name of the group that is permitted or denied from accessing the Internet using an SE.
permit		Specifies the permission action.
enable		Enables the access control list.

Defaults No default behavior or values.

Command Modes Global configuration

Usage Guidelines In the Internet Streamer CDS 2.x software, you can configure group authorization using an access control list (ACL) only after a user has been authenticated against an LDAP HTTP-request authentication server. The use of this list configures a group privilege when members of the group are accessing content provided by the SE. You can use the ACL to allow the users who belong to certain groups or to prevent them from viewing specific content. This authorization feature offers more granular access control by specifying that access is only allowed to specific groups.

Use the **access-lists enable** global configuration command to enable the use of the ACL.

Use the **access-lists 300** command to permit or deny a group from accessing the Internet using the SE. For instance, use the **access-lists 300 deny groupname marketing** command to prevent any user from the marketing group from accessing content through the SE.

At least one login authentication method, such as local, TACACS+, or RADIUS, must be enabled.



Note

We recommend that you configure the local login authentication method as the primary method.

In Cisco Internet Streamer Release 2.4 software, the access control list contains the following feature enhancements and limitations:

- A user can belong to several groups.
- A user can belong to an unlimited number of groups within group name strings.
- A group name string is a case-sensitive string with mixed-case alphanumeric characteristics.
- Each unique group name string cannot exceed 128 characters.



Note If the unique group name string is longer than 128 characters, the group is ignored.

- The group names in a group name string are separated by a comma.
- The total string of individual group names cannot exceed 750 characters.

For Windows-based user groups, you must append the domain name in front of the group name in the form domain or group as follows:

For Windows NT-based user groups, use the domain NetBIOS name.

Examples

The following example shows how to display the configuration of the access control list by using the **show access-lists 300** command:

```
ServiceEngine#show access-lists 300
Access Control List Configuration
-----
Access Control List is enabled

Groupname-based List (300)
1. permit groupname techpubs
2. permit groupname acmel
3. permit groupname engineering
4. permit groupname sales
5. permit groupname marketing
6. deny groupname any
```

The following example shows how to display statistical information for the access control list by using the **show statistics access-lists 300** command:

```
ServiceEngine#show statistics access-lists 300
Access Control Lists Statistics
-----
Groupname and username-based List (300)
Number of requests:      1
Number of deny responses: 0
Number of permit responses: 1
```

The following example shows how to reset the statistical information for the access control list by using the **clear statistics access-lists 300** command:

```
ServiceEngine#clear statistics access-lists 300
ServiceEngine(config)#access-lists 300 permit groupname acmel position 2
```

Related Commands

show access-lists 300
show statistics access-list 300

acquirer (EXEC)

To start or stop content acquisition on a specified acquirer delivery service, use the **acquirer** EXEC command. You can also use this command to verify and correct the Last-Modified-Time attribute in content acquired using the Cisco Internet Streamer CDS software.

```
acquirer {check-time-for-old-content [delivery-service-id delivery-service-num |
delivery-service-name delivery-service-name] | [correct [delivery-service-id
delivery-service-num | delivery-service-name delivery-service-name]] | start-delivery-service
{delivery-service-id delivery-service-num | delivery-service-name delivery-service-name} |
stop-delivery-service {delivery-service-id delivery-service-num | delivery-service-name
delivery-service-name} | test-url url [use-http-proxy url | use-smb-options smb-options]}
```

Syntax Description

check-time-for-old-content	Checks the content for Last-Modified-Time attributes in the local time format.
delivery-service-id	(Optional) Sets the delivery service number identifier.
<i>delivery-service-num</i>	(Optional) Delivery service number (0–4294967295).
delivery-service-name	(Optional) Sets the delivery service name descriptor.
<i>delivery-service-name</i>	(Optional) Delivery service name.
correct	(Optional) Changes the Last-Modified-Time attributes in the local time format to the Greenwich mean time (GMT) format.
start-delivery-service	Starts the content acquisition.
stop-delivery-service	Stops the content acquisition.
test-url	Tests the accessibility of a URL, using HTTP, HTTPS, FTP, or SMB.
<i>url</i>	URL to be tested.
	Note For the Server Message Block (SMB) protocol, use the uniform naming convention (UNC) path, for example, //host/share/file.
use-http-proxy	(Optional) Specifies the HTTP proxy. The connectivity of the URL (content request over HTTP) through the HTTP proxy server (the SE) is tested. Use this option only when the HTTP protocol is used.
<i>url</i>	HTTP proxy URL. Use one of the following formats to specify the HTTP proxy URL: http://proxyIpAddress:proxyPort http://proxyUser:proxypasswd@proxyIpAddress:proxyPort
use-smb-options	(Optional) Specifies the username, password, port, and domain for the SMB URL.
<i>smb-options</i>	Parameters to be specified when an SMB URL is used. Use the following format to specify these parameters: username=xxx,password=xxx,port=xxx,workgroup=xxx Note All the comma-separated key=value pairs are optional and need to be specified only if the SMB host requires them.

Defaults

If you do not specify the delivery service, this command applies to all delivery services assigned to the root SE.

Command Modes EXEC**Usage Guidelines**

The acquirer is a software agent that gathers delivery service content before it is distributed to the receiver SEs in an Internet Streamer CDS network. The acquirer maintains a task list, which it updates after receiving a notification of changes in its delivery service configuration.

The acquirer stores the Last-Modified-Time attribute in the local time format. Content acquired using earlier software releases has a Last-Modified-Time attribute that is incorrect if used with later versions of the Internet Streamer CDS software, which use GMT format.

With Internet Streamer CDS Release 2.4 software, you must correct the Last-Modified-Time attributes for content acquired with earlier releases by entering the following command from the privileged EXEC prompt:

acquirer check-time-for-old-content correct [**delivery-service-id** *delivery-service-num* **delivery-service-name** *delivery-service-name*]

This command changes the Last-Modified-Time attributes for content in all delivery services assigned to the root SE unless you specify the delivery service ID or name.

SEs running Internet Streamer CDS Release 2.4 software identify changes in the Last-Modified-Time attribute and download content only when changes have occurred.

Use the **acquirer start-delivery-service** command to immediately start acquisition tasks for the selected delivery-service. Use the **acquirer stop-delivery-service** command to immediately stop all acquisition tasks for the selected delivery service.

Use the **acquirer test-url url** EXEC command to test whether a URL is accessible or not. The actual content is dumped into the path /dev/null.

Examples

The following example shows how the acquirer starts acquiring content on delivery service 86:

```
ServiceEngine#acquirer start-delivery-service delivery-service-id 86

ServiceEngine#acquirer start-delivery-service delivery-service-name corporate
```

The following example shows how the acquirer stops acquiring content on delivery service 86:

```
ServiceEngine#acquirer stop-delivery-service delivery-service-id 86

ServiceEngine#acquirer stop-delivery-service delivery-service-name corporate
```

The following example shows how the **acquirer test-url** command is used to test a URL:

```
ServiceEngine#acquirer test-url http://172.16.150.26
--05:16:41-- http://10.107.150.26
=> /dev/null'
Connecting to 10.107.150.26:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1,722 [text/html]

100%[=====] 1,722 1.64M/s ETA 00:00

02:45:40 (1.64 MB/s) - '/dev/null' saved [1722/1722]
```

Related Commands

show acquirer
show statistics acquirer

acquirer (global configuration)

To provide authentication when the acquirer obtains content through a proxy server, use the **acquirer** global configuration command. To disable acquirer proxy authentication, use the **no** form of this command.

acquirer proxy authentication {**outgoing** {*hostname* | *ip-address*} *port-num*} *username* | **password** *password*}

no acquirer proxy authentication {**outgoing** {*hostname* | *ip-address*} *port-num*} *username* | **password** *password*}

Syntax Description		
proxy		Configures parameters for outgoing proxy-mode requests for content acquisition.
authentication		Enables authentication so the acquirer can obtain content through a proxy server.
outgoing		Enables authentication for a nontransparent proxy server.
<i>hostname</i>		Hostname of a nontransparent proxy server.
<i>ip-address</i>		IP address of a nontransparent proxy server.
<i>port-num</i>		Port number of a nontransparent proxy server (1–65535).
<i>username</i>		Username for authentication using a maximum of 256 characters.
password		Allows the use of a password for authentication.
<i>password</i>		Password for authentication using a maximum of 256 characters.

Defaults No default behavior or values.

Command Modes Global configuration

Usage Guidelines Use the **acquirer proxy authentication outgoing** global configuration command to configure authentication when you enable content acquisition through a proxy server. You must first configure the proxy host and the port using the **http proxy outgoing host** global configuration command. The maximum number of outgoing proxies allowed is eight. When you remove an outgoing proxy using the **no http outgoing proxy** command, the authentication information associated with that proxy is automatically removed.

Use the **acquirer proxy authentication transparent** command for transparent caches in the Internet Streamer CDS network that require authentication.

The acquirer supports a proxy with basic authentication. Content acquisition through a proxy server is supported only for HTTP and not for HTTPS or FTP. Also, authentication is only supported for a single proxy server in a chain, so if multiple proxy servers in a chain require authentication, the request will fail.

Acquisition through a proxy server can be configured when the root SE cannot directly access the origin server because the origin server is set up to allow access only by a specified proxy server. When a proxy server is configured for root SE content acquisition, the acquirer contacts the proxy server instead of the origin server, and all requests to that origin server go through the proxy server.

**Note**

Content acquisition through a proxy server is only supported for HTTP requests. It is not supported for HTTPS, FTP, MMS, or MMS-over-HTTP requests.

There are three ways to configure the proxy server: through the CDSM GUI, through the SE CLI, or through the manifest file. If you need to configure the SE to use the proxy for both caching and pre-positioned content, use the CLI to configure the proxy. The CLI command is a global configuration command that configures the entire SE to use the proxy. If only the acquirer portion of the SE needs to use the proxy for acquiring the pre-positioned content, use the manifest file or specify the outgoing proxy. When you configure the proxy server in the manifest file, you are configuring the acquirer to use the proxy to fetch the content for a particular delivery service.

**Note**

Proxy configurations in the manifest file take precedence over proxy configurations in the CLI. A *noProxy* attribute configuration in the manifest file takes precedence over the other proxy server configurations in the manifest file.

You can also configure a proxy for fetching the manifest file by using the CDSM GUI (the Creating New Delivery Service or Modifying Delivery Service window). When you configure a proxy server in the CDSM GUI, the proxy configuration is valid only for acquiring the manifest file itself and not for acquiring the delivery service content. Requests for the manifest file go through the proxy server, and requests for the content go directly to the origin server.

**Tip**

Before configuring a proxy server, verify that the root SE is able to ping the proxy server. To check whether the proxy server is accepting incoming HTTP traffic at the configured port, use the **acquirer test-url** `http://proxyIP:proxyport` global configuration command in the root SE CLI, where the URL in the command is the URL of the proxy server being tested. If the proxy is not servicing the configured port, this message displays “failed: Connection refused.”

Examples

The following example shows the authentication configuration for a transparent proxy server with basic authentication:

```
ServiceEngine(config)#acquirer proxy authentication transparent 192.168.1.1 8080 myname
```

Related Commands

http proxy outgoing
show acquirer

acquisition-distribution

To start or stop the content acquisition and distribution process, use the **acquisition-distribution EXEC** command.

acquisition-distribution {database-cleanup {start | stop} | start | stop}

Syntax Description	database-cleanup	Cleans up the acquisition and distribution database to maintain consistency with the file system.
	start	Starts the cleanup of the acquisition and distribution database.
	stop	Stops the cleanup of the acquisition and distribution database.
	start	Starts the acquisition and distribution process.
	stop	Stops the acquisition and distribution process.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines When you use the **acquisition-distribution database-cleanup** command, the acquisition and distribution database is checked to ensure that all pre-positioned content is available in cdnfs. If any pre-positioned content is found to be missing from cdnfs, the content is replicated to all SEs in the Internet Streamer CDS network. Root SEs assigned to a delivery service acquire the content directly from the origin server and replicate the content through the delivery service either by unicast or multicast transmission to other SEs in the delivery service. Receiver SEs obtain the content from forwarder SEs either by unicast or multicast. In the case of a disk00 failure when the database is stored on disk00 in an internal file system (/state), the recovery of the acquisition and distribution database is done automatically. You should run the acquisition and distribution database cleanup if a failure occurs or if you have to replace a disk drive other than disk00.

Examples The following example starts the acquisition and distribution database cleanup process:

```
ServiceEngine#acquisition-distribution database-cleanup start
```

The following example starts the acquisition and distribution process:

```
ServiceEngine#acquisition-distribution start
```

The following example stops the acquisition and distribution process:

```
ServiceEngine#acquisition-distribution stop
```

Related Commands

- cdnfs cleanup
- show acquirer
- show distribution

alarm overload-detect

To detect alarm overload situations, use the **alarm overload-detect** global configuration command. To disable alarm overload detection, use the **no** form of this command.

alarm overload-detect {**clear** 1-999 [**raise** 10-1000] | **enable** | **raise** 10-1000 [**clear** 1-999]}

no alarm overload-detect {**clear** 1-999 [**raise** 10-1000] | **enable** | **raise** 10-1000 [**clear** 1-999]}

Syntax Description

clear	Specifies the threshold below which the alarm overload state on the SE is cleared and the SNMP traps and alarm notifications to the Centralized Management System (CMS) resume. Note The alarm overload-detect clear value must be less than the alarm overload-detect raise value.
1-999	Number of alarms per second that ends an alarm overload condition.
raise	(Optional) Specifies the threshold at which the CDE enters an alarm overload state and SNMP traps and alarm notifications to CMS are suspended.
10-1000	Number of alarms per second that triggers an alarm overload.
enable	(Optional) Enables the detection of alarm overload situations.

Defaults

raise: 10 alarms per second

clear: 1 alarm per second

Command Modes

Global configuration

Usage Guidelines

When multiple applications running on an SE experience problems at the same time, numerous alarms are set off simultaneously, and the SE may stop responding. In the Internet Streamer CDS 2.2 software and later releases, you can use the **alarm overload-detect** global configuration command to set an overload limit for the incoming alarms from the node health manager. If the number of alarms exceeds the maximum number of alarms allowed, the SE enters an alarm overload state until the number of alarms drops down to the number defined in the **clear** option.

When the SE is in the alarm overload state, the following events occur:

- An alarm overload notification is sent to SNMP and the CMS. The **clear** and **raise** values are also communicated to SNMP and the CMS.
- SNMP traps and CMS notifications for subsequent alarm raise and clear operations are suspended.
- An alarm overload clear notification is sent.
- The SE remains in the alarm overload state until the rate of incoming alarms decreases to the **clear** value.

**Note**

In the alarm overload state, applications continue to raise alarms and the alarms are recorded within the SE. The **show alarms** and **show alarms history EXEC** commands will display all the alarms even in the alarm overload state.

Examples

The following example enables the detection of alarm overload:

```
ServiceEngine(config)#alarm overload-detect enable
```

The following example sets the threshold for triggering the alarm overload at 100 alarms per second:

```
ServiceEngine(config)#alarm overload-detect raise 100
```

The following example sets the level for clearing the alarm overload at 10 alarms per second:

```
ServiceEngine(config)#alarm overload-detect clear 10
```

Related Commands

show alarms
show alarm status

asset

To to configure the CISCO-ENTITY-ASSET-MIB, use the **asset** global configuration command. To remove the asset tag name, use the **no** form of this command.

```

asset tag name

no asset tag name

```

Syntax Description

tag	Sets the asset tag.
<i>name</i>	Asset tag name string.

Defaults

No default behavior or values.

Command Modes

Global configuration

Examples

The following example shows how to configure a tag name for the asset tag string:

```

ServiceEngine(config)#asset tag entitymib

```


authentication

To specify authentication and authorization methods, use the **authentication** global configuration command. To selectively disable options, use the **no** form of this command.

authentication {**configuration** {**local** | **radius** | **tacacs**} **enable** [**primary** | **secondary**] | **fail-over** **server-unreachable** | **login** {**local** | **radius** | **tacacs**} **enable** [**primary** | **secondary**]}

no authentication {**configuration** {**local** | **radius** | **tacacs**} **enable** [**primary** | **secondary**] | **fail-over** **server-unreachable** | **login** {**local** | **radius** | **tacacs**} **enable** [**primary** | **secondary**]}

Syntax Description	
configuration	Sets configuration authentication (authorization).
local	Selects the local database for authentication or authorization.
radius	Selects a RADIUS server for authentication or authorization.
tacacs	Selects TACACS+ server authentication.
enable	Enables the source of authorization information.
primary	(Optional) Sets the first authentication method used.
secondary	(Optional) Sets the second authentication method used.
fail-over	Sets the condition to use the next authentication scheme, when primary authentication fails.
server-unreachable	Specifies that a failover to the secondary authentication scheme should occur only if the primary authentication server is unreachable.
login	Selects the local method for authentication.

Defaults

The local authentication method is enabled by default.

Command Modes

Global configuration

Usage Guidelines

Authentication, also referred to as login, is the act of verifying usernames and passwords. Authorization is the action of determining what a user is allowed to do. It permits or denies privileges for authenticated users in the network. For example, if you log in to an SE with a superuser administrator account (for example, the predefined admin account), you have the highest level of access privileges and can perform any administrative task such as the following:

- Configure the standalone SE.
- Obtain statistical information that the standalone SE has collected.
- Reload the device.

Generally, authentication precedes authorization in a network.

The **authentication** command configures both the authentication and authorization methods that govern login and configuration access to the SE. Login and configuration privileges can be maintained in two different databases in the Internet Streamer CDS 2.4 software: the local database and RADIUS database. If all databases are enabled, then all three databases are queried. If the user data cannot be found in the first database queried, then the second and third databases are queried.

When an administrator can log in to the SE through the console or the SE GUI, the SE checks the specified authentication database to verify the user's username and password to process these administrative login requests and to determine the access rights that this particular administrator should be granted during this login session. When the SE receives an administrative login request, the SE can check its local database or a remote third-party database to verify the username with the password and to determine the access privileges of the administrator.

When defining or modifying the authentication configuration method for an SE, follow these guidelines:

- You can use the **authentication** command to choose between using an external access server or the internal (local) SE-based AAA system for user access management.
- You can configure any combination of these authentication and authorization methods to control access and set privileges on an SE:
 - Local authentication and authorization
 - RADIUS authentication and authorization
- Authentication configuration applies to the following:
 - Console and Telnet connection attempts
 - Secure FTP (SFTP), SSH (SSH Version 1 and Version 2), and Websense server access
- If you configure a RADIUS key on the SE (the RADIUS client), make sure that you configure an identical key on the RADIUS server.
- If you configure multiple RADIUS servers, the first server configured is the primary server, and authentication requests are sent to this server first. You can also specify secondary servers for authentication and authorization purposes.
- By default, the SE uses the local database to authenticate and authorize administrative login requests. The SE verifies whether all authentication databases are disabled and if so, sets the system to the default state. For information on this default state, see the [“Default Administrative Login Authentication and Authorization Configuration”](#) section on page 2-26.

The **authentication login** command determines whether the user has any level of permission to access the SE. The **authentication configuration** command authorizes the user with privileged access (configuration access) to the SE.

The **authentication login local** and the **authentication configuration local** commands use a local database for authentication and authorization.

The **authentication login radius** and **authentication configuration radius** commands use a remote RADIUS server to determine the level of user access.

By default, the local method is enabled, RADIUS both disabled for login and configuration. Whenever RADIUS is disabled, local is automatically enabled. RADIUS and local methods can be enabled at the same time. The **primary** option specifies the first method to attempt for both login and configuration; the **secondary** option specifies the method to use if the primary method fails. If all methods of an **authentication login** or **authentication configuration** commands are configured as primary or secondary, local is attempted first, then RADIUS.

Default Administrative Login Authentication and Authorization Configuration

By default, the SE uses the local database to obtain login authentication and authorization privileges for administrative users.

**Note**

Use the **authentication** global configuration command to configure the authentication methods that govern administrative login and configuration access to the SE.

Table 2-2 lists the default configuration for administrative login authentication and authorization.

Table 2-2 *Default Configuration for Administrative Login Authentication and Authorization*

Feature	Default Value
Administrative login authentication	Enabled
Administrative configuration authorization	Enabled
Authentication server failover because the authentication server is unreachable	Disabled
RADIUS login authentication (console and Telnet)	Disabled
RADIUS authorization (console and Telnet)	Disabled
RADIUS server IP address	None specified
RADIUS server UDP authorization port	Port 1645
RADIUS key	None specified
RADIUS server timeout	5 seconds
RADIUS retransmit attempts	2 times

Enforcing Authentication with the Primary Method

The **authentication fail-over server-unreachable** global configuration command allows you to specify that failover to the secondary authentication method should occur only if the primary authentication server is unreachable. This feature ensures that users gain access to the SE using the local database only when nonlocal authentication servers are unreachable.

Server Redundancy

You can specify authentication servers with the corresponding authentication server (LDAP, or RADIUS) **host** command options to configure additional servers. These additional servers provide authentication redundancy and improved throughput, especially when SE load-balancing schemes distribute the requests evenly between the servers. If the SE cannot connect to any of the authentication servers, no authentication takes place and users who have not been previously authenticated are denied access.

Login Authentication and Authorization Through the Local Database

Local authentication and authorization use locally configured login and passwords to authenticate administrative login attempts. The login and passwords are local to each SE and are not mapped to individual usernames.

By default, local login authentication is enabled first. You can disable local login authentication only after enabling one or more of the other administrative login authentication methods. However, when local login authentication is disabled, if you disable all other administrative login authentication methods, local login authentication is re-enabled automatically.

Specifying RADIUS Authentication and Authorization Settings

RADIUS authentication clients reside on the SE running Cisco Internet Streamer Release 2.4 software. When enabled, these clients send authentication requests to a central (remote) RADIUS server, which contains login authentication and network service access information.

To configure RADIUS authentication on an SE, you must configure a set of RADIUS authentication server settings on the SE. You can use the SE GUI or the CLI to configure this set of RADIUS authentication server settings for an SE.

Table 2-3 describes the RADIUS authentication settings.

Table 2-3 RADIUS Authentication Settings

Setting	Description
RADIUS server	RADIUS servers that the SE is to use for RADIUS authentication. To enable the SE to use a specific RADIUS server, enter the IP address or hostname of the RADIUS server and port information. Up to five different hosts are allowed. Early deployment of RADIUS was done using port number 1645, although the official port number for RADIUS is now 1812. Up to five different ports are allowed.
RADIUS key	Key used to encrypt and authenticate all communication between the RADIUS client (the SE) and the RADIUS server. The maximum number of characters in the key is 15. There is no default. Tip Make sure that the same RADIUS key is enabled on the RADIUS server.
RADIUS timeout interval	Number of seconds that the SE waits for a response from the specified RADIUS authentication server before declaring a timeout. The range is 1 to 20 seconds. The default value is 5 seconds.
RADIUS retransmit count	Number of times that the SE is to retransmit its connection to the RADIUS if the RADIUS timeout interval is exceeded. The range is one to three tries. The default value is two tries.

After configuring these RADIUS authentication settings on the SE, you can enable RADIUS login authentication and authorization on the SE.

Examples

The following example shows the output of the **show authentication user** command:

```
ServiceEngine#show authentication user
Login Authentication: Console/Telnet/Ftp/SSH Session
-----
local disabled
Radius disabled
Tacacs+ disabled

Configuration Authentication: Console/Telnet/Ftp/SSH Session
-----
local disabled
Radius disabled
Tacacs+ disabled
```

The following example shows the output of the **show statistics authentication** command:

```
ServiceEngine#show statistics authentication
Authentication Statistics
-----
Number of access requests: 37
Number of access deny responses: 14
Number of access allow responses: 23
```

Related Commands

radius-server
show authentication
show statistics authentication
username

authsvr

To enable and configure the Authorization server, use the **authsvr** global configuration command. To disable the Authorization server, use the **no** form of this command.

authsvr {enable | unknown-server allow}

no authsvr {enable | unknown-server allow}

Syntax Description	enable	Enables the Authorization server.
	unknown-server	Configures the Authorization server unknown server or domain.
	allow	Allows requests for an unknown server or domain.

Defaults	authsvr: enabled unknown-server: blocked

Command Modes	Global configuration

Examples	The following example shows how to enable the Authorization server: <pre>ServiceEngine(config)#authsvr enable Authserver is enabled</pre>

Related Commands	debug authsvr trace debug authsvr error debug authsvr show statistics authsvr

bandwidth (global configuration)

To set an allowable bandwidth usage limit and its duration for Cisco Streaming Engine WMT streaming media, use the **bandwidth** global configuration command. To remove individual options, use the **no** form of this command.

```
bandwidth {movie-streamer {incoming bandwidth | outgoing bandwidth {default |  
    max-bandwidth start-time day hour end-time day hour}} | wmt {incoming bandwidth |  
    outgoing bandwidth}}
```

```
no bandwidth {movie-streamer {incoming bandwidth | outgoing bandwidth {default |  
    max-bandwidth start-time day hour end-time day hour}} | wmt {incoming bandwidth |  
    outgoing bandwidth}}
```

Syntax Description

movie-streamer	Configures the maximum pacing bit rate in kilobits per second (kbps) for the Movie Streamer.
incoming	Configures the duration of allowable incoming bandwidth settings for WMT.
<i>bandwidth</i>	Bandwidth size for the Movie Streamer in kilobits per second (kbps) (0–2147483647).
outgoing	Configures the duration of allowable outgoing bandwidth settings for WMT.
default	Specifies the default value for bandwidth if the scheduled bandwidth is not configured.
max-bandwidth	Specifies the maximum value of bandwidth in Kbps.
start-time	Specifies the start time for this bandwidth setting.
<i>day</i>	Day of the week.
<i>hour</i>	Time to start (hh:mm) (0–23:0–59)
end-time	Specifies the end time for this bandwidth setting.
wmt	Configures the duration of allowable bandwidth settings for WMT. For more information, see the “Configuring Incoming and Outgoing WMT Bandwidth” section on page 2-32.

Defaults

No default behavior or values.

Command Modes

Global configuration

Usage Guidelines

With the various types of traffic originating from a device, every type of traffic, such as streaming media, HTTP, and metadata, consumes network resources. Use the **bandwidth** command to limit the amount of network bandwidth used by the WMT streaming media.

The content services bandwidth includes the bandwidth allocation for WMT. WMT bandwidth settings apply to WMT streaming of live, cached, and pre-positioned content.

For each type of bandwidth, you can specify the amount of bandwidth to be used for a particular time period. This type is called *scheduled bandwidth*. The *default bandwidth* is the amount of bandwidth associated with each content service type when there is no scheduled bandwidth. In centrally managed deployments (the SEs are registered with a CDSM), if an SE is assigned to a device group and no default bandwidth has been configured for the SE itself, the device group default bandwidth settings are applied. However, if the default bandwidth has been configured for the SE, then that setting overrides the device group settings. If the SE is a member of multiple device groups, the most recently updated default bandwidth settings are applied.

The *maximum bandwidth* specifies the upper limit for the allowable bandwidth. The total bandwidth configured for all content services must not exceed the bandwidth limits specified for any SE platform model in the Internet Streamer CDS network. In addition, the license keys configured for WMT further restrict the maximum bandwidth available for each SE model.

Configuring Incoming and Outgoing WMT Bandwidth

The bandwidth between the WMT proxy server (the SE) and the WMT client is called the WMT outgoing bandwidth.

The bandwidth between the WMT proxy and the origin streaming server is called the incoming bandwidth. Because the bandwidth from the edge to the outside IP WAN is limited, you must specify a per session limit (the maximum bit rate per request) for each service that is running on the SE and that consumes the incoming bandwidth (for example, the WMT streaming service), and an aggregate limit (the maximum incoming bandwidth.) You need to control the outgoing bandwidth based on the WMT license that is configured on the SE.

The **bandwidth wmt outgoing** and **bandwidth incoming** global configuration commands enable you to specify a WMT incoming and an outgoing bandwidth as follows:

- Use the **bandwidth wmt outgoing** *kbits* global configuration command to specify the outgoing WMT bandwidth in kbps. This command sets the maximum bandwidth for the WMT content that can be delivered to a client that is requesting WMT content. The range of values is between 0–2,147,483,647 kilobits per second (kbps).

If the specified outgoing bandwidth is above the limit specified by the WMT license, then a warning message displays. However, the specified outgoing bandwidth setting is applied to the SE because the outgoing bandwidth may be configured before the WMT licenses are enabled or an enabled WMT license could be changed to a higher value at a later time.

- Use the **bandwidth wmt incoming** *kbits* global configuration command to specify the incoming WMT bandwidth in kbps. This command sets the maximum bandwidth for the WMT content that can be delivered to an SE from the origin streaming server or another SE in the case of a cache miss. The specified bit rate is the maximum incoming WMT per session bit rate. The range of values is between 0–2,147,483,647 kbps. The incoming bandwidth applies to VoD content from the origin server for a cache miss.

Related Commands

- bandwidth** (interface configuration)
- interface**
- show bandwidth**
- show interface**
- show running-config**
- show startup-config**
- show statistics bandwidth**

bandwidth (interface configuration)

To configure an interface bandwidth, use the **bandwidth** interface configuration command. To restore default values, use the **no** form of this command.

bandwidth {10 | 100 | 1000}

no bandwidth {10 | 100 | 1000}

Syntax Description	10	Sets the bandwidth to 10 megabits per second (Mbps).
	100	Sets the bandwidth to 100 Mbps.
	1000	Sets the bandwidth to 1000 Mbps. This option is not available on all ports.

Defaults No default behavior or values.

Command Modes Interface configuration

Usage Guidelines To configure an interface bandwidth on an SE, use the **bandwidth** interface configuration command. The bandwidth is specified in megabits per second (Mbps). The **1000** Mbps option is not available on all ports. On a Service Engine model that has an optical Gigabit Ethernet interface, you cannot change the of this interface. Therefore, Gigabit Ethernet interfaces only run at 1000 Mbps. For newer models of the SE that have a Gigabit Ethernet interface over copper, this restriction does not apply; you can configure these Gigabit Ethernet interfaces to run at 10, 100, or 1000 Mbps.

You can configure the Gigabit Ethernet interface settings (bandwidth, and duplex settings) if the Gigabit-over-copper-interface is up or down. If the interface is up, it will apply the specific interface settings. If the interface is down, the specified settings are stored and then applied when the interface is brought up. For example, you can specify any of the following commands for a Gigabit-over-copper-interface, which is currently down, and have these settings automatically applied when the interface is brought up:

```
ServiceEngine(config-if)# bandwidth 10
ServiceEngine(config-if)# bandwidth 100
ServiceEngine(config-if)# bandwidth 1000
```

You cannot configure the Gigabit Ethernet interface settings on an optical Gigabit Ethernet interface.

Examples The following example shows how to set an interface bandwidth to 10 Mbps:

```
ServiceEngine(config-if)#bandwidth 10
```

The following example shows how to restore default bandwidth values on an interface:

```
ServiceEngine(config-if)#no bandwidth
```

Related Commands **interface**

banner

To configure the EXEC, login, and message-of-the-day (MOTD) banners, use the **banner** global configuration command. To disable the banner feature, use the **no** form of this command.

```
banner {enable | exec {message line | message_text} | login {message line | message_text} | motd
{message line | message_text}}
```

```
no banner {enable | exec [message] | login [message] | motd [message]}
```

Syntax Description

enable	Enables banner support on the SE.
exec	Configures an EXEC banner.
message	Specifies a message to be displayed when an EXEC process is created.
<i>line</i>	EXEC message text on a single line. The SE translates the \n portion of the message to a new line when the EXEC banner is displayed to the user.
<i>message_text</i>	EXEC message text on one or more lines. Press the Return key or enter delimiting characters (\n) to specify an EXEC message to appear on a new line. Supports up to a maximum of 980 characters, including new-line characters (\n). Enter a period (.) at the beginning of a new line to save the message and return to the prompt for the global configuration mode. Note The EXEC banner content is obtained from the command line input that the user enters after being prompted for the input.
login	Configures a login banner.
message	Specifies a message to be displayed before the username and password login prompts.
<i>line</i>	Login message text on a single line. The SE translates the \n portion of the message to a new line when the login banner is displayed to the user.
<i>message_text</i>	Login message text on one or more lines. Press the Return key or enter delimiting characters (\n) to specify a login message to appear on a new line. Supports up to a maximum of 980 characters, including new-line characters (\n). Enter a period (.) at the beginning of a new-line to save the message and return to the prompt for the global configuration mode. Note The login banner content is obtained from the command line input that the user enters after being prompted for the input.
motd	Configures an MOTD banner.
message	Specifies an MOTD message.
<i>line</i>	MOTD message text on a single line. The SE translates the \n portion of the message to a new line when the MOTD banner is displayed to the user.
<i>message_text</i>	MOTD message text on one or more lines. Press the Return key or enter delimiting characters (\n) to specify an MOTD message to appear on a new line. Supports up to a maximum of 980 characters, including new-line characters (\n). Enter a period (.) at the beginning of a new line to save the message and return to the prompt for the global configuration mode. Note The MOTD banner content is obtained from the command line input that the user enters after being prompted for the input.

Defaults

Banner support is disabled by default

Command Modes

Global configuration

Usage Guidelines

You can configure the following three types of banners in any Internet Streamer CDS software device mode:

- The MOTD banner sets the message of the day. This message is the first message that is displayed when a login is attempted.
- The login banner is displayed after the MOTD banner but before the actual login prompt appears.
- The EXEC banner is displayed after the EXEC CLI shell has started.

**Note**

All of these banners are effective on a console, Telnet, or a Secure Shell (SSH) version 2 session.

After you configure the banners, enter the **banner enable** global configuration command to enable banner support on the SE. Enter the **show banner** EXEC command to display information about the configured banners.

**Note**

When you run an SSH version 1 client and log in to the SE, the MOTD and login banners are not displayed. You need to use SSH version 2 to display the banners when you log in to the SE.

Examples

The following example shows how to enable banner support on the SE:

```
ServiceEngine(config)# banner enable
```

The following example shows how to use the **banner motd message** global configuration command to configure the MOTD banner. In this example, the MOTD message consists of a single line of text.

```
ServiceEngine(config)# banner motd message This is an Internet Streamer CDS 2.3 device
```

The following example shows how to use the **banner motd message** global command to configure a MOTD message that is longer than a single line. In this case, the SE translates the \n portion of the message to a new line when the MOTD message is displayed to the user.

```
ServiceEngine(config)# banner motd message "This is the motd message.
\nThis is an Internet Streamer CDS 2.3 device\n"
```

The following example shows how to use the **banner login message** global configuration command to configure a MOTD message that is longer than a single line. In this case, SE A translates the \n portion of the message to a new line in the login message that is displayed to the user.

```
ServiceEngine(config)# banner login message "This is login banner.
\nUse your password to login\n"
```

The following example shows how to use the **banner exec** global configuration command to configure an interactive banner. The **banner exec** command is similar to the **banner motd message** commands except that for the **banner exec** command, the banner content is obtained from the command line input that the user enters after being prompted for the input.

```
ServiceEngine(config)# banner exec
```

```
Please type your MOTD messages below and end it with '.' at beginning of line:
(plain text only, no longer than 980 bytes including newline)
This is the EXEC banner.\nUse your Internet Streamer CDS username and password to log in
to this SE.\n
.
Message has 99 characters.
ServiceEngine(config)#
```

Assume that an SE has been configured with the MOTD, login, and EXEC banners as shown in the previous examples. When a user uses an SSH session to log in to the SE, the user will see a login session that includes a MOTD banner and a login banner that asks the user to enter a login password as follows:

```
This is the motd banner.
This is an Internet Streamer CDS 2.3 device
This is login banner.
Use your password to login.
```

```
Cisco SE
```

```
admin@ce's password:
```

After the user enters a valid login password, the EXEC banner is displayed, and the user is asked to enter the Internet Streamer CDS username and password as follows:

```
Last login: Fri Oct 1 14:54:03 2004 from client
System Initialization Finished.
This is the EXEC banner.
Use your Internet Streamer CDS username and password to log in to this SE.
```

After the user enters a valid Internet Streamer CDS username and password, the SE CLI is displayed. The CLI prompt varies depending on the privilege level of the login account. In the following example, because the user entered a username and password that had administrative privileges (privilege level of 15), the EXEC mode CLI prompt is displayed:

```
ServiceEngine#
```

Related Commands

show banner

bitrate

To configure the maximum pacing bit rate for large files for the Movie Streamer and to separately configure WMT bit-rate settings, use the **bitrate** global configuration command. To remove the bit-rate settings, use the **no** form of this command.

bitrate {**movie-streamer** *bitrate* | **wmt** {**incoming** *bitrate* | **outgoing** *bitrate*}}

no bitrate {**movie-streamer** *bitrate* | **wmt** {**incoming** | **outgoing**}}

Syntax Description

movie-streamer	Configures the maximum pacing bit rate in kilobits per second (kbps) for the Movie Streamer.
<i>bitrate</i>	Bit rate in kbps (1–2147483647).
wmt	Configures the bit rate, in kbps, for large files sent using the WMT protocol.
incoming	Sets the incoming bit-rate settings.
<i>bitrate</i>	Incoming bit rate in kbps (0–2147483647).
outgoing	Sets the outgoing bit-rate settings.
<i>bitrate</i>	Outgoing bit rate in kbps (0–2147483647).

Defaults

movie-streamer *bitrate*: 1500 kbps

wmt incoming *bitrate*: 0 (no limit)

wmt outgoing *bitrate*: 0 (no limit)

Command Modes

Global configuration

Usage Guidelines

The Internet Streamer CDS 2.x software includes the Windows Media Technologies (WMT) proxy, which has the ability to cache on-demand media files when the user requests these files for the first time. All subsequent requests for the same file are served by the WMT proxy using the RTSP protocol. The WMT proxy can also live-split a broadcast, which causes only a single unicast stream to be requested from the origin server in response to multiple client requests for the stream.

The bit rate between the proxy and the origin server is called the incoming bit rate. Use the **bitrate** command to limit the maximum bit rate per session for large files. The **bitrate wmt incoming** and **bitrate wmt outgoing** global configuration commands enable you to specify a WMT incoming and outgoing WMT per session bit rate as follows:

- Use the **bitrate wmt incoming** *bitrate* global configuration command to specify the maximum incoming streaming bit rate per session that can be delivered to the WMT proxy server (an SE) from the origin streaming server or another SE in the case of a cache miss. The specified bit rate is the maximum incoming WMT per session bit rate. The range of values is between 0–2,147,483,647 kbps. The default value is 0 (no bit-rate limit).

- Use the **bitrate wmt outgoing** *bitrate* global configuration command to set the maximum outgoing streaming bit rate per session that can be delivered to a client that is requesting WMT content. The specified bit rate is the maximum outgoing WMT per session bit rate. The range of values is between 0–2,147,483,647 kbps. The default value is 0 (no bit-rate limit). The outgoing bandwidth applies to VoD content from the WMT proxy server on the SE in the case of a cache miss.

**Note**

The aggregate bandwidth used by all concurrent users is still limited by the default device bandwidth or by the limit configured using the **bandwidth** global configuration command.

Variable WMT Bit Rates

A content provider can create streaming media files at different bit rates to ensure that different clients who have different connections—for example, modem, DSL, or LAN—can choose a particular bit rate. The WMT caching proxy can cache multiple bit-rate files or variable bit-rate (VBR) files, and based on the bit rate specified by the client, it serves the appropriate stream. Another advantage of creating variable bit-rate files is that you only need to specify a single URL for the delivery of streaming media.

**Note**

In the case of multiple bit-rate files, the SE that is acting as the WMT proxy server only retrieves the bit rate that the client has requested.

Examples

The following example shows how to configure an incoming bit rate for the Movie Streamer:

```
ServiceEngine(config)#bitrate movie-streamer incoming 100
```

The following example shows how to configure an incoming bit rate for a file sent using WMT. Use the **show wmt** command to verify that the incoming bit rate has been modified.

```
ServiceEngine(config)#bitrate wmt incoming 300000
ServiceEngine(config)#exit
ServiceEngine#show wmt
----- WMT Server Configurations -----
WMT is enabled
WMT disallowed client protocols: none
WMT bandwidth platform limit: 1000000 Kbits/sec
WMT outgoing bandwidth configured is 500000 Kbits/sec
WMT incoming bandwidth configured is 500000 Kbits/sec
WMT max sessions configured: 14000
WMT max sessions platform limit: 14000
WMT max sessions enforced: 14000 sessions
WMT max outgoing bit rate allowed per stream has no limit
WMT max incoming bit rate allowed per stream has no limit
WMT cache is enabled
WMT cache max-obj-size: 25600 MB
WMT cache revalidate for each request is not enabled
WMT cache age-multiplier: 30%
WMT cache min-ttl: 60 minutes
WMT cache max-ttl: 1 days
WMT debug client ip not set
WMT debug server ip not set
WMT accelerate live-split is enabled
WMT accelerate proxy-cache is enabled
WMT accelerate VOD is enabled
WMT fast-start is enabled
WMT fast-start max. bandwidth per player is 3500 (Kbps)
WMT fast-cache is enabled
WMT fast-cache acceleration factor is 5
```

```

WMT maximum data packet MTU (TCP) enforced is 1472 bytes
WMT maximum data packet MTU (UDP) is 1500 bytes
WMT client idle timeout is 60 seconds
WMT forward logs is enabled
WMT server inactivity-timeout is 65535
WMT Transaction Log format is Windows Media Services 4.1 logging
RTSP Gateway incoming port 554

```

```

----- WMT HTTP Configurations -----
WMT http extensions allowed:
asf none nsc wma wmv nsclog

```

```

----- WMT Proxy Configurations -----
Outgoing Proxy-Mode:
-----
MMS-over-HTTP Proxy-Mode:
is not configured.
RTSP Proxy-Mode:
is not configured. ServiceEngine#

```

Related Commands **show wmt**

cache

To restrict the maximum number of contents in the CDS, use the **cache** global configuration command.

cache content max-cached-entries *num*

Syntax Description

content	Browses the cdnfs directories and files.
max-cached-entries	Cleans up the unwanted entries in the cdnfs.
<i>num</i>	Max cached entries (1–10000000).

Defaults

The max-cached-entries default is 3000000 entries.

Command Modes

Global configuration

Usage Guidelines

The **cache** command configures the cached content maximum entries. The CDS, by default, allows a maximum of three million cached entries, regardless of the amount of space available in the cdnfs.

Examples

The following example shows how to configure the cache content:

```
ServiceEngine#cache content max-cached-entries 1000
```

Related Commands

show cache

capability

To modify the capability configuration, use the **capability** global configuration command. To disable capability, use the **no** form of this command.

capability config profile *number* [**add attrib** {**capability-url** *url* | **user-agent** *name*} | **description**]

no capability config

Syntax Description

config	Enters the capability exchange submode.
profile	Populates the profile database.
<i>number</i>	The profile ID (1–65535).
add	(Optional) Adds the capability attributes.
attrib	Adds the capability attributes.
capability-url	Specifies the capability URL.
<i>url</i>	The capability URL string.
user-agent	Specifies the user-agent.
<i>name</i>	The user-agent name.
description	(Optional) Specifies the profile description.

Defaults

No default behavior or values.

Command Modes

Global configuration

Related Commands

show capability

cd

To change from one directory to another directory, use the **cd** EXEC command.

cd *directoryname*

Syntax Description	<i>directoryname</i> Directory name.
Defaults	No default behavior or values.
Command Modes	EXEC
Usage Guidelines	Use this command to maneuver between directories and for file management. The directory name becomes the default prefix for all relative paths. Relative paths do not begin with a slash (/). Absolute paths begin with a slash (/).
Examples	The following example shows how to use a relative path: <pre>ServiceEngine(config)#cd local1</pre> The following example shows how to use an absolute path: <pre>ServiceEngine(config)#cd /local1</pre>
Related Commands	deltree dir lls ls mkdir pwd

cdnfs

To manage the Internet Streamer CDS network file system (cdnfs), use the **cdnfs** EXEC command.

cdnfs {browse | cleanup {info | start {force} | stop}}

Syntax Description

browse	Browses the cdnfs directories and files.
cleanup	Cleans up the unwanted entries in the cdnfs.
info	Summarizes the information about unwanted entries without starting the cleanup process.
start	Starts the cleanup of unwanted entries in the cdnfs.
force	Removes objects that are in transient states.
stop	Stops the cleanup of unwanted entries in the cdnfs.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

The Internet Streamer CDS network file systems (cdnfs) stores the pre-positioned Internet Streamer CDS network content to be delivered by all supported protocols. You can configure the cdnfs size of each SE using the **disk configure** command.

The **cdnfs cleanup** command cleans up the content of deleted channels from the acquisition and distribution database. In certain cases, the acquirer is not notified by the Centralized Management System (CMS) about deleted channels, and it fails to clear all unified name space (UNS) content. In such cases, the **cdnfs cleanup** EXEC command can be used to clean up all UNS content associated with deleted channels.



Note

You can use the **cdnfs cleanup start** to clean up the orphan content. The orphan content is content that is not associated with any channel to which an SE is subscribed.

The **cdnfs browse** command is an interactive command and has the following subcommands used to view Internet Streamer CDS network files and directories:

```
ServiceEngine#cdnfs browse

----- CDNFS interactive browsing -----
dir, ls:  list directory contents
cd, chdir: change current working directory
info:    display attributes of a file
more:    page through a file
cat:     display a file
exit,quit: quit CDNFS browse shell

/>dir
                               www.gidtest.com/
/>cd www.gidtest.com
```

```

/www.gidtest.com/>dir
764 Bytes          index.html
/www.gidtest.com/>info index.html

CDNFS File Attributes:
  Status              3   (Ready)
  File Size           764 Bytes
  Start Time          null
  End Time            null
  Last-modified Time   Sun Sep  9 01:46:40 2001

Internal path to data file:
/disk06-00/d/www.gidtest.com/05/05d201b7ca6fdd41d491eaec7cfc6f14.0.data.html
  note: data file actual last-modified time: Tue Feb 15 00:47:35 2005

/www.gidtest.com/>

```

Because the **cdnfs** is empty in this example, the **ls** command does not show any results. Typically, if the **cdnfs** contained information, it would list the websites as directories, and file attributes and content could be viewed using these subcommands.

The **cdnfs cleanup** command synchronizes the state of the acquisition and distribution database with the content stored on the **cdnfs**. You should use this command after replacing a failed disk drive.

Examples

The following example shows the output of the **cdnfs cleanup info** command:

```

ServiceEngine#cdnfs cleanup info
Gathering cleanup information. This may take some time....
(Use Ctrl+C or 'cdnfs cleanup stop' to interrupt)
.....

Summary of garbage resource entries found
-----
Number of entries      : 605
Size of entries (KB)   : 60820911

```

Related Commands

show cdnfs
show statistics cdnfs

cdsm

To configure the Content Delivery System (CDSM) IP address to be used for the SEs or SRs, or to configure the role and GUI parameters on a CDSM device, use the **cdsm** global configuration command. To negate these actions, use the **no** form of this command.

cdsm {**ip** {*hostname* | *ip-address* | **role** {**primary** | **standby**} | **ui port** *port-num*}}

no cdsm {**ip** | **role** {**primary** | **standby**} | **ui port**}

Syntax Description

ip	Configures the CDSM hostname or IP address.
<i>hostname</i>	Hostname of the CDSM.
<i>ip-address</i>	IP address of the CDSM.
role	Configures the CDSM role to either primary or standby (available from the CDSM CLI only).
primary	Configures the CDSM to be the primary CDSM.
standby	Configures the CDSM to be the standby CDSM.
ui	Configures the CDSM GUI port address (available from the CDSM CLI only).
port	Configures the CDSM GUI port.
<i>port-num</i>	Port number (1–65535).

Defaults

No default behavior or values.

Command Modes

Global configuration

Usage Guidelines

You can use the **cdsm ui port** global configuration command to change the CDSM GUI port from the standard number 8443 as follows:

```
CDSM(config)#cdsm ui port 35535
```



Note

The **role** and **ui** options are available on CDSM devices only. Changing the CDSM GUI port number automatically restarts the Centralized Management System (CMS) service if this has been enabled.

The **cdsm ip** command associates the device with the CDSM so that the device can be approved as a part of the network.

After the device is configured with the CDSM IP address, it presents a self-signed security certificate and other essential information, such as its IP address or hostname, disk space allocation, and so forth, to the CDSM.

Configuring Devices Inside a NAT

In an Internet Streamer CDS network, there are two methods for a device registered with the CDSM (SEs, SRs, or standby CDSM) to obtain configuration information from the primary CDSM. The primary method is for the device to periodically poll the primary CDSM on port 443 to request a configuration update. You cannot configure this port number. The backup method is when the CDSM pushes configuration updates to a registered device as soon as possible by issuing a notification to the registered device on port 443. This method allows changes to take effect in a timelier manner. You cannot configure this port number even when the backup method is being used. Internet Streamer CDS networks do not work reliably if devices registered with the CDSM are unable to poll the CDSM for configuration updates. Similarly, when a receiver SE requests content and content metadata from a forwarder SE, it contacts the forwarder SE on port 443.

All the above methods become complex in the presence of Network Address Translation (NAT) firewalls. When a device (SEs at the edge of the network, SRs, and primary or standby CDSMs) is inside a NAT firewall, those devices that are inside the same NAT use one IP address (the inside local IP address) to access the device and those devices that are outside the NAT use a different IP address (the inside global IP address) to access the device. A centrally managed device advertises only its inside local IP address to the CDSM. All other devices inside the NAT use the inside local IP address to contact the centrally managed device that resides inside the NAT. A device that is not inside the same NAT as the centrally managed device is not able to contact it without special configuration.

If the primary CDSM is inside a NAT, you can allow a device outside the NAT to poll it for getUpdate requests by configuring a *static translation* (inside global IP address) for the CDSM's inside local IP address on its NAT, and using this address, rather than the CDSM's inside local IP address, in the **cdsm ip ip-address** global configuration command when you register the device to the CDSM. If an SE or SR is inside a NAT and the CDSM is outside the NAT, you can allow the SE or SR to poll for getUpdate requests by configuring a static translation (inside global IP address) for the SE or SR's inside local address on its NAT and specifying this address in the Use IP Address field under the NAT Configuration heading in the Device Activation window.

**Note**

Static translation establishes a one-to-one mapping between your inside local address and an inside global address. Static translation is useful when a host on the inside must be accessible by a fixed address from the outside.

Standby CDSMs

The Cisco Internet Streamer CDS software implements a standby CDSM. This process allows you to maintain a copy of the Internet Streamer CDS network configuration. If the primary CDSM fails, the standby can be used to replace the primary.

For interoperability, when a standby CDSM is used, it must be at the same software version as the primary CDSM in order to maintain the full CDSM configuration. Otherwise, the standby CDSM detects this status and does not process any configuration updates that it receives from the primary CDSM until the problem is corrected.

**Note**

We recommend that you upgrade your standby CDSM first and then upgrade your primary CDSM. We also recommend that you create a database backup on your primary CDSM and copy the database backup file to a safe place before you upgrade the software.

Switching a CDSM from Warm Standby to Primary

If your primary CDSM becomes inoperable for some reason, you can manually reconfigure one of your warm standby CDSMs to be the primary CDSM. Configure the new role by using the global configuration **cdsm role primary** command as follows:

```
ServiceEngine#configure
ServiceEngine(config)#cdsm role primary
```

This command changes the role from standby to primary and restarts the management service to recognize the change.



Note

Check the status of recent updates from the primary CDSM. Use the **show cms info** EXEC command and check the time of the last update. To be current, the update time should be between 1 and 5 minutes old. You are verifying that the standby CDSM has fully replicated the primary CDSM configuration. If the update time is not current, check whether there is a connectivity problem or if the primary CDSM is down. Fix the problem, if necessary, and wait until the configuration has replicated as indicated by the time of the last update. Make sure that both CDSMs have the same Coordinated Universal Time (UTC) configured.

If you switch a warm standby CDSM to primary while your primary CDSM is still online and active, both CDSMs detect each other, automatically shut themselves down, and disable management services. The CDSMs are switched to halted, which is automatically saved in flash memory.

Examples

The following example configures an IP address and a primary role for a CDSM:

```
CDSM(config)#cdsm ip 10.1.1.1
CDSM(config)#cdsm role primary
```

The following example configures a new GUI port to access the CDSM GUI:

```
CDSM(config)#cdsm ui port 8550
```

The following example configures the CDSM as the standby CDSM:

```
CDSM(config)#cdsm role standby
Switching CDSM to standby will cause all configuration settings made on this CDSM
to be lost.
Please confirm you want to continue [no]?yes
Restarting CMS services
```

The following example configures the standby CDSM with the IP address of the primary CDSM by using the **cdsm ip ip-address** global configuration command. This command associates the device with the primary CDSM so that it can be approved as a part of the network.

```
CDSM# cdsm ip 10.1.1.1
```


clear

To clear the HTTP object cache, the hardware interface, statistics, archive working transaction logs, and other settings, use the **clear** EXEC command.

On the SE:

```
clear cache [all | content 1-1000000 | flash-media-streaming]
```

```
clear content url url
```

```
clear ip access-list counters [acl-num | acl-name]
```

```
clear logging
```

```
clear statistics {access-lists 300 | all | authentication | authsvr | distribution {all |  
    metadata-receiver | metadata-sender | unicast-data-receiver | unicast-data-sender} |  
    flash-media-streaming | history | http {all | ims | object | pcmm | performance | requests |  
    rule} | icap | icmp | ip | movie-streamer | qos policy-service | radius | rule {action action-type  
    | all | pattern {1-512 | all} | rtsp} | running | snmp | tacacs | tcp | transaction-logs | udp | wmt}
```

```
clear transaction-log
```

```
clear users administrative
```

```
clear wmt stream-id 1-999999
```

On the SR:

```
clear ip access-list counters [acl-num | acl-name]
```

```
clear logging
```

```
clear statistics {all | authentication | history | http {all | ims | object | pcmm | performance |  
    requests | rule} | icmp | ip | radius | running | service-router | snmp | tacacs | tcp | udp}
```

```
clear users administrative
```

On the CDSM:

```
clear ip access-list counters [acl-num | acl-name]
```

```
clear logging
```

```
clear statistics {all | authentication | distribution {all | metadata-receiver | metadata-sender |  
    unicast-data-receiver | unicast-data-sender} | history | icmp | ip | radius | running | snmp |  
    tacacs | tcp | udp}
```

```
clear users administrative
```

Syntax Description

cache	Clears the HTTP objects from the cache.
all	(Optional) Clears all cached objects.
content	(Optional) Clears cached content.

<i>1-1000000</i>	Free space in MBs.
flash-media-streaming	Clears the Flash Media Streaming edge server cached content and DVR cached content.
content	Clears all cached content.
url	Clears cached content with its original URL.
<i>url</i>	The URL for the content object to delete.
ip access-list	Clears the IP access list statistical information.
counters	Clears the IP access list counters.
<i>acl-name</i>	(Optional) Counters for the specified access list, identified using an alphanumeric identifier up to 30 characters, beginning with a letter.
<i>acl-num</i>	(Optional) Counters for the specified access list, identified using a numeric identifier (standard access list: 1–99; extended access list: 100–199).
logging	Clears the syslog messages saved in the disk file.
statistics	Clears the statistics as specified.
access-lists	Clears the access control list statistics.
300	Clears the group name-based access control list.
all	Clears all statistics.
authentication	Clears the authentication statistics.
authsvr	Clears the Authorization Server statistics.
distribution	Clears the distribution statistics.
all	Clears the distribution statistics for every component.
metadata-receiver	Clears the distribution statistics for the metadata receiver.
metadata-sender	Clears the distribution statistics for the metadata sender.
unicast-data-receiver	Clears the distribution statistics for the unicast data receiver.
unicast-data-sender	Clears the distribution statistics for the unicast data sender.
flash-media-streaming	Clears the Flash Media Streaming statistics.
history	Clears the statistics history.
http	Clears the cache containing HTTP and FTP objects.
all	(Optional) Clears all HTTP statistics.
ims	(Optional) Clears the HTTP if-modified-since (IMS) statistics.
object	(Optional) Clears the HTTP object statistics.
pcmm	(Optional) Clears the HTTP PCMM statistics.
performance	(Optional) Clears the HTTP performance statistics.
requests	(Optional) Clears the nontunneled HTTPS request statistics.
rule	(Optional) Clears the HTTP rule statistics.
icap	Clears the ICAP statistics.
icmp	Clears the ICMP statistics.
ip	Clears the IP statistics.
movie-streamer	Clears the Movie Streamer statistics.
qos	Clears the QoS statistics.
policy-service	Specifies the Camiant cdn-am service.

radius	Clears the RADIUS statistics.
rule	Clears the rules statistics.
action	Clears the statistics of all the rules with the same action.
<i>action-type</i>	Specifies one of the following actions: allow append-username-header block cache-non-cacheable cache-only dscp client cache-hit dscp client cache-miss dscp server freshness-factor insert-no-cache no-auth no-cache no-persistent-connection no-proxy no-url-filtering redirect redirect-url-for-cdn refresh reset rewrite use-icap-service use-proxy use-proxy failover use-server use-xforward-clt-ip
all	Clears the statistics of all the rules.
pattern	Clears the statistics of the pattern lists.
1-512	Pattern list number.
all	Clears the statistics for all the pattern lists.
rtsp	Clears the statistics for the configured RTSP rules (rules configured for RTSP requests from RealMedia players [the RTSP rules] and rules configured for RTSP requests from Windows Media 9 players [the WMT-RTSP rules]).
running	Clears the running statistics.
snmp	Clears the SNMP statistics.
tacacs	Clears the TACACS+ statistics.
tcp	Clears the TCP statistics.
transaction-logs	Clears the transaction log export statistics.
udp	Clears the UDP statistics.
wmt	Clears all WMT statistics.
transaction-log	Archives the working transaction log files.
users	Clears the connections (login) of authenticated users.

administrative	Clears the connections of administrative users authenticated through a remote login service.
wmt	Clears the WMT streams.
stream-id	Clears the WMT streams that have the specified WMT stream ID. Also stops the SE's WMT process that is associated with the specified stream ID.
<i>1-999999</i>	WMT stream ID to clear.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

The **clear cache** command removes all cached contents from the currently mounted cache volumes. Objects being read or written are removed when they stop being busy. The equivalent to this command is the **cache clear** command.

**Caution**

This command is irreversible, and all cached content will be erased.

The **clear cache force** command deletes all objects, whether busy or not, and may generate broken GIF or HTML messages for objects that were being read from the disk when the command was executed.

The **clear logging** command removes all current entries from the syslog.txt file, but does not make an archive of the file. It puts a "Syslog cleared" message in the syslog.txt file to indicate that the syslog has been cleared, as shown in the following example:

```
Feb 14 12:17:18 ServiceEngine#exec_clear_logging:Syslog cleared
```

The **clear statistics** command clears all statistical counters from the parameters given. Use this command to monitor fresh statistical data for some or all features without losing cached objects or configurations.

The **clear transaction-log** command causes the transaction log to be archived immediately to the SE hard disk. This command has the same effect as the **transaction-log force archive** command.

The **clear users administrative** command clears the connections for all administrative users who are authenticated through a remote login service, such as TACACS. This command does not affect an administrative user who is authenticated through the local database.

Examples

The following example shows that the **clear transaction-log** option forces the working transaction log file to be archived:

```
ServiceEngine#clear transaction-log
```

Related Commands

cache clear
show interface
show statistics

clock (EXEC)

To set or clear clock functions or update the calendar, use the **clock** EXEC command.

clock { **read-calendar** | **set** *time day month year* | **update-calendar** }

Syntax Description	read-calendar	Reads the calendar and updates the system clock.
	set	Sets the time and date.
	<i>time</i>	Current time in hh:mm:ss format (hh: 00–23; mm: 00–59; ss: 00–59).
	<i>day</i>	Day of the month (1–31).
	<i>month</i>	Month of the year (January, February, March, April, May, June, July, August, September, October, November, December).
	<i>year</i>	Year (1993–2035).
	update-calendar	Updates the calendar with the system clock.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines If you have an outside source on your network that provides time services (such as a Network Time Protocol [NTP] server), you do not need to set the system clock manually. When setting the clock, enter the local time. The SE calculates the Coordinated Universal Time (UTC) based on the time zone set by the **clock timezone** global configuration command.



Note

We strongly recommend that you configure the SE for the Network Time Protocol (NTP) by using the **ntp** global configuration command. See the [“ntp” section on page -157](#) for more details.

Two clocks exist in the system: the software clock and the hardware clock. The software uses the software clock. The hardware clock is used only at startup to initialize the software clock. The calendar clock is the same as the hardware clock that runs continuously on the system, even if the system is powered off or rebooted. This clock is separate from the software clock settings, which are erased when the system is powered cycled or rebooted.

The **set** keyword sets the software clock. If the system is synchronized by a valid outside timing mechanism, such as a Network Time Protocol (NTP) clock source, you do not need to set the system clock. Use this command if no other time sources are available. The time specified in this command is relative to the configured time zone.

To perform a one-time update of the hardware clock (calendar) from the software clock or to copy the software clock settings to the hardware clock (calendar), use the **clock update-calendar** EXEC command.

Examples

The following example sets the software clock on the SE:

```
ServiceEngine#clock set 13:32:00 01 February 2000
```

Related Commands

clock timezone
ntp
show clock detail

clock (global configuration)

To set the summer daylight saving time and time zone for display purposes, use the **clock** global configuration command. To disable this function, use the **no** form of this command.

clock {**summertime** *timezone* {**date** *startday startmonth startyear starthour endday endmonth endyear offset* | **recurring** {**1-4** *startweekday startmonth starthour endweekday endmonth endhour offset* | **first** *startweekday startmonth starthour endweekday endmonth endhour offset* | **last** *startweekday startmonth starthour endweekday endmonth endhour offset*}} | **timezone** {*timezone houroffset minutesoffset*}}

no clock {**summertime** *timezone* {**date** *startday startmonth startyear starthour endday endmonth endyear offset* | **recurring** {**1-4** *startweekday startmonth starthour endweekday endmonth endhour offset* | **first** *startweekday startmonth starthour endweekday endmonth endhour offset* | **last** *startweekday startmonth starthour endweekday endmonth endhour offset*}} | **timezone** {*timezone houroffset minutesoffset*}}

Syntax Description

summertime	Configures the summer or daylight saving time.
<i>timezone</i>	Name of the summer time zone.
date	Configures the absolute summer time.
<i>startday</i>	Date (1–31) to start.
<i>startmonth</i>	Month (January through December) to start.
<i>startyear</i>	Year (1993–2032) to start.
<i>starthour</i>	Hour (0–23) to start in (hh:mm) format.
<i>endday</i>	Date (1–31) to end.
<i>endmonth</i>	Month (January through December) to end.
<i>endyear</i>	Year (1993–2032) to end.
<i>endhour</i>	Hour (0–23) to end in (hh:mm) format.
<i>offset</i>	Minutes offset (see Table B-1 on page B-1) from Coordinated Universal Time (UTC) (0–59).
recurring	Configures the recurring summer time.
1-4	Configures the starting week number 1–4.
first	Configures the summer time to recur beginning the first week of the month.
last	Configures the summer time to recur beginning the last week of the month.
<i>startweekday</i>	Day of the week (Monday–Friday) to start.
<i>startmonth</i>	Month (January–December) to start.
<i>starthour</i>	Hour (0–23) to start in (hh:mm) format.
<i>endweekday</i>	Weekday (Monday–Friday) to end.
<i>endmonth</i>	Month (January–December) to end.
<i>endhour</i>	Hour (0–23) to end in hour:minute (hh:mm) format.
<i>offset</i>	Minutes offset (see Table B-1 on page B-1) from UTC (0–59).
timezone	Configures the standard time zone.
<i>timezone</i>	Name of the time zone.

clock (global configuration)

<i>houroffset</i>	Hours offset (see Table B-1 on page B-1) from UTC (–23 to +23).
<i>minutesoffset</i>	Minutes offset (see Table B-1 on page B-1) from UTC (0–59).

Defaults

No default behavior or values.

Command Modes

Global configuration

Usage Guidelines

To set and display the local and UTC current time of day without an NTP server, use the **clock timezone** command with the **clock set** command. The **clock timezone** parameter specifies the difference between UTC and local time, which is set with the **clock set EXEC** command. The UTC and local time are displayed with the **show clock detail EXEC** command.

Use the **clock timezone offset** command to specify a time zone, where *timezone* is the desired time zone entry from [Table B-1 on page B-1](#) and *0 0* is the offset (ahead or behind) Coordinated Universal Time (UTC) in hours and minutes. UTC was formerly known as Greenwich mean time (GMT).

```
SE(config)#clock timezone timezone 0 0
```

**Note**

The time zone entry is case sensitive and must be specified in the exact notation listed in the time zone table as shown in [Appendix B, “Standard Time Zones.”](#) When you use a time zone entry from [Table B-1 on page B-1](#), the system is automatically adjusted for daylight saving time.

The offset (ahead or behind) UTC in hours, as displayed in [Table B-1 on page B-1](#), is in effect during winter time. During summer time or daylight saving time, the offset may be different from the values in the table and are calculated and displayed accordingly by the system clock.

**Note**

An accurate clock and timezone setting is required for the correct operation of the HTTP proxy caches.

Examples

The following example specifies the local time zone as Pacific Standard Time with an offset of 8 hours behind UTC:

```
ServiceEngine(config)#clock timezone PST -8
Custom Timezone: PST will be used.
```

The following example configures a standard time zone on the SE:

```
ServiceEngine(config)#clock timezone US/Pacific 0 0
Resetting offset from 0 hour(s) 0 minute(s) to -8 hour(s) 0 minute(s)
Standard Timezone: US/Pacific will be used.
ServiceEngine(config)#
```

The following example negates the time zone setting on the SE:

```
ServiceEngine(config)#no clock timezone
```

The following example configures daylight saving time:

```
ServiceEngine(config)#clock summertime PDT date 10 October 2001 23:59 29 April 2002 23:59
60
```

Related Commands

clock
show clock detail

cms (EXEC)

To configure the Centralized Management System (CMS) embedded database parameters, use the **cms EXEC** command.

```
cms {config-sync | database {backup | create | delete | downgrade [script filename] |
    maintenance {full | regular} | restore filename | validate} | deregister [force] | recover
    {identity word}}
```

Syntax Description

config-sync	Sets the node to synchronize configuration with the CDSM.
database	Creates, backs up, deletes, restores, or validates the CMS-embedded database management tables or files.
backup	Backs up the database management tables.
create	Creates the embedded database management tables.
delete	Deletes the embedded database files.
downgrade	Downgrades the CMS database.
script	(Optional) Downgrades the CMS database by applying a downgrade script.
<i>filename</i>	Downgraded script filename.
maintenance	Cleans and reindexes the embedded database tables.
full	Specifies a full maintenance routine for the embedded database tables.
regular	Specifies a regular maintenance routine for the embedded database tables.
restore	Restores the database management tables using the backup local filename.
<i>filename</i>	Database local backup filename.
validate	Validates the database files.
deregister	Removes the registration of the CMS proto device.
force	(Optional) Forces the removal of the node registration.
recover	Recovers the identity of an CDS network device.
identity	Specifies the identity of the recovered device.
<i>word</i>	Identity of the recovered device.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

The CDS network is a collection of SR, SE, and CDSM nodes. One primary CDSM retains the CDS network settings and provides other CDS network nodes with updates. Communication between nodes occurs over secure channels using the Secure Shell Layer (SSL) protocol, where each node on the CDS network uses a Rivest, Shamir, Adelman (RSA) certificate-key pair to communicate with other nodes.

Use the **cms config-sync** command to enable registered SRs, SEs, and standby CDSM to contact the primary CDSM immediately for a getUpdate (get configuration poll) request before the default polling interval of 5 minutes. For example, when a node is registered with the primary CDSM and activated, it

appears as Pending in the CDSM GUI until it sends a getUpdate request. The **cms config-sync** command causes the registered node to send a getUpdate request at once, and the status of the node changes as Online.

Use the **cms database create** command to initialize the CMS database. Before a node can join an CDS network, it must first be registered and then activated. The **cms enable** global configuration command automatically registers the node in the database management tables and enables the CMS. The node sends its attribute information to the CDSM over the SSL protocol and then stores the new node information. The CDSM accepts these node registration requests without admission control and replies with registration confirmation and other pertinent security information required for getting updates. Activate the node using the CDSM GUI.

Once the node is activated, it automatically receives configuration updates and the necessary security RSA certificate-key pair from the CDSM. This security key allows the node to communicate with any other node in the CDS network. The **cms deregister** command removes the node from the CDS network by deleting registration information and database tables.

To back up the existing management database for the CDSM, use the **cms database backup** command. For database backups, specify the following items:

- Location, password, and user ID
- Dump format in PostgreSQL plain text syntax

The naming convention for backup files includes the time stamp.

When you use the **cms recover identity word** command when recovering lost registration information, or replacing a failed node with a new node that has the same registration information, you must specify the device recovery key that you configured in the Modifying Config Property, System.device.recovery.key window of the CDSM GUI.

Use the **lcm** command to configure local/central management (LCM) on an CDS network device. The LCM feature allows settings configured using the device CLI or GUI to be stored as part of the CDS network-wide configuration data (enable or disable).

When you enter the **cms lcm enable** command, the CMS process running on SEs, SRs, and the standby CDSM detects the configuration changes that you made on these devices using CLIs and sends the changes to the primary CDSM.

When you enter the **cms lcm disable** command, the CMS process running on SEs, SRs, and the standby CDSM does not send the CLI changes to the primary CDSM. Settings configured using the device CLIs will not be sent to the primary CDSM.

If LCM is disabled, the settings configured through the CDSM GUI will overwrite the settings configured from the SE or SR; however, this rule applies only to those local device settings that have been overwritten by the CDSM when you have configured the local device settings. If you (as the local CLI user) change the local device settings after the particular configuration has been overwritten by the CDSM, the local device configuration will be applicable until the CDSM requests a full device statistics update from the SE or SR (clicking the **Force full database update** button from the Device Home window of the CDSM GUI triggers a full update). When the CDSM requests a full update from the device, the CDSM settings will overwrite the local device settings.

Examples

The following example backs up the database management tables:

```
CDSM# cms database backup
creating backup file with label `backup'
backup file local1/CDS-db-9-22-2002-17-36.dump is ready. use `copy' commands to move the
backup file to a remote host.
```

The following example validates the database management tables:

```
CDSM# cms database validate
Management tables are valid
```

In the following example, the CMS deregistration process has problems deregistering the SE, but it proceeds to deregister it from the CMS database when the **force** option is used:

```
ServiceEngine#cms deregister force
Deregistration requires management service to be stopped.
You will have to manually start it. Stopping management service on this node...
This operation needs to restart http proxy and streaming proxies/servers (if running) for
memory reconfiguration. Proceed? [no]yes
management services stopped
Thu Jun 26 13:17:34 UTC 2003 [I] main: creating 24 messages
Thu Jun 26 13:17:34 UTC 2003 [I] main: creating 12 dispatchers
Thu Jun 26 13:17:34 UTC 2003 [I] main: sending eDeRegistration message to CDSM
10.107.192.168
...
ServiceEngine#
```

The following example shows the use of the **cms recover identity** command when the recovery request matches the SE record, and the CDSM updates the existing record and sends a registration response to the requesting SE:

```
ServiceEngine#cms recover identity default
Registering this node as Service Engine...
Sending identity recovery request with key default
Thu Jun 26 12:54:42 UTC 2003 [I] main: creating 24 messages
Thu Jun 26 12:54:42 UTC 2003 [I] main: creating 12 dispatchers
Thu Jun 26 12:54:42 UTC 2003 [I] main: Sending registration message to CDSM
10.107.192.168
Thu Jun 26 12:54:44 UTC 2003 [W] main: Unable to load device info file in TestServer
Thu Jun 26 12:54:44 UTC 2003 [I] main: Connecting storeSetup for SE.
Thu Jun 26 12:54:44 UTC 2003 [I] main: Instantiating AStore
'com.cisco.unicorn.schema.PSqlStore'...
Thu Jun 26 12:54:45 UTC 2003 [I] main: Successfully connected to database
Thu Jun 26 12:54:45 UTC 2003 [I] main: Registering object factories for persistent
store...
Thu Jun 26 12:54:51 UTC 2003 [I] main: Dropped Sequence IDSET.
Thu Jun 26 12:54:51 UTC 2003 [I] main: Successfully removed old management tables
Thu Jun 26 12:54:51 UTC 2003 [I] main: Registering object factories for persistent
store...
.
.
.
Thu Jun 26 12:54:54 UTC 2003 [I] main: Created Table FILE_CDSM.
Thu Jun 26 12:54:55 UTC 2003 [I] main: Created SYS_MESS_TIME_IDX index.
Thu Jun 26 12:54:55 UTC 2003 [I] main: Created SYS_MESS_NODE_IDX index.
Thu Jun 26 12:54:55 UTC 2003 [I] main: No Consistency check for store.
Thu Jun 26 12:54:55 UTC 2003 [I] main: Successfully created management tables
Thu Jun 26 12:54:55 UTC 2003 [I] main: Registering object factories for persistent
store...
Thu Jun 26 12:54:55 UTC 2003 [I] main: AStore Loading store data...
Thu Jun 26 12:54:56 UTC 2003 [I] main: ExtExpiresRecord Loaded 0 Expires records.
Thu Jun 26 12:54:56 UTC 2003 [I] main: Skipping Construction RdToClusterMappings on
non-CDSM node.
Thu Jun 26 12:54:56 UTC 2003 [I] main: AStore Done Loading. 327
Thu Jun 26 12:54:56 UTC 2003 [I] main: Created SYS_MESS_TIME_IDX index.
Thu Jun 26 12:54:56 UTC 2003 [I] main: Created SYS_MESS_NODE_IDX index.
Thu Jun 26 12:54:56 UTC 2003 [I] main: No Consistency check for store.
Thu Jun 26 12:54:56 UTC 2003 [I] main: Successfully initialized management tables
Node successfully registered with id 103
Registration complete.
```

```
ServiceEngine#
```

The following example shows the use of the **cms recover identity** command when the hostname of the SE does not match the hostname configured in the CDSM graphical user interface:

```
ServiceEngine#cms recover identity default
Registering this node as Service Engine...
Sending identity recovery request with key default
Thu Jun 26 13:16:09 UTC 2003 [I] main: creating 24 messages
Thu Jun 26 13:16:09 UTC 2003 [I] main: creating 12 dispatchers
Thu Jun 26 13:16:09 UTC 2003 [I] main: Sending registration message to CDSM
10.107.192.168
There are no SE devices in CDN
register: Registration failed.
ServiceEngine#
```

Related Commands

cms enable
show cms

cms (global configuration)

To schedule maintenance and enable the Centralized Management System (CMS) on a given node, use the **cms** global configuration command. To negate these actions, use the **no** form of this command.

```
cms {database maintenance {full {enable | schedule weekday at time} | regular {enable | schedule weekday at time}} | enable | rpc timeout {connection 5-1800 | incoming-wait 10-600 | transfer 10-7200}}
```

```
no cms {database maintenance {full {enable | schedule weekday at time} | regular {enable | schedule weekday at time}} | enable | rpc timeout {connection 5-1800 | incoming-wait 10-600 | transfer 10-7200}}
```

Syntax Description	
database maintenance	Configures the embedded database clean or reindex maintenance routine.
full	Configures the full maintenance routine and cleans the embedded database tables.
enable	Enables the full maintenance routine to be performed on the embedded database tables.
schedule	Sets the schedule for performing the maintenance routine.
<i>weekday</i>	Day of the week to start the maintenance routine. every-day Every day Fri every Friday Mon every Monday Sat every Saturday Sun every Sunday Thu every Thursday Tue every Tuesday Wed every Wednesday
at	Sets the maintenance schedule time of day to start the maintenance routine.
<i>time</i>	Time of day to start the maintenance routine (0–23:0–59) (hh:mm).
regular	Configures the regular maintenance routine and reindexes the embedded database tables.
enable	Enables the node CMS process.
rpc timeout	Configures the timeout values for remote procedure call connections.
connection	Specifies the maximum time to wait when making a connection.
<i>5-1800</i>	Timeout period in seconds. The default for the CDSM is 30 seconds; the default for the SE and the SR is 180 seconds.
incoming-wait	Specifies the maximum time to wait for a client response.
<i>10-600</i>	Timeout period in seconds. The default is 30 seconds.
transfer	Specifies the maximum time to allow a connection to remain open.
<i>10-7200</i>	Timeout period in seconds. The default is 300 seconds.

Defaults

database maintenance regular: enabled
database maintenance full: enabled
connection: 30 seconds for CDSM; 180 seconds for the SE and the SR
incoming wait: 30 seconds
transfer: 300 seconds

Command Modes

Global configuration

Usage Guidelines

Use the **cms database maintenance** command to schedule routine full maintenance cleaning (vacuuming) or a regular maintenance reindexing of the embedded database. The full maintenance routine runs only when the disk is more than 90 percent full and only runs once a week. Cleaning the tables returns reusable space to the database system.

The **cms enable** command automatically registers the node in the database management tables and enables the CMS process. The **no cms enable** command only stops the management services on the device and does not disable a primary sender. You can use the **cms deregister** command to remove a primary or backup sender SE from the CDS network and to disable communication between the two multicast senders.

Examples

The following example schedules a regular (reindexing) maintenance routine to start every Friday at 11:00 p.m.:

```
ServiceEngine(config)#cms database maintenance regular schedule Fri at 23:00
```

The following example shows how to enable the CMS process on an SE:

```
ServiceEngine(config)#cms enable
This operation needs to restart http proxy and streaming proxies/servers (if running) for
memory reconfiguration. Proceed? [no]yes
Registering this node as Service Engine...
Thu Jun 26 13:18:24 UTC 2003 [I] main: creating 24 messages
Thu Jun 26 13:18:25 UTC 2003 [I] main: creating 12 dispatchers
Thu Jun 26 13:18:25 UTC 2003 [I] main: Sending registration message to CDSM
10.107.192.168
Thu Jun 26 13:18:27 UTC 2003 [I] main: Connecting storeSetup for SE.
Thu Jun 26 13:18:27 UTC 2003 [I] main: Instantiating AStore
'com.cisco.unicorn.schema.PSqlStore'...
Thu Jun 26 13:18:28 UTC 2003 [I] main: Successfully connected to database
Thu Jun 26 13:18:28 UTC 2003 [I] main: Registering object factories for persistent
store...
Thu Jun 26 13:18:35 UTC 2003 [I] main: Dropped Sequence IDSET.
Thu Jun 26 13:18:35 UTC 2003 [I] main: Dropped Sequence GENSET.
Thu Jun 26 13:18:35 UTC 2003 [I] main: Dropped Table USER_TO_DOMAIN.
.
.
.
Thu Jun 26 13:18:39 UTC 2003 [I] main: Created Table FILE_CDSM.
Thu Jun 26 13:18:40 UTC 2003 [I] main: Created SYS_MESS_TIME_IDX index.
Thu Jun 26 13:18:40 UTC 2003 [I] main: Created SYS_MESS_NODE_IDX index.
Thu Jun 26 13:18:40 UTC 2003 [I] main: No Consistency check for store.
Thu Jun 26 13:18:40 UTC 2003 [I] main: Successfully created management tables
Thu Jun 26 13:18:40 UTC 2003 [I] main: Registering object factories for persistent
store...
```

cms (global configuration)

```
Thu Jun 26 13:18:40 UTC 2003 [I] main: AStore Loading store data...
Thu Jun 26 13:18:41 UTC 2003 [I] main: ExtExpiresRecord Loaded 0 Expires records.
Thu Jun 26 13:18:41 UTC 2003 [I] main: Skipping Construction RdToClusterMappings on
non-CDSM node.
Thu Jun 26 13:18:41 UTC 2003 [I] main: AStore Done Loading. 336
Thu Jun 26 13:18:41 UTC 2003 [I] main: Created SYS_MESS_TIME_IDX index.
Thu Jun 26 13:18:41 UTC 2003 [I] main: Created SYS_MESS_NODE_IDX index.
Thu Jun 26 13:18:41 UTC 2003 [I] main: No Consistency check for store.
Thu Jun 26 13:18:41 UTC 2003 [I] main: Successfully initialized management tables
Node successfully registered with id 28940
Registration complete.
Warning: The device will now be managed by the CDSM. Any configuration changes
made via CLI on this device will be overwritten if they conflict with settings on the
CDSM.
Please preserve running configuration using 'copy running-config startup-config'.
Otherwise management service will not be started on reload and node will be shown
'offline' in CDSM UI.
management services enabled
ServiceEngine(config)#
```

Related Commands

cms database
cms deregister
show cms

configure

To enter global configuration mode, use the **configure** EXEC command. You must be in global configuration mode to enter global configuration commands.

configure

To exit global configuration mode, use the **end** or **exit** commands. In addition, you can press **Ctrl-Z** to exit from global configuration mode.

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Use this command to enter global configuration mode.

Examples

The following example shows how to enable global configuration mode:

```
ServiceEngine#configure
ServiceEngine(config)#
```

Related Commands

end
exit
show running-config
show startup-config

copy

To copy the configuration or image data from a source to a destination, use the **copy** EXEC command.

copy cdnfs disk *url sysfs-filename*

copy cdrom install *filedir filename*

copy disk {ftp {hostname | ip-address} remotefiledir remotefilename localfilename | startup-config filename}

copy ftp {disk {hostname | ip-address} remotefiledir remotefilename localfilename | install {hostname | ip-address} remotefiledir remotefilename}

copy http install {{hostname | ip-address} remotefiledir remotefilename} [port port-num [proxy {hostname | ip-address} | username username password [proxy {hostname | ip-address} proxy_portnum]] | proxy {hostname | ip-address} proxy_portnum | username username password [proxy {hostname | ip-address} proxy_portnum]]

copy running-config {disk filename | startup-config | remotefilename}

copy startup-config {disk filename | running-config | remotefilename}

copy system-status disk filename

copy tech-support {disk filename | remotefilename}

Syntax Description

cdnfs	Copies a file from the cdnfs to the sysfs.
disk	Copies a file to the disk.
<i>url</i>	URL of the cdnfs file to be copied to the sysfs.
<i>sysfs-filename</i>	Filename to be copied in the sysfs.
cdrom	Copies a file from the CD-ROM.
install	Installs the software release file.
<i>filedir</i>	Directory location of the software release file.
<i>filename</i>	Filename of the software release file.
disk	Copies a local disk file.
ftp	Copies to a file on an FTP server.
<i>hostname</i>	Hostname of the FTP server.
<i>ip-address</i>	IP address of the FTP server.
<i>remotefiledir</i>	Directory on the FTP server to which the local file is copied.
<i>remotefilename</i>	Name of the local file once it has been copied to the FTP server.
<i>localfilename</i>	Name of the local file to be copied.
startup-config	Copies the configuration file from the disk to startup configuration (NVRAM).
<i>filename</i>	Name of the existing configuration file.
ftp	Copies a file from an FTP server.
disk	Copies a file to a local disk.

<i>hostname</i>	Hostname of the FTP server.
<i>ip-address</i>	IP address of the FTP server.
<i>remotefiledir</i>	Directory on the FTP server where the file to be copied is located.
<i>remotefilename</i>	Name of the file to be copied to the local disk.
<i>localfilename</i>	Name of the copied file as it appears on the local disk.
install	Copies the file from an FTP server and installs the software release file to the local device.
<i>hostname</i>	Name of the FTP server.
<i>ip-address</i>	IP address of the FTP server.
<i>remotefiledir</i>	Remote file directory.
<i>remotefilename</i>	Remote filename.
http install	Copies the file from an HTTP server and installs the software release file on a local device.
<i>hostname</i>	Name of the HTTP server.
<i>ip-address</i>	IP address of the HTTP server.
<i>remotefiledir</i>	Remote file directory.
<i>remotefilename</i>	Remote filename.
port	(Optional) Specifies the port to connect to the HTTP server (default is 80).
<i>port-num</i>	HTTP server port number (1–65535).
proxy	Allows the request to be redirected to an HTTP proxy server.
<i>hostname</i>	Name of the HTTP server.
<i>ip-address</i>	IP address of the HTTP server.
<i>proxy_portnum</i>	HTTP proxy server port number (1–65535).
username	Specifies the username to access the HTTP proxy server.
<i>username</i>	User login name.
running-config	Copies the current system configuration.
disk	Copies the current system configuration to a disk file.
<i>filename</i>	Name of the file to be created on disk.
startup-config	Copies the running configuration to the startup configuration (NVRAM).
<i>remotefilename</i>	Remote filename of the configuration file to be created on the TFTP server. Use the complete pathname.
startup-config	Copies the startup configuration.
disk	Copies the startup configuration to a disk file.
<i>filename</i>	Name of the startup configuration file to be copied to the local disk.
running-config	Copies the startup configuration to a running configuration.
<i>remotefilename</i>	Remote filename of the startup configuration file to be created on the TFTP server. Use the complete pathname.
system-status disk	Copies the system status to a disk file.
<i>filename</i>	Name of the file to be created on the disk.
tech-support	Copies system information for technical support.
disk	Copies system information for technical support to a disk file.

<i>filename</i>	Name of the file to be created on disk.
<i>remotefilename</i>	Remote filename of the system information file to be created on the TFTP server. Use the complete pathname.

Defaults**HTTP server port:** 80**Default working directory for sysfs files:** /local1**Command Modes**

EXEC

Usage Guidelines

The **copy cdnfs** EXEC command copies data files out of the cdnfs to the sysfs for further processing. For example, you can use the **install imagefilename** EXEC command to provide the copied files to the command.

The **copy disk ftp** command copies files from a sysfs partition to an FTP server. The **copy disk startup-config** command copies a startup configuration file to NVRAM.

The **copy ftp disk** command copies a file from an FTP server to a sysfs partition.

Use the **copy ftp install** command to install an image file from an FTP server. Part of the image goes to the disk and part goes to the flash memory.

Use the **copy http install** command to install an image file from an HTTP server and install it on a local device. It transfers the image from an HTTP server to the SE using HTTP as the transport protocol and installs the software on the device. Part of the image goes to the disk and part goes to the flash memory. You can also use this command to redirect your transfer to a different location or HTTP proxy server, by specifying the **proxy hostname | ip-address** option. A username and a password will have to be authenticated with the remote HTTP server if the server is password protected and requires authentication before the transfer of the software release file to the SE is allowed.

Use the **copy cdrom install** option to install the image from the rescue CD.

```
ServiceEngine#copy cdrom install /images CDS24.bin
```

Use the **copy running-config** command to copy the running system configuration to a sysfs partition or flash memory. The **copy running-config startup-config** command is equivalent to the **write memory** command.

The **copy startup-config** command copies the startup configuration file to a sysfs partition.

The **copy system-status** command creates a file on a sysfs partition containing hardware and software status information.

The **copy tech-support tftp** command can copy technical support information to a sysfs partition.

Related Commands

```
install
reload
show running-config
show startup-config
write
```

cpfile

To make a copy of a file, use the **cpfile** EXEC command.

cpfile *oldfilename newfilename*

Syntax Description	<i>oldfilename</i>	Name of the file to copy.
	<i>newfilename</i>	Name of the copy to be created.

Defaults	No default behavior or values.

Command Modes	EXEC

Usage Guidelines	Use this command to create a copy of a file. Only sysfs files can be copied.

Examples	The following example shows how to create a copy of a file: ServiceEngine# cpfile syslog.txt syslog.txt.save

Related Commands	copy dir lls ls mkfile rename rmdir

debug

To monitor and record caching application functions, use the **debug** EXEC command. To disable **debug**, use the **no** form of this command.

debug *option*

no debug *option*

Syntax Description

<i>option</i>	Specifies the debugger type; see the “Usage Guidelines” section for valid values.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines



Note

We recommend that you use the **debug** command only at the direction of Cisco TAC because the SE performance is affected when you enter the **debug** command.

You can use the **logging disk priority debug** global configuration command with the **debug** command. This configuration causes the debugging messages to be logged in the syslog file, which is available in the /local1 directory by default. You can then download the messages from the SE, copy them to a local disk file (for example, using the **copy disk ftp** command), and forward the logs to Cisco TAC for further investigation. By default, system log messages are logged to the console and you need to copy and paste the output to a file. However, this method of obtaining logs is more prone to errors than capturing all messages in the syslog.txt file. When you use system logging to a disk file instead of system logging to a console, there is no immediate feedback that debug logging is occurring, except that the syslog.txt file gets larger (you can track the lines added to the syslog.txt file by entering the **type-tail syslog.txt follow** command). When you have completed downloading the system logs to a local disk, you must disable the debugging functions by using the **undebug** command (see the [“undebug”](#) section on page -820 for more details), and reset the level of logging disk priority to any other setting that you want (for example, **notice** priority).

Valid values for *option* are as follows:

access-lists 300	Debugs the access control list.
dump	Dumps the access control list contents.
query	Queries the access control list configuration.
username username	Queries the access control list username.
groupname groupnames	Queries the access control list group name or names of groups of which the user is a member. Each group name must be separated by a comma.

acquirer	Debugs the acquirer.
error	Sets the debug level to error.
trace	Sets the debug level to trace.
all	Enables all debugging.
authentication	Debugs authentication.
user	Debugs the user login against the system authentication.
authsvr	Debugs the Authentication Server.
error	Sets the debug level to error.
trace	Sets the debug level to trace.
bandwidth	Debugs the bandwidth module.
advanced	Advanced bandwidth controller debug commands.
error	Sets the debug level to error.
trace	Sets the debug level to trace.
buf	Debugs the buffer manager.
all	Debugs all buffer manager functions.
dmbuf	Debugs the buffer manager dmbuf.
dmsg	Debugs the buffer manager dmsg.
cache-content	Debugs the caching service.
all	(Optional) Sets the debug level to all.
error	(Optional) Sets the debug level to error.
trace	(Optional) Sets the debug level to trace.
cache-router	Debugs the caching router.
error	Sets the debug level to error.
trace	Sets the debug level to trace.
cdnfs	Debugs the CDS network file system (cdnfs).
cli	Debugs the CLI command.
all	Debugs all CLI commands.
bin	Debugs the CLI command binary program.
parser	Debugs the CLI command parser.
cms	Debugs the CMS.
dataserver	Debugs the data server.
all	Debugs all data server functions.
clientlib	Debugs the data server client library module.
server	Debugs the data server module.

dfs	Debugs the DFS.
all	Sets the debug level to all.
api	Debugs the DFS application API.
diskcache	Debugs the DFS in-memory disk-directory cache management.
memcache	Debugs the DFS in-memory cache.
rawio	Debugs the DFS raw disk I/O.
dhcp	Debugs the DHCP.
distribution	Debugs the distribution components.
all	Debugs all distribution components.
error	Debugs all distribution components to error level 1 (show error).
trace	Debugs all distribution components to trace level 2 (show error and trace).
metadata-receiver	Debugs the metadata receiver distribution component.
error	Debugs the metadata receiver distribution component to error level 1.
trace	Debugs the metadata receiver distribution component to trace level 2.
metadata-sender	Debugs the metadata sender distribution component.
error	Debugs the metadata sender distribution component to error level 1.
trace	Debugs the metadata sender distribution component to trace level 2.
mcast-receiver	Debugs the multicast receiver distribution component.
error	Debugs the multicast receiver distribution component to error level 1.
trace	Debugs the multicast receiver distribution component to trace level 2.
mcast-sender	Debugs the multicast sender distribution component.
error	Debugs the multicast sender distribution component to error level 1.
trace	Debugs the multicast sender distribution component to trace level 2.
unicast-data-receiver	Debugs the unicast receiver distribution component.
error	Debugs the unicast receiver distribution component to error level 1.
trace	Debugs the unicast receiver distribution component to trace level 2.
unicast-data-sender	Debugs the unicast sender distribution component.
error	Debugs the unicast sender distribution component to error level 1.
trace	Debugs the unicast sender distribution component to trace level 2.

emdb	Debugs the embedded database.
level	(Optional) Debug level.
(0-16)	Debug level 0 through 16.
flash-media-streaming	Debugs Flash Media Streaming.
error	Debugs the Flash Media Streaming log level error.
trace	Debugs the Flash Media Streaming log level debug.
icap	Debugs ICAP.
all	Debugs both ICAP client and ICAP daemon processing.
client	Debugs the ICAP client (caching proxy) processing.
daemon	Debugs the ICAP daemon processing.
logging	Debugs logging.
all	Debugs all logging functions.
malloc	Debug commands for memory allocation.
cache-app	Debugging commands for cache application memory allocation.
all	Sets the debug level to all.
caller-accounting	Collects statistics for every distinct allocation call-stack.
catch-double-free	Alerts if application attempts to release the same memory twice.
check-boundaries	Checks boundary over and under run scribble.
check-free-chunks	Checks if free chunks are over-written after release.
clear-on-alloc	Ensures all allocations are zero-cleared.
statistics	Allocator use statistical summary.
dns-server	DNS Caching Service memory allocation debugging.
all	Sets the debug level to all.
caller-accounting	Collects statistics for every distinct allocation call-stack.
catch-double-free	Alerts if application attempts to release the same memory twice.
check-boundaries	Checks boundary over and under run scribble.
icap	ICAP Service memory allocation debugging.
caller-accounting	Collects statistics for every distinct allocation call-stack.
catch-double-free	Alerts if application attempts to release the same memory twice.
check-boundaries	Checks boundary over and under run scribble.
log-directory	Memory allocation debugging log directory.
word	Directory path name.
movie-streamer	Debug commands for the Movie Streamer.
error	Sets the debug level to error.
trace	Sets the debug level to trace.
ntp	Debugs NTP.

qos	Debug commands for the QoS component.
policy service	Debug commands for the policy service.
error	Sets the debug level to error.
trace	Sets the debug level to trace.
rbc	Debugs the RBCP (Router Blade Configuration Protocol) functions.
rpc	Displays the remote procedure calls (RPC) logs.
detail	Displays the RPC logs of priority “detail” level or higher.
trace	Displays the RPC logs of priority “trace” level or higher.
rtsp	Debugs the RTSP functions.
gateway	Debugs the RTSP gateway.
error	Debugs the RTSP gateway to level 1 (show error).
trace	Debugs the RTSP gateway to level 2 (show error and trace).
rule	Debugs the Rules Template.
action	Debugs the rule action.
all	Debugs all rule functions.
pattern	Debugs the rule pattern.
service-router	Debug commands for the service router.
servicemonitor	Debug commands for the service monitor.
session-manager	Session manager debug commands.
critical	Sets the debug level to critical.
error	Sets the debug level to error.
trace	Sets the debug level to trace.
snmp	Debugs SNMP.
all	Debugs all SNMP functions.
cli	Debugs the SNMP CLI.
main	Debugs the SNMP main.
mib	Debugs the SNMP MIB.
traps	Debugs the SNMP traps.
standby	Debugs standby.
all	(Optional) Debugs all standby functions.
stats	Debugs the statistics.
all	Debugs all statistics functions.
collection	Debugs the statistics collection.
computation	Debugs the statistics computation.
history	Debugs the statistics history.

translog	Debugs the transaction logging.
all	Debugs all transaction logging.
archive	Debugs the transaction log archive.
export	Debugs the transaction log FTP export.
uns	Unified naming service debug commands.
all	(Optional) Sets the debug level to all.
error	(Optional) Sets the debug level to error.
trace	(Optional) Sets the debug level to trace.
webengine	WebEngine debug commands.
error	Sets the debug level to error.
trace	Sets the debug level to trace.
wi	Debugs the web interface.
wmt	Debugs the WMT component.
error	Debugs the WMT level 1 functionality. For more information, see the “Using WMT Error Logging” section on page 2-75.
client-ip <i>cl-ip-address</i>	(Optional) Debugs the request from a specific client IP address to level 1 (show error).
server-ip <i>sv-ip-address</i>	(Optional) Debugs the request to a specific server IP address to level 1 (show error).
trace	Debugs the WMT level 2 functionality.
client-ip <i>cl-ip-address</i>	(Optional) Debugs the request from a specific client IP address to level 2 (show error and trace).
server-ip <i>sv-ip-address</i>	(Optional) Debugs the request to a specific server IP address to level 2 (show error and trace).

Debugging Cdnfs

You can use the **debug cdnfs** command to monitor the lookup and serving of pre-positioned files. If pre-positioned files are available in cdnfs but are not served properly, you can use cdnfs debug.

Using WMT Error Logging

In the Internet Streamer CDS Release 2.4 software, WMT error logging was enhanced. More information is now logged about the following events:

- When a WMT client is abruptly disconnected
- When any WMT streams are cleared on the SE

Error logs are in the same format and location as syslogs. The WMT log messages are logged to /local1/errorlog/wmt_errorlog.current.

You can configure the SE for WMT error logging by using the **debug wmt error EXEC** command. This command debugs WMT level 1 functionality.

Logging WMT Client Disconnects

When a WMT client is disconnected abruptly, the reasons for the client disconnect (for example, the request was blocked by the rules, the maximum incoming or outgoing bit-rate limit was reached, the maximum incoming or outgoing bandwidth limit was reached) are logged in Internet Streamer CDS software error logs.

The client information includes the client IP address, the server IP address, the requested URL, the client protocol, the version of the client media player, the number of packets that the client received, and the number of packets that the server sent.

Related Commands

logging
show debugging
undebug

delfile

To delete a file, use the **delfile** EXEC command.

delfile *filename*

Syntax Description	<i>filename</i> Name of the file to delete.
Defaults	No default behavior or values.
Command Modes	EXEC
Usage Guidelines	Use this command to remove a file from a sysfs partition.
Examples	The following example shows how to delete a file: <pre>ServiceEngine#delfile /local1/tempfile</pre>
Related Commands	cpfile deltree mkdir mkfile rmdir

deltree

To remove a directory with its subdirectories and files, use the **deltree** EXEC command.

deltree *directory*

Syntax Description	<i>directory</i> Name of the directory tree to delete.
Defaults	No default behavior or values.
Command Modes	EXEC
Usage Guidelines	Use this command to remove a directory and all files within the directory from the SE sysfs file system. Do not remove files or directories required for proper SE functioning.
Examples	The following example shows how to delete a directory from the /local1 directory: ServiceEngine# deltree /local1/testdir
Related Commands	delfile mkdir mkfile rmdir

device

To configure the mode of operation on a device as a CDSM, SE or SR, use the **device** global configuration command. To reset the mode of operation on a device, use the **no** form of this command.

device mode {**content-delivery-system-manager** | **service-engine** | **service-router**}

no device mode {**content-delivery-system-manager** | **service-engine** | **service-router**}

Syntax Description	mode	Sets the mode of operation of a device to CDSM, SE or SR.
	content-delivery-system-manager	Configures the device operation mode as a CDSM.
	service-engine	Configures the device operation mode as an SE.
	service-router	Configures the device operation mode as an SR.

Defaults The default device operation mode is SE.

Command Modes Global configuration

Usage Guidelines A CDSM is the content management and device management station of an CDS network that allows you to specify what content is to be distributed, and where the content should be distributed. If an SR is deployed in the CDS network, the SR redirects the client based on redirecting policy. An SE is the device that serves content to the clients. There are typically many SEs deployed in an CDS network, each serving a local set of clients. IP/TV brings movie-quality video over enterprise networks to the desktop of the CDS network user.

Because different device modes require disk space to be used in different ways, disk space must also be configured when the device mode changes from being an SE or SR to CDSM (or the other way around). You must reboot the device before the configuration changes to the device mode take effect.

Disks must be configured before device configuration is changed. Use the **disk configure** command to configure the disk before reconfiguring the device to the SE or SR mode. Disk configuration changes using the **disk configure** command takes effect after the next device reboot.

To enable CDS network-related applications and services, use the **cms enable** command. Use the **no** form of this command to disable the CDS network.

All CDS devices ship from the factory as SEs. Before configuring network settings for CDSMs and SRs using the CLI, you must change the device from an SE to the proper device mode.

Configuring the device mode is not a supported option on all hardware models. However, you can configure some hardware models to operate as any one of the four content networking device types. Devices that can be reconfigured using the **device mode** global configuration command are shipped from the factory by default as SEs.

To change the device mode of your SE, you must also configure the disk space allocations, as required by the different device modes, and reboot the device for the new configuration to take effect.

When you change the device mode of an SE to an SR or CDSM, you may need to reconfigure the system file system (sysfs). However, SRs and CDSMs do not require any disk space other than sysfs. When you change the device mode to an SR or a CDSM, disk configuration changes are not required because the device already has some space allotted for sysfs. sysfs disk space is always preconfigured on a factory-fresh CDS network device. See the [“Disk Space-Allocation Guidelines for Service Routers” section on page 2-85](#) and [“Disk Space-Allocation Guidelines for CDSMs” section on page 2-85](#) for more information.

If you are changing the device mode of an SR or a CDSM back to an SE, you must configure disk space allocations for the caching, pre-positioning (cdnfs) and system use (sysfs) file systems that are used on the SE. You can configure disk space allocations either before or after you change the device mode to an SE.

Examples

The following examples show the configuration from the default mode, SE, to the CDSM, SR, and SE modes:

```
ServiceEngine(config)#device mode content-delivery-system-manager
```

```
CDSM(config)#device mode service-router
```

```
ServiceRouter(config)#device mode service-engine
```

Related Commands

show device-mode

dir

To view a long list of files in a directory, use the **dir** EXEC command.

dir [*directory*]

Syntax Description	<i>directory</i> (Optional) Name of the directory to list.
Defaults	No default behavior or values.
Command Modes	EXEC
Usage Guidelines	Use this command to view a detailed list of files contained within the working directory, including names, sizes, and time created. The equivalent command is lls .
Examples	The following example shows how to view a list of files in a directory: <pre>ServiceEngine#dir size time of last change name ----- 3931934 Tue Sep 19 10:41:32 2000 errlog-cache-20000918-164015 431 Mon Sep 18 16:57:40 2000 ii.cfg 431 Mon Sep 18 17:27:46 2000 ii4.cfg 431 Mon Sep 18 16:54:50 2000 iii.cfg 1453 Tue Sep 19 10:34:03 2000 syslog.txt 1024 Tue Sep 19 10:41:31 2000 <DIR> testdir</pre>
Related Commands	lls ls

direct-server-return

To enable a VIP for direct server return, use the **direct-server-return** global configuration command. To disable direct server return, use the **no** form of this command.

direct-server-return *vip ip address*

no direct-server-return *vip ip address*

Syntax Description	vip	Specifies the VIP for direct-server-return.
	<i>ip address</i>	VIP for direct-server-return.

Defaults	No default behavior or values.

Command Modes	Global configuration

Usage Guidelines	Direct Server Return (DSR) is a method used by load balancer servers in a load balancing configuration. DSR responds directly to the client, bypassing the load balancer in the response path. Table 2-4 shows the Direct Server Return flow.

Table 2-4 Direct Server Return Flow

Step	Process	Source IP	Destination IP	Destination MAC
Step 1	Client to load balancer	171.71.50.140	170.1.1.45	00:30:48:C3:C7:C5
Step 2	Load balancer to SR	171.71.50.140	170.1.1.45	00:14:5E:83:6E:7E
Step 3	SR to client	170.1.1.45	171.71.50.140	Default Gateway MAC

Examples	The following example shows how to enable direct server return:

```
ServiceEngine(config)#direct-server-return vip 1.1.1.1
ServiceEngine(config)#
```

Related Commands	show direct-server-return

disable

To turn off privileged EXEC commands, use the **disable** EXEC command.

disable

Syntax Description	This command has no arguments or keywords.
Defaults	No default behavior or values.
Command Modes	EXEC
Usage Guidelines	The disable command places you in the user-level EXEC shell. To turn privileged EXEC mode back on, use the enable command.
Examples	The following example shows how to enter the user-level EXEC mode: <pre>ServiceEngine#disable ServiceEngine></pre>
Related Commands	enable

disk (EXEC)

To configure disks and allocate disk space for devices that are using the CDS software, use the **disk** EXEC command.

disk mark *diskname* {**bad** | **good**}

disk recover-system-volumes

disk reformat *diskname*

disk unuse *diskname*

Syntax Description

mark	Marks a disk drive as good or bad.
<i>diskname</i>	Name of the disk to be marked (disk01, disk02, and so on).
bad	Marks the disk drive as bad.
good	Marks the disk drive as good.
recover--system-volumes	Erases all SYSTEM and SYSFS volumes.
reformat	Performs a low-level format of the SCSI, IDE, or SATA disks and remaps disk errors.
<i>diskname</i>	Name of the disk to be reformatted (disk01, disk02, and so on).
unuse	Stops applications from using a disk drive.
<i>diskname</i>	Name of the disk to be stopped for application use (disk01, disk02, and so on).

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

The disk space in the CDS software is allocated on a per-file system basis, rather than on a per-disk basis. You can configure your overall disk storage allocations according to the kinds of client protocols that you expect to use and the amount of storage that you need to provide for each of the functions.



Note

For details on the Cisco Internet Streamer CDS software disk storage and configuration requirements for SEs, see the *Cisco Internet Streamer CDS 2.4 Software Configuration Guide*.

The cndfs and sysfs partitions use the ext2 file system. With ext2 file systems, if the system crashed or if the system is not shut down cleanly, a file system check of these partitions takes a long time. If there are sector failures on the disk, the time to perform a file system check with an ext2 file system increases even more. By migrating to the ext3 file system, the amount of time required to perform a file system check of the cndfs and sysfs partitions is decreased, which increases the availability of the SE. If you are upgrading from an earlier release of the CDS software, the ext2 file system is automatically converted to the ext3 file system.

The `cdnfs` amounts are reported by the actual usable amounts of storage for applications. Due to the internal file system overhead of approximately 3 percent, the reported amounts may be smaller than what you configured.

To view disk details, use the **show disks details**.

**Note**

The **show disks details** command shows the amount of disk space that is allocated to system use. This detail is not shown by using the **show disks current** command.

To show the space allocation in each individual file system type, use the **show statistics cdnfs** command.

**Note**

For information on disk allocation guidelines for SEs, see the *Cisco Internet Streamer CDS 2.4 Software Configuration Guide*.

For higher-end models that might be used as a dedicated HTTP cache or RealProxy cache, you could give cache storage more disk space.

After upgrading from an earlier release of Internet Streamer CDS software to Cisco Internet Streamer Release 2.4 software and later releases, your disk space allocation remains the same as previously configured.

Disk Space-Allocation Guidelines for Service Routers

In Cisco Internet Streamer Release 2.4 software, SRs are used as DNS servers for the delegated DNS zone used in simplified hybrid routing. The DNS servers do not store any content and do not participate in acquisition or distribution of the pre-positioned content. The only disk space that needs to be configured on the SR is the `sysfs`.

Disk Space-Allocation Guidelines for CDSMs

CDSMs are used to manage content distribution for CDS networks. Because the CDSM does not store the content, the only file system that needs to be configured is the `sysfs`.

Remapping of Bad Sectors on Disk Drives

The **disk reformat** *diskname* EXEC command performs a low-level format of the SCSI, IDE, or SATA disks. This command erases all of the content on the disk.

If a disk drive continues to report a failure after you have used the **disk reformat** command, you must replace the disk drive.

**Caution**

Be careful when using the **disk reformat** *diskname* command because this command causes all content on the specified disk to be deleted.

In Cisco Internet Streamer Release 2.4 software, SCSI and Serial Advanced Technology Attachment (SATA) drives can be reformatted.

Stopping Applications from Using a Disk Drive

The **disk unuse** EXEC command allows you to stop applications from using a specific disk drive (for example, `disk01`) without having to reboot the device:

```
ServiceEngine# disk unuse disk01
```

The **disk unuse** command has the following behavior:

1. Cannot be used with SYSFS disk if the state of RAID-1 is not “Normal”.
2. Cannot be used with the cdnfs disk, which contains the “/uns-symlink-tree” directory.
3. Can be used with any disk except as in scenario 1 and 2 above.

Examples

The following examples show usage of the **disk unuse** command and the resultant actions:

```
ServiceEngine#disk unuse disk00
```

```
disk00 has key CDNFS data and can not be unused!
```

```
ServiceEngine#disk unuse disk01
```

```
This will restart applications currently using disk01
and unmount all partitions on disk01.
```

```
Do you want to continue? (Yes/No): yes
```

```
[WARNING] CDNFS and RAID SYSTEM partitions detected on disk01
```

```
[WARNING] Unusing a RAID SYSTEM disk results in boot-time RAID conflicts that cause the
drive to be erased and repartitioned. This has little effect on RAID volumes,
as their data will resync. However, any CDNFS data on the drive will be lost!
```

```
Unuse disk01, erasing all CDNFS data? (Yes/No): yes
```

```
disk01 is now unused
```

```
ServiceEngine#disk unuse disk02
```

```
This will restart applications currently using disk02
and unmount all partitions on disk02.
```

```
Do you want to continue? (Yes/No): yes
```

```
disk02 is now unused
```

The following example shows how to display the current disk space configuration:

```
ServiceEngine#show disks current
```

```
Local disks:
```

```
    SYSFS 32.0GB 0.7%
```

```
    CDNFS 4616.0GB 99.3%
```

The following example shows how to view disk details:

```
ServiceEngine#show disks details
```

```
disk00: Normal      (h02 c00 i00 l00 -      mptsas) 476937MB(465.8GB)
        disk00/04: SYSFS      32765MB( 32.0GB) mounted at /local1
        disk00/05: CDNFS      434445MB(424.3GB) mounted internally
        System use:           9726MB(   9.5GB)
        FREE:                 0MB(   0.0GB)
disk01: Normal      (h02 c00 i01 l00 -      mptsas) 476937MB(465.8GB)
        disk01/04: SYSFS      32765MB( 32.0GB) mounted at /local1
        disk01/05: CDNFS      434445MB(424.3GB) mounted internally
        System use:           9726MB(   9.5GB)
        FREE:                 0MB(   0.0GB)
disk02: Normal      (h02 c00 i02 l00 -      mptsas) 476937MB(465.8GB)
        disk02/01: CDNFS      476929MB(465.8GB) mounted internally
        System use:           7MB(   0.0GB)
        FREE:                 0MB(   0.0GB)
```

The following examples show how to view space allocation in each file system type:

```
ServiceEngine#show statistics cdnfs
```

```
CDNFS Statistics:
```

```
-----
```

```
Volume on :
```

```
    size of physical filesystem:          444740904 KB
```

```
    space assigned for CDNFS purposes:    444740904 KB
```

```
    number of CDNFS entries:              40 entries
```

```

space reserved for CDNFS entries:      436011947 KB
available space for new entries:       8728957 KB
physical filesystem space in use:      435593864 KB
physical filesystem space free:        9147040 KB
physical filesystem percentage in use:  98 %

Volume on :
size of physical filesystem:           444740904 KB
space assigned for CDNFS purposes:     444740904 KB
number of CDNFS entries:               43 entries
space reserved for CDNFS entries:      436011384 KB
available space for new entries:       8729520 KB
physical filesystem space in use:      435593720 KB
physical filesystem space free:        9147184 KB
physical filesystem percentage in use:  98 %

Volume on :
size of physical filesystem:           488244924 KB
space assigned for CDNFS purposes:     488244924 KB
number of CDNFS entries:               48 entries
space reserved for CDNFS entries:      479612533 KB
available space for new entries:       8632391 KB
physical filesystem space in use:      479152708 KB
physical filesystem space free:        9092216 KB
physical filesystem percentage in use:  99 %

```

Related Commands

disk (global configuration mode)
show cdnfs
show disks
show disks details
show statistics

disk (global configuration)

To configure how disk errors should be handled and to define a disk device error-handling threshold, use the **disk** global configuration command. To remove the device error-handling options, use the **no** form of this command.

```
disk error-handling {reload | threshold number}

no disk error-handling {reload | threshold number}
```

Syntax Description

error-handling	Configures disk error handling.
reload	Reloads the disk if the system file system (sysfs) (disk00) has problems.
threshold	Sets the number of disk errors allowed before the disk is marked as bad.
<i>number</i>	Number of disk errors allowed before the disk is marked as bad (0–100). The default is 1. The value 0 means that the disk should never be marked as bad.

Defaults

error-handling threshold *number*: 10

Command Modes

Global configuration

Usage Guidelines

In order to operate properly, the SE must have critical disk drives. A critical disk drive is the first disk drive that also contains the first sysfs (system file system) partition. It is referred to as disk00.

The sysfs partition is used to store log files, including transaction logs, system logs (syslogs), and internal debugging logs. It can also be used to store image files and configuration files on an SE.



Note

A critical drive is a disk drive that is either disk00 or a disk drive that contains the first sysfs partition. Smaller single disk drive SEs have only one critical disk drive. Higher-end SEs that have more than one disk drive may have more than one critical disk drive.

When an SE is booted and a critical disk drive is not detected at system startup time, the CDS system on the SE runs at a degraded state. If one of the critical disk drives goes bad at run time, the CDS system applications can malfunction, hang, or crash, or the CDS system can hang or crash. You must monitor the critical disk drives on an SE and report any disk drive errors to Cisco TAC.

With an CDS system, a disk device error is defined as any of the following events:

- A Small Computer Systems Interface (SCSI) or Integrated Drive Electronics (IDE) device error is printed by a Linux kernel.
- A disk device access by an application (for example, an open(2), read(2), or write(2) system call) fails with an EIO error code.
- A disk device that existed at startup time is not accessible at run time.

The disk status is recorded in flash (nonvolatile storage). When an error on an SE disk device occurs, a message is written to the system log (syslog) if the sysfs partition is still intact, and an SNMP trap is generated if SNMP is configured on the SE.

In addition to tracking the state of critical disk drives, you can define a disk device error-handling threshold on the SE. If the number of disk device errors reaches the specified threshold, the corresponding disk device is automatically marked as bad. The CDS system does not stop using the bad disk device immediately; it stops using the bad disk drive after the next reboot.

If the specified threshold is exceeded, the SE either records this event or reboots. If the automatic reload feature is enabled and this threshold is exceeded, then the CDS system automatically reboots the SE. For more information about specifying this threshold, see the [“Specifying the Disk Error-Handling Threshold” section on page 2-89](#).

In Cisco Internet Streamer Release 2.4 software, you can remap bad (but unused) sectors on a SCSI drive and SATA drives.

Specifying the Disk Error-Handling Threshold

In Cisco Internet Streamer CDS Release 2.4 software, you can configure a disk error-handling threshold. This threshold determines how many disk errors can be detected before the disk drive is automatically marked as bad. By default, this threshold is set to 10.

The **disk error-handling threshold** option determines how many disk errors can be detected before the disk drive is automatically marked as bad. By default, this threshold is set to 10.

To change the default threshold, use the **disk error-handling threshold** global configuration command. Specify 0 if you never want the disk drive to be marked as bad.

If the bad disk drive is a critical disk drive, and the automatic reload feature (**disk error-handling reload** command) is enabled, then the Internet Streamer CDS software marks the disk drive as bad and the SE is automatically reloaded. After the SE is reloaded, a syslog message and an SNMP trap are generated.

By default, the automatic reload feature is disabled on an SE. To enable the automatic reload feature, use the **disk error-handling reload** global configuration command. After enabling the automatic reload feature, use the **no disk error-handling reload** global configuration command to disable it.

Examples

The following example shows that five disk drive errors for a particular disk drive (for example, disk00) will be allowed before the disk drive is automatically marked as bad:

```
ServiceEngine(config)# disk error-handling threshold 5
```

Related Commands

disk (EXEC mode)
show disks
show disks details

distribution

To reschedule and refresh content redistribution for a specified delivery service ID or name, use the **distribution EXEC** command.

distribution {**failover** {**delivery-service-id** *delivery-service-num* | **delivery-service-name** *name*} [**force**] | **fallback** {**delivery-service-id** *delivery-service-num* | **delivery-service-name** *name*}}

distribution primary-ip-fallback {**forwarder-id** *forwarder-num* | **forwarder-name** *name*}

distribution refresh {**meta-data** **delivery-service-id** *delivery-service-num* | **object** *object-url*}

Syntax Description		
failover		Triggers the root or forwarder SE to fail over and make this SE the temporary root SE.
delivery-service-id		Specifies the delivery service ID to be used.
<i>delivery-service-num</i>		Delivery service number (0–4294967295).
delivery-service-name		Specifies the delivery service name descriptor to be used.
<i>name</i>		Delivery service name.
force		(Optional) Forces a failover regardless of whether the root or forwarder SE is active.
fallback		Forces the temporary root SE to become a receiver SE.
primary-ip-fallback		Triggers the downstream receiver SEs to contact a forwarder using the forwarder's primary IP address. For more information, see the “distribution primary-ip-fallback Command” section on page 2-91.
forwarder-id		Specifies the forwarder SE ID that is contacted by the receiver SE.
<i>forwarder-num</i>		Forwarder SE ID.
forwarder-name		Specifies the name of the forwarder SE that is contacted by the receiver SE.
<i>name</i>		Forwarder SE name.
refresh		Forces the redistribution of content to be refreshed on every SE.
meta-data		Forces the redistribution of metadata to be refreshed on every SE.
delivery-service-id		Specifies the delivery service ID to be used in the distribution.
<i>delivery-service-num</i>		Delivery service number (0–4294967295).
object		Forces the distribution of objects to be refreshed on every SE.
<i>object-url</i>		Specifies the object URL that needs to be refreshed on every SE.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines When the root SE fails, use the **distribution failover** EXEC command on an SE that is going to be the temporary root SE to trigger an immediate failover to the temporary root SE if you do not want to wait for the automatic failover process to occur. When you enter this command, the current SE becomes the

temporary root SE if its forwarder is an inactive root SE. If the root SE has not failed, a failover to the temporary root SE does not occur if you use the **distribution failover EXEC** command. Use the **distribution failover force** command to force a failover even if the root SE is active.

Use the **distribution fallback** command on an SE that is currently the temporary root SE to cause it to become a receiver SE.

Use the **distribution refresh meta-data {delivery-service-id delivery-service-num}** command to request that the metadata receiver repeat a previous request for all the content metadata for the specified delivery service from its forwarder SE. This method allows you to start over if the metadata receiver fails to replicate some metadata properly. The content metadata (machine-readable information that describes the characteristics of the content) must be distributed to a receiver first before the content can be replicated. The content metadata helps to define what content to retrieve, how content is retrieved, how recently the content has been updated, how the content is to be pre-positioned (for example, expiration time), and so forth. The metadata is always distributed using unicast. The content, however, can be replicated using unicast.

Use the **distribution refresh object object-url** command to reissue a request for unicast distribution of the specified object. This command lets you obtain a new copy of an object if there is a corrupted copy on the SE. After you enter this command, if the distribution is unicast, the unicast receiver reissues the request to its forwarder SE. The old content on the SE is removed and a new copy is replicated.

NACK Interval Multiplier

To identify missing content and trigger a resend of a file, receiver SEs send a negative acknowledgement (NACK) message to the sender SE. NACK messages generated by many receiver SEs could generate more traffic than the sender can handle. Cisco Internet Streamer Release 2.4 software allows you to adjust the average interval between NACKs by configuring a NACK interval multiplier for an individual receiver SE. This value (an integer between 0.1–10) adjusts the default average NACK interval (the default is 20 minutes) by the value configured as the interval multiplier. For example, if you set the NACK interval multiplier to 3, the interval between NACKs becomes 20 minutes x 3, or 60 minutes. This adjustment can be made as needed by choosing **Devices > Devices > Prepositioning > Distribution** in the CDSM GUI.

distribution primary-ip-fallback Command

When downstream receiver SEs at the edge of the network try to access a forwarder SE that is inside a NAT firewall, those receiver SEs that are inside the same NAT use one IP address (called the inside local IP address) to access the forwarder, but other receiver SEs that are outside the NAT need to use a different forwarder's IP address (called the inside global IP address or NAT address) to access the forwarder. A forwarder SE registers the IP address configured on its primary interface with the CDSM, and the CDSM uses the primary IP address for communication with devices in the CDS network. If the registered primary IP address is the inside local IP address and the forwarder is behind a NAT firewall, a receiver that is not inside the same NAT as the forwarder cannot contact it without special configuration. All other receivers inside the NAT use the inside local IP address to contact the forwarder that resides inside the NAT.

Cisco Internet Streamer Release 2.4 software supports NAT for unicast distribution (see the [“NAT Firewall” section on page 2-92](#) for more information). When the receiver SE polls its forwarder from an upstream location for the content metadata or content, the receiver first connects to the forwarder using the forwarder's primary IP address. If it fails and the forwarder's NAT address has been configured, then the unicast receiver tries to poll the forwarder using the forwarder's NAT address. If the receiver polls the forwarder successfully using the NAT address, the receiver continues to use the forwarder's NAT address during the subsequent polling intervals with the same forwarder. The unicast receiver retries to connect to the forwarder using the forwarder's primary IP address only after one hour. Even if the unicast receiver is able to poll the forwarder using the forwarder's primary IP address, it would take one hour for the receiver to fall back to the forwarder's primary IP address automatically. You can use the

distribution primary-ip-fallback command to enable the receiver that is using the NAT address of the forwarder to fall back to the primary IP address immediately, if you are certain that the forwarder's primary IP address is working.

NAT Firewall

Network Address Translation (NAT) enables private IP internetworks that use nonregistered IP addresses to connect to the Internet. NAT is configured on the firewall at the border of a stub domain (referred to as the inside network) and a public network such as the Internet (referred to as the outside network). NAT translates the internal local addresses to globally unique IP addresses before sending packets to the outside network. You can configure NAT to advertise only one address for the entire network to the outside world. This configuration provides additional security, effectively hiding the entire internal network from the world behind that address. NAT has the dual functionality of security and address conservation and is typically implemented in remote access environments.

In the inside network's domain, hosts have addresses in the one address space. While on the outside, they appear to have addresses in another address space when NAT is configured. The first address space is referred to as the local address space while the second is referred to as the global address space.

Hosts in outside networks can be subject to translation and can have local and global addresses.

NAT uses the following definitions:

- Inside local address—The IP address that is assigned to a host on the inside network. The address is probably not a legitimate IP address assigned by the Network Information Center (NIC) or service provider.
- Inside global address—A legitimate IP address (assigned by the NIC or service provider) that represents one or more inside local IP addresses to the outside world.
- Outside local address—The IP address of an outside host as it appears to the inside network. Not necessarily a legitimate address, it was allocated from an address space routable on the inside.
- Outside global address—The IP address assigned to a host on the outside network by the host's owner. The address was allocated from a globally routable address or network space.

Related Commands **show statistics distribution**

dnslookup

To resolve a host or domain name to an IP address, use the **dnslookup** EXEC command.

dnslookup {*hostname* | *domainname*}

Syntax Description	<i>hostname</i>	Name of host on the network.
	<i>domainname</i>	Name of domain.

Defaults	No default behavior or values.

Command Modes	EXEC

Examples The following examples show that the **dnslookup** command is used to resolve the hostname *myhost* to IP address 172.31.69.11, *cisco.com* to IP address 192.168.219.25, and an IP address used as a hostname to 10.0.11.0:

```
ServiceEngine#dnslookup myhost
official hostname: myhost.cisco.com
address: 172.31.69.11
```

```
ServiceEngine#dnslookup cisco.com
official hostname: cisco.com
address: 192.168.219.25
```

```
ServiceEngine#dnslookup 10.0.11.0
official hostname: 10.0.11.0
address: 10.0.11.0
```

enable

To access privileged EXEC commands, use the **enable** EXEC command.

enable

Syntax Description	This command has no arguments or keywords.

Defaults	No default behavior or values.

Command Modes	EXEC

Usage Guidelines	To access privileged EXEC mode from user EXEC mode, use the enable command. The disable command takes you from privileged EXEC mode to user EXEC mode.

Examples	The following example shows how to access privileged EXEC mode:

```
ServiceEngine>enable  
ServiceEngine#
```

Related Commands	disable exit

end

To exit global configuration mode, use the **end** global configuration command.

end

Syntax Description	This command has no arguments or keywords.

Defaults	No default behavior or values.

Command Modes	Global configuration

Usage Guidelines	Use the end command to exit global configuration mode after completing any changes to the running configuration. To save new configurations to NVRAM, use the write command. In addition, you can press Ctrl-Z to exit global configuration mode.

Examples	The following example shows how to exit global configuration mode:

```
ServiceEngine(config)#end
ServiceEngine#
```

Related Commands	exit

exec-timeout

To configure the length of time that an inactive Telnet or Secure Shell (SSH) session remains open, use the **exec-timeout** global configuration command. To revert to the default value, use the **no** form of this command.

exec-timeout *timeout*

no exec-timeout

Syntax Description	<i>timeout</i> Timeout in minutes (0–44640).
Defaults	The default is 15 minutes.
Command Modes	Global configuration
Usage Guidelines	A Telnet or SSH session with the SE can remain open and inactive for the interval of time specified by the exec-timeout command. When the exec-timeout interval elapses, the SE automatically closes the Telnet or SSH session. Configuring a timeout interval of 0 minutes by entering the exec-timeout 0 command is equivalent to disabling the session-timeout feature.
Examples	The following example configures a timeout of 100 minutes: <pre>ServiceEngine(config)#exec-timeout 100</pre> The following example negates the configured timeout of 100 minutes and reverts to the default value of 15 minutes: <pre>ServiceEngine(config)#no exec-timeout</pre>
Related Commands	telnet enable sshd

exit

To access the EXEC command shell from the global, interface, and debug configuration command shells, use the **exit** command.

exit

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC, global configuration, and interface configuration

Usage Guidelines

Use the **exit** command in any configuration mode to return to EXEC mode. Using this command is equivalent to pressing the **Ctrl-Z** key or entering the **end** command.

The **exit** command issued in the user-level EXEC shell terminates the console or Telnet session. You can also use the **exit** command to exit other configuration modes that are available from the global configuration mode for managing specific features (see the commands marked with a footnote in [Table 2-1](#)).

Examples

The following example terminates global configuration mode and returns to the privileged-level EXEC mode:

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

The following example terminates privileged-level EXEC mode and returns to the user-level EXEC mode:

```
ServiceEngine#exit
ServiceEngine>
```

Related Commands

end

external-ip

To configure up to eight external Network Address Translation (NAT) IP addresses, use the **external-ip** global configuration command. To remove the NAT IP addresses, use the **no** form of this command.

external-ip *ip-addresses*

no external-ip *ip-addresses*

Syntax Description	<i>ip-addresses</i>	A maximum of eight external or NAT IP addresses can be configured.

Defaults	No default behavior or values.

Command Modes	Global configuration

Usage Guidelines	Use this command to configure up to eight Network Address Translation IP addresses to allow the router to translate up to eight internal addresses to registered unique addresses and translate external registered addresses to addresses that are unique to the private network. If the IP address of the RTSP gateway has not been configured on the SE, then the external IP address is configured as the IP address of the RTSP gateway.

In an CDS network, there are two methods for a device registered with the CDSM (SEs, SRs, or the standby CDSM) to obtain configuration information from the primary CDSM. The primary method is for the device to periodically poll the primary CDSM on port 443 to request a configuration update. You cannot configure this port number. The backup method is when the CDSM pushes configuration updates to a registered device as soon as possible by issuing a notification to the registered device on port 443. This method allows changes to take effect in a timelier manner. You cannot configure this port number even when the backup method is being used. CDS networks do not work reliably if devices registered with the CDSM are unable to poll the CDSM for configuration updates. When a receiver SE requests the content and content metadata from a forwarder SE, it contacts the forwarder SE on port 443.

When a device (SEs at the edge of the network, SRs, and primary or standby CDSMs) is inside a NAT firewall, those devices that are inside the same NAT use one IP address (the inside local IP address) to access the device and those devices that are outside the NAT use a different IP address (the NAT IP address or inside global IP address) to access the device. A centrally managed device advertises only its inside local IP address to the CDSM. All other devices inside the NAT use the inside local IP address to contact the centrally managed device that resides inside the NAT. A device that is not inside the same NAT as the centrally managed device cannot contact it without a special configuration.

If the primary CDSM is inside a NAT, you can allow a device outside the NAT to poll it for getUpdate requests by configuring a static translation (NAT IP address or inside global IP address) for the CDSM's inside local IP address on its NAT, and using this address, rather than the CDSM's inside local IP address in the **cdsm ip ip-address** global configuration command when you register the device to the CDSM. If an SE or SR is inside a NAT and the CDSM is outside the NAT, you can allow the SE or SR to poll for getUpdate requests by configuring a static translation (NAT IP address or inside global IP address) for the SE or SR's inside local address on its NAT.

**Note**

Static translation establishes a one-to-one mapping between your inside local address and an inside global address. Static translation is useful when a host on the inside must be accessible by a fixed address from the outside.

Examples

The following example configures four external NAT IP addresses:

```
ServiceEngine(config)#external-ip 192.168.43.1 192.168.43.2 192.168.43.3 192.168.43.4
```

Related Commands

interface
ip

find-pattern

To search for a particular pattern in a file, use the **find-pattern** EXEC command.

```
find-pattern {binary filename | case {binary filename | count filename | lineno filename | match
filename | nomatch filename | recursive filename} | count filename | lineno filename | match
filename | nomatch filename | recursive filename}
```

Syntax Description	binary	Does not suppress the binary output.
	<i>filename</i>	Filename.
	case	Matches the case-sensitive pattern.
	count	Prints the number of matching lines.
	lineno	Prints the line number with output.
	match	Prints the matching lines.
	nomatch	Prints the nonmatching lines.
	recursive	Searches a directory recursively.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines Use this command to search for a particular regular expression pattern in a file.

Examples The following example searches a file recursively for a case-sensitive pattern:

```
ServiceEngine#find-pattern case recursive admin removed_core
-rw----- 1 admin root 95600640 Oct 12 10:27 /local/local1/core_dir/c
ore.2.2.1.b5.eh.2796
-rw----- 1 admin root 97054720 Jan 11 11:31 /local/local1/core_dir/c
ore.cache.5.3.0.b131.cnbuild.14086
-rw----- 1 admin root 96845824 Jan 11 11:32 /local/local1/core_dir/c
ore.cache.5.3.0.b131.cnbuild.14823
-rw----- 1 admin root 101580800 Jan 11 12:01 /local/local1/core_dir/
core.cache.5.3.0.b131.cnbuild.15134
-rw----- 1 admin root 96759808 Jan 11 12:59 /local/local1/core_dir/c
ore.cache.5.3.0.b131.cnbuild.20016
-rw----- 1 admin root 97124352 Jan 11 13:26 /local/local1/core_dir/c
ore.cache.5.3.0.b131.cnbuild.30249
-rw----- 1 admin root 98328576 Jan 11 11:27 /local/local1/core_dir/c
ore.cache.5.3.0.b131.cnbuild.8095
```

The following example searches a file for a pattern and prints the matching lines:

```
ServiceEngine#find-pattern match 10 removed_core
Tue Oct 12 10:30:03 UTC 2004
-rw----- 1 admin    root      95600640 Oct 12 10:27 /local/local1/core_dir/c
ore.5.2.1.b5.eh.2796
-rw----- 1 admin    root      101580800 Jan 11 12:01 /local/local1/core_dir/
core.cache.5.3.0.b131.cnbuild.15134
```

The following example searches a file for a pattern and prints the number of matching lines:

```
ServiceEngine#find-pattern count 10 removed_core
3
```

Related Commands

cd
dir
ls
lls

flash-media-streaming

To enable and configure Flash Media Streaming, use the **flash-media-streaming** global configuration command. To disable Flash Media Streaming, use the **no** form of this command.

On the SE:

```
flash-media-streaming {admin-api [ip {allow ip address}] | application-virtual-path vod map
mapping string | enable | max-bandwidth number | max-sessions number | monitoring enable
| non-wholesale-license-bandwidth number | wholesale-license {install number license-name
name bandwidth number start-date date duration number | no-alerts number}}
```

no flash-media-streaming

On the SR:

```
flash-media-streaming {enable | monitoring enable}
```

no flash-media-streaming

Syntax Description

admin-api	Allows accessing admin API from the IP.
ip	Allows an IP Address.
allow	Allows an IP Address
<i>ip address</i>	IP Address or hostname (input maximum 32 of partial or full IP address or hostname, such as 10.60, 10.60.1.133, or foo.com).
application-virtual-path	Configures the virtual-path for applications.
vod	Configures the virtual-path for VOD applications.
map	Maps to a directory.
<i>mapping string</i>	Mapping string.
enable	Enables Flash Media Streaming.
max-bandwidth	Configures Max-bandwidth for Flash Media streaming.
<i>number</i>	Max-bandwidth number (1000–8000000) Kbps.
max-sessions	Configures maximum sessions for Flash Media Streaming.
<i>number</i>	Maximum sessions number (1–15000).
monitoring	Configures Flash Media Streaming monitoring.
enable	Enables monitoring.
non-wholesale-license-bandwidth	Configures non-wholesale-license-bandwidth for Flash Media Streaming.
<i>number</i>	Non-wholesale-license-bandwidth number (1000–8000000) Kbps.
wholesale-license	Adds, modifies, and configures Flash Media Streaming wholesale licenses.
install	Installs wholesale licenses for Flash Media Streaming.
<i>number</i>	License sequence number (1–200).
license-name	Specifies the wholesale license name.
<i>name</i>	Name of the wholesale license.
bandwidth	Specifies the bandwidth of the wholesale license purchased.

<i>number</i>	Wholesale license bandwidth number (1000–4000000) Kbps.
start-date	Specifies the start date of the wholesale license.
<i>date</i>	The start date of the wholesale license in mm-dd-yyyy format, year between 1970 and 2037.
duration	Specifies the duration of the wholesale license, at least 1 month.
<i>number</i>	Duration of the wholesale license.
no-alerts	Disables alerts for Flash Media Streaming wholesale licenses.
<i>number</i>	License sequence number (1–200).
enable	Enables Flash Media Streaming.
monitoring	Configures Flash Media Streaming monitoring.
enable	Enables monitoring.

Defaults

No default behavior or values.

Command Modes

Global configuration

Usage Guidelines

Flash Media Streaming needs an application name (vod, live or dvrcast) as part of a client's request. In the case of a VOD application, the origin server should have a first level directory of “vod” for dynamic ingestion. For example, in a Flash Media Streaming VOD cache miss case, the request from the client should be `rtmp://cdnsecure.bbc.co.uk/vod/iplayerstreaming/secure_auth/scifi.flv`, and the origin server should have `http://cdnsecure.bbc.co.uk/vod/iplayerstreaming/secure_auth/scifi.flv`. However, this restricts customer deployments when “vod” is the only folder name they can use. Therefore, Cisco Internet Streamer Release 2.4 software contains an **application-virtual-path vod** command so customers can map to whichever folder they want on the origin server.

**Note**

The dvrcast option will be available until the 2.4.3 release.

For VOD streams, all RTMP calls in the SWF file must be in the following format:

```
rtmp://rfqdn/vod/path/foo.flv
```

In this format, *rfqdn* is the routing domain name of the Service Router, *vod* is the required directory, and *path* is the directory path to the content file that conforms to the standard URL specification.

If you are unable to store the VOD content in the required “vod” directory on your origin server, you can create a VOD virtual path for all RTMP requests. All client requests for RTMP calls still use the `rtmp://rfqdn/vod/path/foo.flv` format for VOD streams, but the SE replaces the “vod” directory with the string specified in the **flash-media-streaming application-virtual-path vod map** command.

Use the **flash-media-streaming application-virtual-path vod map <mapping string>** command on each SE participating in a Flash Media Streaming delivery service. The mapping string variable accepts all alpha-numeric characters and the slash (/) character, and can be from 1 to 128 characters. For example, to map the “vod” directory to “media” for the go-tv-stream.com origin server, use the **flash-media-streaming application-virtual-path vod map media** command. If `comedy.flv` is the content being requested, the RTMP call in the SWF file would be `rtmp://go-tv-stream.com/vod/`

comedy.flv. The SE would replace the “vod” directory and request `http://go-tv-stream.com/media/comedy.flv` from the upstream SE or origin server. If just the slash (/) character is used to replace the “vod” directory, the SE request would be `http://go-tv-stream.com/comedy.flv`.

Editing a Wholesale License

The wholesale license feature has four operations from the CLI—adding and removing licenses and enabling and disabling alerts. Users read license details from the documentation and add them to the CLI and CDSM. If a user enters a license incorrectly, the only way to edit it is to delete the license and add the it again.

Examples

The following example shows how to map a vod folder:

```
ServiceEngine(config)#flash-media-streaming application-virtual-path vod map media
```

This means mapping vod folder to media. When client request cache-miss case:

`rtmp://Tem4.se.cdsfms.com/vod/foo.flv`, will be mapped to `rtmp://Temp4.se.cdsfms.com/media/foo.flv`

```
ServiceEngine(config)#flash-media-streaming application-virtual-path vod map /
```

This means mapping vod folder to /.

When client request cache-miss case: `rtmp://Tem4.se.cdsfms.com/vod/abc/foo.flv`, will be mapped to `rtmp://Temp4.se.cdsfms.com/abc/foo.flv`

When client request cache-miss case: `rtmp://Tem4.se.cdsfms.com/vod/bar/foo.flv`, will be mapped to `rtmp://Temp4.se.cdsfms.com/bar/foo.flv`.

show flash-media-streaming

show statistics flash-media-streaming

help

To obtain online help for the command-line interface, use the **help** EXEC or global configuration command.

help

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC and global configuration.

Usage Guidelines

You can get help at any point in a command by entering a question mark (?). If nothing matches, the help list will be empty, and you must back up until entering a ? shows the available options.

Two styles of help are provided:

- Full help is available when you are ready to enter a command argument (for example, **show ?**). In addition, full help describes each possible argument.
- Partial help is provided when you enter an abbreviated command and you want to know what arguments match the input (for example, **show stat?**).

Examples

The following example shows the output of the **help** EXEC command:

```
ServiceEngine#help
```

```
Help may be requested at any point in a command by entering a question mark '?'.
```

```
Two styles of help are provided:
```

1. Full help is available when you are ready to enter a command argument.
2. Partial help is provided when an abbreviated argument is entered.

hostname

To configure the device's network hostname, use the **hostname** global configuration command. To reset the hostname to the default setting, use the **no** form of this command.

hostname *name*

no hostname

Syntax Description	<i>name</i>	New hostname for the device; the name is case sensitive. The name may be from 1 to 30 alphanumeric characters.

Defaults	The default hostname is the SE model number.

Command Modes	Global configuration

Usage Guidelines	Use this command to configure the hostname for the SE. The hostname is used for the command prompts and default configuration filenames. This name is also used by content routing and conforms to the following rules: • It can use only alphanumeric characters and hyphens (-). • The maximum length is 30 characters. • The following characters are considered illegal and cannot be used when naming a device: @, #, \$, %, ^, &, *, (), , \"/>, < >.

Examples	The following example changes the hostname to Sandbox:

```
ServiceEngine(config)#hostname Sandbox
Sandbox(config)#
```

The following example removes the hostname:

```
ServiceEngine(config)#no hostname
NO-HOSTNAME(config)#
```

Related Commands	dnslookup ip show hosts

http

To configure HTTP-related parameters, use the **http** global configuration command. To disable HTTP related-parameters, use the **no** form of this command.

http add-cookie *string*

http age-multiplier *num*

http cache-cookies

http cache-fill-range

http cache-on-abort {**enable** | **percent** *num*}

http max-ttl {**days** *num* | **hours** *num* | **minutes** *num* | **seconds** *num*}

http min-ttl *minutes*

http object max-size *maxsize*

http proxy {**incoming** *ports* | **outgoing** {**host** {*hostname* | *ip-address*} *port*}}

http reval-each-request **all**

no http

Syntax Description		
add-cookie		Add a cookie to going HTTP requests to the origin server.
<i>string</i>		Specifies string to be set as the cookie.
age-multiplier		Specifies the HTTP caching heuristic modifiers.
<i>num</i>		Expiration time of text objects as a percentage of their age (0–100).
cache-cookies		Caches the web objects with associated cookies.
cache-fill-range		Completes cache-fill for a range request starting from 0.
cache-on-abort		Sets the cache-on-abort configuration options.
enable		Enables the cache-on-abort feature.
percent		Sets the percent threshold.
<i>num</i>		Percentage value (1–99).
max-ttl		Sets the maximum Time To Live for objects in the cache.
days		Sets the maximum Time To Live for units in days.
<i>num</i>		Maximum time to live (1–1825).
hours		Sets the maximum Time To Live for units in hours.
<i>num</i>		Maximum time to live (1–43800).
minutes		Sets the maximum Time To Live for units in minutes.
<i>num</i>		Maximum time to live (1–2628000).
seconds		Sets the maximum Time To Live for units in seconds.
<i>num</i>		Maximum time to live (1–157680000).
min-ttl		Sets the minimum Time To Live for objects in the cache.

<i>minutes</i>	Minimum Time To Live in minutes (0–86400).
object	Configures HTTP objects.
max-size	Maximum size of a cacheable object in MBytes, 0 means no limit (0–2047).
<i>maxsize</i>	Maximum size of a cacheable object in kilobytes (1–2096128).
proxy	Configures the incoming proxy-mode requests.
incoming	Configures for incoming proxy-mode requests.
<i>ports</i>	Ports on which to listen for incoming HTTP, FTP, and HTTPS proxy requests (1–65535). You can specify a maximum of eight ports. The default is no incoming proxy.
outgoing	Configures the direct outgoing requests to another proxy server.
host	Uses the outgoing HTTP proxy.
<i>hostname</i>	Hostname of the outgoing proxy.
<i>ip-address</i>	IP address of the outgoing proxy.
<i>port</i>	Port number of the outgoing proxy (1–65535).
reval-each-request	Configures the revalidation for every request.
all	Revalidates all objects on every request.

Defaults

age-multiplier: 30 percent for text objects and 60 percent for binary objects

ports: no incoming proxy

days: 1 day

hours: 24 hours.

minutes: 1440 minutes.

seconds: 86400 seconds.

misses number: 0 misses

object max-size: 2 GB

outgoing monitor: 60 seconds

The SE strips the hop-to-hop 407 response sent by the Internet proxy by default.

http cache-on-abort: disabled

The default is no incoming proxy.

Command Modes

Global configuration

Usage Guidelines

Use these commands to configure specific parameters for caching HTTP objects.



Note

Text objects refer to HTML pages. Binary objects refer to all other web objects (for example, GIFs or JPEGs).

Transaction Logging

Once a user has been authenticated through LDAP or a RADIUS server, all transaction logs generated by the SE for that user contain user information. If the SE is acting in proxy mode, the user ID is included in the transaction logs. If the SE is acting in transparent mode, the user IP address is included instead.

The **cache-cookies** option enables the SE to cache the binary content served with HTTP Set-cookie headers and no explicit expiration information.

The **reval-each-request** option enables the SE to revalidate all objects requested from the cache.

Use the **object max-size** option to specify the maximum size in kilobytes of a cacheable object. The default is no maximum size for a cacheable object. The **no** form of the command resets the default value.

The **http proxy** options enable the SE to operate in environments where client browsers have previously been configured to use a legacy proxy server. The SE accepts proxy-style requests when the incoming proxy ports are configured with the **http proxy incoming ports** option. Up to eight incoming proxy ports can be specified on a single command line or on multiple command lines.

To configure the SE to direct all HTTP miss traffic to a parent cache (without using ICP), use the **http proxy outgoing host port** option, where **host** is the system name or IP address of the outgoing proxy server, and **port** is the port number designated by the outgoing (upstream) server to accept proxy requests.

Caching Policy for Client-Aborted Downloads

Typically, a client aborts a download of an object by clicking the **Stop** icon on the browser or by closing the browser during a download. By default, the SE continues to download an object to the cache even after a client aborts the download.

The **cache-on-abort** option lets you specify if and when the SE completes the download of a cacheable object after the client aborts the request. However, if the SE determines that there is another client currently requesting the same object, caching is always completed.

If the **cache-on-abort** option is enabled and no thresholds are enabled, the SE always aborts downloading an object to the cache. You can use any combination of the following thresholds, which are specified in the HTTP header. If the option is not enabled, the client receives an error response. Response errors and read errors are returned to the client, because it is not possible to detect whether these errors are generated at the origin server or at the proxy.

Examples

The following example specifies that the host 10.1.1.1 on port 8088 is designated as the primary proxy server and host 10.1.1.2 is designated as a backup proxy server:

```
ServiceEngine(config)#http proxy outgoing host 10.1.1.1 8088 primary
ServiceEngine(config)#http proxy outgoing host 10.1.1.2 220
```

The following example shows the output for the **show http proxy** command:

```
ServiceEngine#show http proxy
Incoming Proxy-Mode:
  Servicing Proxy mode HTTP connections on ports:    8080

Outgoing Proxy-Mode:
  Primary proxy server: 172.16.63.150    port 1 Failed
  Backup proxy servers: 172.16.236.151    port 8005
                        172.16.236.152    port 123
                        172.16.236.153    port 65535 Failed
                        172.16.236.154    port 10
Monitor Interval for Outgoing Proxy Servers is 60 seconds
Use of Origin Server upon Proxy Failures is disabled.
```

The following example shows the output for the **show statistics http requests** command:

```
ServiceEngine#show statistics http requests
```

```
Statistics - Requests
```

	Total	% of Requests
Total Received Requests:	49103	-
Forced Reloads:	109	0.2
Client Errors:	23	0.0
Server Errors:	348	0.7
URL Blocked:	0	0.0
Sent to Outgoing Proxy:	0	0.0
Failures from Outgoing Proxy:	0	0.0
Excluded from Outgoing Proxy:	0	0.0
ICP Client Hits:	0	0.0
ICP Server Hits:	0	0.0
HTTP 0.9 Requests:	2	0.0
HTTP 1.0 Requests:	49101	100.0
HTTP 1.1 Requests:	0	0.0
HTTP Unknown Requests:	0	0.0
Non HTTP Requests:	0	0.0
Non HTTP Responses:	46	0.1
Chunked HTTP Responses:	0	0.0
Http Miss Due To DNS:	0	0.0
Http Deletes Due To DNS:	0	0.0
Objects cached for min ttl:	2674	5.0

The following example shows the output for the **show statistics http proxy outgoing** command:

```
ServiceEngine#show statistics http proxy outgoing
```

```
HTTP Outgoing Proxy Statistics
```

IP	PORT	ATTEMPTS	FAILURES
172.16.23.150	8000	0	0
172.16.23.151	8080	0	0
172.16.23.152	9000	0	0
172.16.23.153	9001	0	0
172.16.23.154	9005	0	0

```
Requests when all proxies were failed: 0
```

The following example shows that with the default configuration (all **cache-on-abort** thresholds disabled), client abort processing is configured to always abort downloading an object to the cache:

```
ServiceEngine(config)#http cache-on-abort enable
```

The following example shows that the SE is configured to always continue downloading an object to the cache (this configuration is the default):

```
ServiceEngine(config)#no http cache-on-abort
```

The following example shows that the SE is configured to use the default minimum threshold when the **cache-on-abort** option has been enabled and the threshold is set to 16 kilobytes:

```
ServiceEngine(config)#http cache-on-abort min 16
```

The following example shows that the SE is configured to ignore the minimum threshold:

```
ServiceEngine(config)#no http cache-on-abort min
```

Related Commands

acquirer (EXEC mode)
dnslookup
ip name-server
show acquirer
show http
show http proxy
show statistics http requests

icap

To use the Internet Content Adaptation Protocol (ICAP) to help the SE interact with third-party software applications and plug-ins, use the **icap** global configuration command. To disable individual options, use the **no** form of this command.



Note

See the “[icap service](#)” section on page 2-115 for information about configuring specific ICAP services.

```
icap {append-x-headers {x-client-ip | x-server-ip} | apply rules-template | service camiant
    {enable | error-handling {bypass | return-error} | server url}
```

```
no icap {append-x-headers {x-client-ip | x-server-ip} | apply rules-template | service camiant
    {enable | error-handling {bypass | return-error} | server url}
```

Syntax Description

append-x-headers	Appends x-headers during the ICAP protocol handshake. Disabled by default. Can have multiple entries for various x-headers to be appended.
x-client-ip	Appends x-client-IP headers to the request that is sent to the ICAP server. Disabled by default.
x-server-ip	Appends x-server-IP headers to the request that is sent to the ICAP server. Disabled by default.
apply	Enables ICAP processing for HTTP requests.
rules-template	Enables ICAP processing for HTTP requests that match the rule action use-icap-service global configuration command.
service	Configures ICAP service.
camiant	Policy server for QoS.
enable	Enables ICAP service.
error-handling	Specifies the error handling option for this service.
bypass	Bypasses this service.
return-error	Returns the error to the client and ends the request.
server	Specifies the server for this service.
url	Specifies the server URL for the style.

Command Modes

Global configuration

Usage Guidelines

ICAP is an open standard for content adaptation, typically at the network edge. Content adaptation is the process of modifying the content to improve its usability. The content adaptation can include virus scanning, content translation, content filtering, content insertion, and other ways of improving the value of content for end users. ICAP specifies how an SE, acting as an HTTP proxy server, can communicate with an external device acting as an ICAP server, which filters and adapts the requested content.

ICAP provides two content-processing modes for HTTP services. These modes define the transactions that can occur between an SE acting as an ICAP client and an ICAP server. The two modes are as follows:

- Request modification (reqmod)—Allows modification of requests as they are sent from the SE to the ICAP server on their way to the origin server. The ICAP server can modify these requests depending on the services requested.
- Response modification (respmod)—Allows modification of requests after they return from the origin server. The ICAP server only acts on requested objects, after they return from the origin server.

The following is a complete list of the ICAP vendors that have been certified to interoperate with the SE:

- TrendMicro for reqmod and respmod
- Symantec for respmod

The maximum file size that is supported in the Internet Streamer CDS software is 2 GB. Files that exceed this size limit are not supported for ICAP processing.

Use the **icap append-x-headers** global configuration command to specify the ICAP extension headers that are passed to the ICAP server during the session negotiation between the SE and the ICAP server as follows:

- You can configure the SE to append the client and server IP address headers to the request that is passed to the ICAP server. This capability allows you to use your ICAP server to perform URL filtering based on the client IP address and server IP address. To enable this capability, you must use the **icap append-x-headers x-client-ip** and **icap append-x-headers x-server-ip** command options.
- You can configure the SE to append the username and group name headers to the request that is passed to the ICAP server. This capability allows you to use your ICAP server to perform URL filtering based on username and group name.

Also, you can choose to apply ICAP services on all HTTP requests processed by the SE or apply ICAP processing only to requests that match the Rules Template. Use the **icap apply {all | rules-template}** global configuration command to specify which ICAP services should be performed on which requests that are received by the SE. For example, use the **icap apply rules-template** global configuration command to instruct the SE to run only the ICAP services that match the rules action **use-icap-service**. Alternatively, you could use the **icap apply all** global configuration command to instruct the SE to run all of the ICAP services on all of the HTTP requests that it receives.

To exclude other traffic from ICAP processing, use the **rule action use-icap-service** command. The Rules Template can be used to turn off ICAP processing for various requests by applying the patterns available in the Rules Template to the incoming request. These patterns can include the following attributes of the incoming request:

- User-agent field
- Destination IP address
- Domain name

Use the **icap service** command to enter ICAP configuration mode and to configure a specific ICAP service.

Examples

The following example applies ICAP processing to all traffic:

```
ServiceEngine(config)#icap apply all
```

The following examples exclude intranet traffic from ICAP processing:

```
ServiceEngine(config)#rule pattern-list 1 domain !cisco.com
ServiceEngine(config)#rule action use-icap-service trend-reqmod 1 protocol all
ServiceEngine(config)#rule action use-icap-service trend-respmod 1 protocol all
```

```
ServiceEngine(config)#rule enable
ServiceEngine(config)#icap apply rules-template
```

The following example shows how to use the **icap service** *service-id* global configuration command to configure and enable various ICAP services on this SE:

```
ServiceEngine(config)#icap service trend-reqmod
ServiceEngine(config-icap-service)#enable
ServiceEngine(config-icap-service)#vector-point reqmod-precache
ServiceEngine(config-icap-service)#server icap//172.19.227.150/REQ-Service
ServiceEngine#exit
```

```
ServiceEngine(config)#icap service trend-respmod
ServiceEngine(config-icap-service)#enable
ServiceEngine(config-icap-service)#vector-point respmod-precache
ServiceEngine(config-icap-service)#server icap//172.19.227.150/interscan
ServiceEngine#exit
```

Related Commands

```
icap service
rule use-icap-service
show icap
show icap service
show rule action use-icap-service
```

icap service

To enter ICAP service configuration mode and configure ICAP services, enter the **icap service** global configuration command. To disable individual options, use the **no** form of this command.

icap service camiant {enable | error-handling {bypass | return-error} | server url}

no icap service camiant {enable | error-handling {bypass | return-error} | server url}

Syntax Description	
camiant	Sets the Policy Server for QoS.
enable	Enables ICAP service.
error-handling	Specifies error-handling option for this service.
bypass	Bypasses this service.
return-error	Returns error to client and end request.
server	Configures servers for this service (1 or more).
<i>url</i>	Server URL of style.

Defaults

server url: Port 1344 is assumed if no explicit port is included in the URL.

Command Modes

Global configuration

Usage Guidelines

An ICAP service defines attributes that define the service and one or more servers that provide ICAP services. You can configure a maximum of ten ICAP services on a single SE and a maximum of five ICAP servers for each ICAP service. To select the type of load balancing to use among a cluster of ICAP servers, use the **load-balancing** option.

In the syntax, replace *service-id* with a name of your choice for the current ICAP service. When you enter the **icap service** command and provide a name for the ICAP service, the system displays this ICAP service configuration prompt:

```
ServiceEngine(config-icap-service)#
```

Within ICAP service configuration mode, all commands that you enter apply to the current ICAP service. To return to global configuration mode, enter the **exit** command.

The point at which ICAP services are applied to content is called the *vectoring point*, specified using the **vector-point** option. The following three vectoring points are supported:

- Client request vectoring point (**reqmod-precache**)—The ICAP server performs one of the following actions in response to the client request:
 - Terminates the connection
 - Sends a modified error response
 - Searches the cache using the URL in the request
 - Searches the cache using a modified URL
 - Modifies the request header or request body in the case of a cache miss

- Cache miss vectoring point (**reqmod-postcache**)—The ICAP server performs one of the following actions before forwarding the request to the origin server:
 - Terminates the connection
 - Sends a modified error response
 - Sends the request to the origin server using the original URL
 - Sends the request to the origin server using an alternative URL
 - Modifies the request header or request body
- Server response vectoring point (**respmod-precache**)—The ICAP server performs one of the following actions after receiving the response from the origin server:
 - Returns the response to the client
 - Modifies the request header or request body
 - Caches the response using the original URL
 - Caches the response using an alternative URL

With the **respmod** vectoring point, which is used by virus-scanning ICAP vendors, the performance of the SE will be 300 transactions per second.

With the **reqmod-precache** vectoring point, which is used by URL filtering ICAP vendors, the performance of the SE will drop 20 percent from the rated performance.

**Note**

The performance of the SE will be limited by the performance of the ICAP server.

**Note**

Different ICAP services assigned to the same vectoring point can use different load-balancing options.

ICAP servers process HTTP requests from clients based on the ICAP services configured at various vectoring points. ICAP servers perform content adaptation such as a request or response modification and filtering of requests or responses at the configured vectoring points while processing HTTP requests.

You can configure the maximum number of connections and the weight that can be handled by an ICAP server in a cluster of servers. The weight parameter represents the load percentage that can be redirected to the ICAP server. An ICAP server with a weight of 40 denotes that this server handles 40 percent of the load. If the total weight of all ICAP servers in a load-balanced cluster exceeds 100, the load percentage for each ICAP server is recalculated as a percentage measure represented by the weight parameters.

**Note**

Always locate the ICAP server on a public LAN and configure its public IP address on the SE. The ICAP server should not be located behind a NAT device.

ICAP servers configured at various vectoring points (especially the request modification precache vectoring points) may become overloaded with HTTP requests, because all requests pass through this point. Therefore, a cluster of ICAP servers (a load-balanced collection of ICAP servers) is made available for configuration. At a particular vectoring point, you can choose to load balance requests among the ICAP cluster of servers based on various parameters such as weighted load, client IP and server IP address-based hash, or round-robin format.

More than one ICAP service can be associated with a vectoring point. An ICAP service configured at a vectoring point can have only one load-balancing scheme, irrespective of the number of servers. However, multiple ICAP services configured at one or all of the vectoring points can have different load-balancing schemes.

To identify the specific ICAP server and service, use the **server url** command, where the URL is in the following format:

icap://ICAPserverIPAddress/service-name

The value used for the *service-name* must match the identifier used by the specific ICAP vendor. For example, one vendor uses the service name REQ-Service for **reqmod-precache** and interscan for **respmod-precache**, while another vendor supports only **respmod-precache** and uses the service name avscan.

When ICAP processing is enabled and an HTTP browser with a streaming Java applet is opened, several undesirable things occur as follows:

- The data for the Java applet is not updated in the browser. For example, when viewing a stock investment website, a user would not see any streaming stock updates.
- The ICAP daemon on the SE continues to send updates (from the HTTP response) to the ICAP server, which overloads the ICAP server.

These conditions occur because the ICAP server is set up to inspect the entire data packet before delivering a response to the client. However, because there is a streaming request, the data continues flowing to the ICAP server indefinitely, deadlocking any response to the requesting client.

Two workarounds are available. You can configure the ICAP server to bypass the scanning process, or you can configure rules on the SE to skip ICAP processing on websites that are known to contain streaming Java applets.

To configure the ICAP server to bypass scanning, use rules such as `client_skip_content` or `server_skip_content` as follows:

- The `client_skip_content` rule bypasses scanning on the basis of an HTTP request. The software looks for patterns in the HTTP header and bypasses all requests that exactly match the patterns specified in the `intscan.ini` file as follows:

```
client_skip_content=User Agent: Windows Media Player 9.0.1
```

- The `server_skip_content` rule bypasses scanning on the basis of an HTTP response. The software looks for patterns in the HTTP header and bypasses all responses that exactly match the patterns specified in the `intscan.ini` file as follows:

```
server_skip_content=Content-Type: X-Dave_Content
```

Alternatively, you can configure the SE to bypass ICAP processing based on user agents or any of the patterns available in the Rules Template, by using the **rule** command.

Examples

The following examples show a typical configuration for a virus scanning service that requires processing on two vectoring points (**reqmod-precache** and **respmod-precache**):

```
ServiceEngine(config)#icap apply all
ServiceEngine(config)#icap service trend-reqmod
ServiceEngine(config-icap-service)#enable
ServiceEngine(config-icap-service)#vector-point reqmod-precache
ServiceEngine(config-icap-service)#server icap://172.19.227.150/REQ-Service
ServiceEngine#exit
ServiceEngine#icap service trend-respmod
ServiceEngine(config-icap-service)#enable
```

```
ServiceEngine(config-icap-service)#vector-point respmod-precache
ServiceEngine(config-icap-service)#server icap://172.19.227.150/interscan
ServiceEngine#exit
```

The following example shows that if an ICAP vendor supports the same service name for more than one vectoring point, you can configure a single service and add the supported vectoring points:

```
ServiceEngine(config)#icap service myicap-service
ServiceEngine(config-icap-service)#enable
ServiceEngine(config-icap-service)#vector-point reqmod-precache
ServiceEngine(config-icap-service)#vector-point respmod-precache
ServiceEngine(config-icap-service)#server icap://172.19.227.150/icap-service-name
ServiceEngine(config-icap-service)#exit
ServiceEngine(config)#
```

The following example shows that the SE is configured to bypass ICAP processing on the intranet site cisco.com and on the trusted Internet site datek.com:

```
SE(config)#rule enable
SE(config)#rule action use-icap-service trend-reqmod pattern-list 1 protocol all
SE(config)#rule action use-icap-service trend-respmod pattern-list 1 protocol all
SE(config)#rule pattern-list 1 domain !(*cisco\.com|.*datek\.com)!
SE(config)#icap apply rules-template
SE(config)#icap service trend-reqmod
SE(config-icap-service)#enable
SE(config-icap-service)#vector-point reqmod-precache
SE(config-icap-service)#server icap://172.19.227.150/REQ-Service
SE(config-icap-service)#exit
SE(config)#icap service trend-respmod
SE(config-icap-service)#enable
SE(config-icap-service)#vector-point respmod-precache
SE(config-icap-service)#server icap://172.19.227.150/interscan
SE(config-icap-service)#exit
```

Related Commands

```
icap
rule use-icap-service
show icap
show icap service
show rule action use-icap-service
```

install

To install the Internet Streamer CDS software image, use the **install** EXEC command.

install *imagefilename*

Syntax Description

<i>imagefilename</i>	Name of the .bin file that you want to install.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

The **install** command loads the system image into flash memory and the disk.

To install a system image, copy the image file to the sysfs directory local1 or local2. Before entering the **install** command, change the present working directory to the directory where the system image resides. When the **install** command is executed, the image file is expanded. The expanded files overwrite the existing files in the SE. The newly installed version takes effect after the system image is reloaded.

**Note**

The **install** command does not accept .pax files. Files should be of the .bin type (for example, CDS-2.2.1.7-K9.bin). Also, if the release being installed does not require a new system image, then it may not be necessary to write to flash memory. If the newer version has changes that require a new system image to be installed, then the **install** command may result in a write to flash memory.

Examples

The following example shows how to install a .bin file on the SE:

```
ServiceEngine#install CDS-2.2.1.7-K9.bin
```

Related Commands

copy ftp install
copy http install
reload

interface

To configure a Gigabit Ethernet or port-channel interface, use the **interface** global configuration command. To disable selected options, restore default values, or enable a shutdown interface, use the **no** form of this command.

```

interface GigabitEthernet slot/port

interface PortChannel {1 | 2}

interface standby group number

no interface {GigabitEthernet slot/port | PortChannel {1 | 2} | Standby group number}
```

Syntax Description

GigabitEthernet	Selects a Gigabit Ethernet interface to configure.
<i>slot/port</i>	Slot and port number for the selected interface. The slot range is 0–12; the port range is 0–0. The slot number and port number are separated with a forward slash character (/).
PortChannel	Selects the EtherChannel of interfaces to configure.
1	Sets the port-channel interface number to 1.
2	Sets the port-channel interface number to 2.
Standby	Sets the standby group for the interface.
<i>group number</i>	Group number for the selected interface. The group number range is 1–4.

Defaults

No default behavior or values.

Command Modes

Global configuration

Usage Guidelines

Configuring Interfaces for DHCP

During the initial configuration of an SE, you have the option of configuring a static IP address for the SE or using interface-level DHCP to dynamically assign IP addresses to the interfaces on the SE.

If you do not enable interface-level DHCP on the SE, you must manually specify a static IP address and network mask for the SE. If the SE moves to another location in another part of the network, you must manually enter a new static IP address and network mask for this SE.

An interface can be enabled for DHCP by using the **ip address dhcp** [*client_id* | *hostname*] interface configuration command. The client identifier is an ASCII value. The SE sends its configured client identifier and hostname to the DHCP server when requesting network information. DHCP servers can be configured to identify the client identifier information and the hostname information that the SE is sending and then send back the specific network settings that are assigned to the SE.

String to Be Set as Cookie Port-Channel (EtherChannel) Interface

EtherChannel for the Internet Streamer CDS Release 2.x software supports the grouping of up to four same- network interfaces into one virtual interface. This grouping allows the setting or removing of a virtual interface that consists of two Gigabit Ethernet interfaces. EtherChannel also provides

interoperability with Cisco routers, switches, and other networking devices or hosts supporting EtherChannel, load balancing, and automatic failure detection and recovery based on each interface's current link status.

You can use the Gigabit Ethernet ports to form an EtherChannel. A physical interface can be added to an EtherChannel subject to the device configuration.

Examples

The following example creates an EtherChannel. The port channel is port channel 2 and is assigned an IP address of 10.10.10.10 and a netmask of 255.0.0.0:

```
ServiceEngine# configure
ServiceEngine(config)# interface PortChannel 2
ServiceEngine(config-if)# exit
```

The following example removes an EtherChannel:

```
ServiceEngine(config)# interface PortChannel 2
ServiceEngine(config-if)# exit
ServiceEngine(config)# no interface PortChannel 2
```

The following example shows a sample output of the **show running-config EXEC** command:

```
ServiceEngine# show running-config
.
.
.
interface GigabitEthernet 0/0
  description This is an interface to the WAN
  ip address dhcp
  ip address 192.168.1.200 255.255.255.0
bandwidth 100
exit
.
.
```

The following example shows the sample output of the **show interface** command:

```
ServiceEngine# show interface GigabitEthernet 1/0
Description: This is the interface to the lab
type: Ethernet
```

The following example shows how to create standby groups on SEs:

```
ServiceEngine(config)#interface GigabitEthernet 1/0 standby 2 priority 300
ServiceEngine(config)#interface GigabitEthernet 2/0 standby 2 priority 200
ServiceEngine(config)#interface GigabitEthernet 3/0 standby 2 priority 100
ServiceEngine(config)#interface standby 2 errors 10000
```

Related Commands

show interface
show running-config
show startup-config

ip

To change initial network device configuration settings, use the **ip** global configuration command. To delete or disable these settings, use the **no** form of this command. The **dscp** option allows you to set the global Type of Service (ToS) or differentiated services code point (DSCP) values in IP packets.

ip default-gateway *ip-address*

ip domain-name *name1 name2 name3*

ip dscp { **client** { **cache-hit** { **match-server** | **set-dscp** *dscp-packets* | **set-tos** *tos-packets* } | **cache-miss** { **match-server** | **set-dscp** *dscp-packets* | **set-tos** *tos-packets* } } | **server** { **match-client** | **set-dscp** *dscp-packets* | **set-tos** *tos-packets* } }

ip name-server *ip-addresses*

ip path-mtu-discovery **enable**

ip route *dest_addrs net_addrs gateway_addrs*

no ip { **default-gateway** | **domain-name** | **dscp** { **client** { **cache-hit** | **cache-miss** } | **server** } | **name-server** *ip-addresses* | **path-mtu-discovery** **enable** | **route** *dest_addrs net_addrs gateway_addrs* }

Syntax Description

default-gateway	Specifies the default gateway (if not routing IP).
<i>ip-address</i>	IP address of the default gateway.
domain-name	Specifies domain names.
<i>name1</i> through <i>name3</i>	Domain name (up to three can be specified).
dscp	Configures IP differentiated services code point (DSCP) and Type of Service (ToS) fields.
client	Configures DSCP for responses to the client.
cache-hit	Configures the cache hit responses to the client.
cache-miss	Configures the cache miss responses to the client.
match-server	Uses the original ToS/DSCP value of the server.
set-dscp	Configures differentiated services code point (DSCP) values.
<i>dscp-packets</i>	DSCP values; see Table 2-5 on page 2-124 for valid values.
set-tos	Configures Type of Service (ToS).
<i>tos-packets</i>	ToS value; see Table 2-7 on page 2-128 for valid values.
server	Configures DSCP for outgoing requests.
match-client	Uses the original ToS/DSP value of the client.
name-server	Specifies the address of the name server.
<i>ip-addresses</i>	IP addresses of the name servers (up to a maximum of eight).
path-mtu-discovery	Configures RFC 1191 Path Maximum Transmission Unit (MTU) discovery.
enable	Enables Path MTU discovery.
route	Specifies the net route.

<i>dest_addrs</i>	Destination route address.
<i>net_addrs</i>	Netmask address.
<i>gateway_addrs</i>	Gateway address.

Defaults

No default behavior or values.

Command Modes

Global configuration

Usage Guidelines

To define a default gateway, use the **ip default-gateway** command. Only one default gateway can be configured. To remove the IP default gateway, use the **no** form of this command. The SE uses the default gateway to route IP packets when there is no specific route found to the destination.

To define a default domain name, use the **ip domain-name** command. To remove the IP default domain name, use the **no** form of this command. Up to three domain names can be entered. If a request arrives without a domain name appended in its hostname, the proxy tries to resolve the hostname by appending *name1*, *name2*, and *name3* in that order until one of these names succeeds.

The SE appends the configured domain name to any IP hostname that does not contain a domain name. The appended name is resolved by the DNS server and then added to the host table. The SE must have at least one domain name server specified for hostname resolution to work correctly.

To specify the address of one or more name servers to use for name and address resolution, use the **ip name-server ip-addresses** command. To disable IP name servers, use the **no** form of this command. For proper resolution of the hostname to the IP address or the IP address to the hostname, the SE uses DNS servers. Use the **ip name-server** command to point the SE to a specific DNS server. You can configure up to eight servers.

Path MTU autodiscovery discovers the MTU and automatically sets the correct value. Use the **ip path-mtu-discovery enable** command to start this autodiscovery utility. By default, this feature is enabled. When this feature is disabled, the sending device uses a packet size that is smaller than 576 bytes and the next hop MTU. Existing connections are not affected when this feature is turned on or off.

The Cisco Internet Streamer CDS software supports IP Path MTU Discovery, as defined in RFC 1191. When enabled, Path MTU Discovery discovers the largest IP packet size allowable between the various links along the forwarding path and automatically sets the correct value for the packet size. By using the largest MTU that the links will bear, the sending device can minimize the number of packets that it must send.

**Note**

IP Path MTU Discovery is useful when a link in a network goes down, forcing the use of another, different MTU-sized link. IP Path MTU Discovery is also useful when a connection is first being established and the sender has no information at all about the intervening links.

IP Path MTU Discovery is initiated by the sending device. If a server does not support IP Path MTU Discovery, the receiving device will have no mechanism available to avoid fragmenting datagrams generated by the server.

Use the **ip route** command to add a specific static route for a network or host. Any IP packet designated for the specified destination uses the configured route.

To configure static IP routing, use the **ip route** command. To remove the route, use the **no** form of this command. Do not use the **ip route 0.0.0.0 0.0.0.0** command to configure the default gateway; use the **ip default-gateway** command instead.

In the CDS network, you can configure SEs, SRs, and CDSMs for the Type of Service (ToS) or differentiated services code point (DSCP) using the **ip dscp** command.

Differentiated Services

The differentiated services (DiffServ) architecture is based on a simple model where traffic entering a network is classified and possibly conditioned at the boundaries of the network. The class of traffic is then identified with a differentiated services (DS) code point or bit marking in the IP header. Within the core of the network, packets are forwarded according to the per-hop behavior associated with the DS code point.

To set the global ToS or DSCP values for the IP header from the CLI, use the **ip dscp** command.

DiffServ describes a set of end-to-end QoS (Quality of Service) capabilities. End-to-end QoS is the ability of the network to deliver service required by specific network traffic from one end of the network to another. QoS in the Internet Streamer CDS software supports differentiated services.

With differentiated services, the network tries to deliver a particular kind of service based on the QoS specified by each packet. This specification can occur in different ways, for example, using the 6-bit DSCP setting in IP packets or source and destination addresses. The network uses the QoS specification to classify, mark, shape, and police traffic, and to perform intelligent queueing.

Differentiated services is used for several mission-critical applications and for providing end-to-end QoS. Typically, differentiated services is appropriate for aggregate flows because it performs a relatively coarse level of traffic classification.

Use the **ip dscp {client | server} {cache-hit | cache-miss} set-dscp dscp-packets** command to set the DSCP values for the IP header. Valid values for *dscp-packets* are listed in [Table 2-5](#).

Table 2-5 *dscp-packets Values*

Value or Keyword	Description ¹
0–63	Sets DSCP values.
af11	Sets packets with AF11 DSCP (001010).
af12	Sets packets with AF12 DSCP (001100).
af13	Sets packets with AF13 DSCP (001110).
af21	Sets packets with AF21 DSCP (010010).
af22	Sets packets with AF22 DSCP (010100).
af23	Sets packets with AF23 DSCP (010110).
af31	Sets packets with AF31 DSCP (011010).
af32	Sets packets with AF32 DSCP (011100).
af33	Sets packets with AF33 DSCP (011110).
af41	Sets packets with AF41 DSCP (100010).
af42	Sets packets with AF42 DSCP (100100).
af43	Sets packets with AF43 DSCP (100110).
cs1	Sets packets with CS1 (precedence 1) DSCP (001000).
cs2	Sets packets with CS2 (precedence 2) DSCP (010000).

Table 2-5 *dscp-packets Values (continued)*

Value or Keyword	Description ¹
cs3	Sets packets with CS3 (precedence 3) DSCP (011000).
cs4	Sets packets with CS4 (precedence 4) DSCP (100000).
cs5	Sets packets with CS5 (precedence 5) DSCP (101000).
cs6	Sets packets with CS6 (precedence 6) DSCP (110000).
cs7	Sets packets with CS7 (precedence 7) DSCP (111000).
default	Sets packets with the default DSCP (000000).
ef	Sets packets with EF DSCP (101110).

1. The number in parentheses denotes the DSCP value for each per-hop behavior keyword.

DS Field Definition

A replacement header field, called the DS field, is defined by differentiated services. The DS field supersedes the existing definitions of the IPv4 ToS octet (RFC 791) and the IPv6 traffic class octet. Six bits of the DS field are used as the DSCP to select the Per Hop Behavior (PHB) at each interface. A currently unused (CU) 2-bit field is reserved for explicit congestion notification (ECN). The value of the CU bits is ignored by DS-compliant interfaces when determining the PHB to apply to a received packet.

Per-Hop Behaviors

RFC 2475 defines PHB as the externally observable forwarding behavior applied at a DiffServ-compliant node to a DiffServ Behavior Aggregate (BA).

With the ability of the system to mark packets according to the DSCP setting, collections of packets that have the same DSCP setting and that are sent in a particular direction can be grouped into a BA. Packets from multiple sources or applications can belong to the same BA.

A PHB refers to the packet scheduling, queueing, policing, or shaping behavior of a node on any given packet belonging to a BA, as configured by a service level agreement (SLA) or a policy map.

There are four available standard PHBs as follows:

- Default PHB (as defined in RFC 2474)
- Class-Selector PHB (as defined in RFC 2474)
- Assured Forwarding (AFny) PHB (as defined in RFC 2597)
- Expedited Forwarding (EF) PHB (as defined in RFC 2598)

The following sections describe the PHBs.

Default PHB

The default PHB specifies that a packet marked with a DSCP value of 000000 (recommended) receives the traditional best-effort service from a DS-compliant node (a network node that complies with all of the core DiffServ requirements). Also, if a packet arrives at a DS-compliant node, and the DSCP value is not mapped to any other PHB, the packet gets mapped to the default PHB.

Class-Selector PHB

To preserve backward compatibility with any IP precedence scheme currently in use on the network, DiffServ has defined a DSCP value in the form xxx000, where x is either 0 or 1. These DSCP values are called Class-Selector Code Points. (The DSCP value for a packet with default PHB 000000 is also called the Class-Selector Code Point.)

The PHB associated with a Class-Selector Code Point is a Class-Selector PHB. These Class-Selector PHBs retain most of the forwarding behavior as nodes that implement IP precedence-based classification and forwarding.

For example, packets with a DSCP value of 110000 (the equivalent of the IP precedence-based value of 110) have preferential forwarding treatment (for scheduling, queueing, and so on), as compared to packets with a DSCP value of 100000 (the equivalent of the IP precedence-based value of 100). These Class-Selector PHBs ensure that DS-compliant nodes can coexist with IP precedence-based nodes.

Assured Forwarding PHB

Assured Forwarding PHB is nearly equivalent to Controlled Load Service, which is available in the integrated services model. AFny PHB defines a method by which BAs can be given different forwarding assurances.

For example, network traffic can be divided into the following classes:

- Gold—Traffic in this category is allocated 50 percent of the available bandwidth.
- Silver—Traffic in this category is allocated 30 percent of the available bandwidth.
- Bronze—Traffic in this category is allocated 20 percent of the available bandwidth.

The AFny PHB defines four AF classes: AF1, AF2, AF3, and AF4. Each class is assigned a specific amount of buffer space and interface bandwidth according to the SLA with the service provider or policy map.

Within each AF class, you can specify three drop precedence (dP) values: 1, 2, and 3. Assured Forwarding PHB can be expressed as shown in the following example: AFny. In this example, n represents the AF class number (1, 2, or 3) and y represents the dP value (1, 2, or 3) within the AFn class.

In instances of network traffic congestion, if packets in a particular AF class (for example, AF1) need to be dropped, packets in the AF1 class will be dropped according to the following guideline:

$$dP(AFny) \geq dP(AFnz) \geq dP(AFnx)$$

where dP (AFny) is the probability that packets of the AFny class will be dropped and y denotes the dP within an AFn class.

In the following example, packets in the AF13 class will be dropped before packets in the AF12 class, which in turn will be dropped before packets in the AF11 class:

$$dP(AF13) \geq dP(AF12) \geq dP(AF11)$$

The dP method penalizes traffic flows within a particular BA that exceed the assigned bandwidth. Packets on these offending flows could be re-marked by a policer to a higher drop precedence.

An AFx class can be denoted by the DSCP value, xyzab0, where xyz can be 001, 010, 011, or 100, and ab represents the dP value.

Table 2-6 lists the DSCP value and corresponding dP value for each AF PHB class.

Table 2-6 DSCP Values and Corresponding Drop Precedence Values for Each AF PHB Class

Drop Precedence	Class 1	Class 2	Class 3	Class 4
Low drop precedence	001010	010010	011010	100010
Medium drop precedence	001100	010100	011100	100100
High drop precedence	001110	010110	011110	100110

Expedited Forwarding PHB

Resource Reservation Protocol (RSVP), a component of the integrated services model, provides a guaranteed bandwidth service. Applications, such as Voice over IP (VoIP), video, and online trading programs, require this type of service. The EF PHB, a key ingredient of DiffServ, supplies this kind of service by providing low loss, low latency, low jitter, and assured bandwidth service.

You can implement EF by using priority queueing (PQ) and rate limiting on the class (or BA). When implemented in a DiffServ network, EF PHB provides a virtual leased line or premium service. For optimal efficiency, however, you should reserve EF PHB for only the most critical applications because, in instances of traffic congestion, it is not feasible to treat all or most traffic as high priority.

EF PHB is suited for applications such as VoIP that require low bandwidth, guaranteed bandwidth, low delay, and low jitter.

IP Precedence for ToS

IP precedence allows you to specify the class of service (CoS) for a packet. You use the three precedence bits in the IPv4 header's type of service (ToS) field for this purpose.

Using the ToS bits, you can define up to six classes of service. Other features configured throughout the network can then use these bits to determine how to treat the packet. These other QoS features can assign appropriate traffic-handling policies including congestion management strategy and bandwidth allocation. For example, although IP precedence is not a queueing method, queueing methods such as weighted fair queueing (WFQ) and Weighted Random Early Detection (WRED) can use the IP precedence setting of the packet to prioritize traffic.

By setting precedence levels on incoming traffic and using them with the Internet Streamer CDS software QoS queueing features, you can create differentiated service. You can use features, such as policy-based routing (PBR) and Committed Access Rate (CAR), to set the precedence based on an extended access list classification. For example, you can assign the precedence based on the application or user or by destination and source subnetwork.

So that each subsequent network element can provide service based on the determined policy, IP precedence is usually deployed as close to the edge of the network or the administrative domain as possible. IP precedence is an edge function that allows core or backbone QoS features, such as WRED, to forward traffic based on CoS. You can also set IP precedence in the host or network client, but this setting can be overridden by the service provisioning policy of the domain within the network.

The following QoS features can use the IP precedence field to determine how traffic is treated:

- Distributed-WRED
- WFQ
- CAR

How the IP Precedence Bits Are Used to Classify Packets

You use the three IP precedence bits in the ToS field of the IP header to specify a CoS assignment for each packet. You can partition traffic into up to six classes—the remaining two classes are reserved for internal network use—and then use policy maps and extended ACLs to define network policies in terms of congestion handling and bandwidth allocation for each class.

Each precedence corresponds to a name. These names, which continue to evolve, are defined in RFC 791. The numbers and their corresponding names, are listed from least to most important.

IP precedence allows you to define your own classification mechanism. For example, you might want to assign the precedence based on an application or an access router. IP precedence bit settings 96 and 112 are reserved for network control information, such as routing updates.

The IP precedence field occupies the three most significant bits of the ToS byte. Only the three IP precedence bits reflect the priority or importance of the packet, not the full value of the ToS byte.

Use the **ip dscp {client | server} {cache-hit | cache-miss} set-tos tos-packets** command to specify either of the two arguments—IP precedence or ToS byte value—to set the same ToS. You may specify either the ToS byte value or IP precedence; one is required. IP precedence uses the three precedence bits in the ToS field of the IPv4 header to specify the class of service for each packet. The ToS byte in the IP header defines the three high-order bits as IP precedence bits and the five low-order bits as ToS bits. The ToS byte value is written to the five low-order bits (bits 0 to 4) of the ToS byte in the IP header of a packet. The IP precedence value is written to the three high-order bits (bits 5 to 7) of the ToS byte in the IP header of a packet.

The following is a list of precedence names:

- **critical**
- **flash**
- **flash-override**
- **immediate**
- **internet**
- **network**
- **priority**
- **routine**

The following is a list of ToS names:

- **max-reliability**
- **max-throughput**
- **min-delay**
- **min-monetary-cost**
- **normal**

Valid values for *tos-packets* are listed in [Table 2-7](#).

Table 2-7 *tos-packets Values*

Value, Precedence, or ToS Name	Description ¹
0–127	Sets the ToS value.
critical	Sets packets with critical precedence (80).
flash	Sets packets with flash precedence (48).
flash-override	Sets packets with flash override precedence (64).
immediate	Sets packets with immediate precedence (32).
internet	Sets packets with internetwork control precedence (96).
max-reliability	Sets packets with maximum reliable ToS (2).
max-throughput	Sets packets with maximum throughput ToS (4).
min-delay	Sets packets with minimum delay ToS (8).
min-monetary-cost	Sets packets with minimum monetary cost ToS (1).
network	Sets packets with network control precedence (112).

Table 2-7 *tos-packets Values (continued)*

Value, Precedence, or ToS Name	Description ¹
normal	Sets packets with normal ToS (0).
priority	Sets packets with priority precedence (16).

1. The number in parentheses denotes the ToS value for each IP precedence or ToS name setting.

Examples

The following example configures a default gateway for the SE:

```
ServiceEngine(config)#ip default-gateway 192.168.7.18
```

The following example disables the default gateway:

```
ServiceEngine(config)#no ip default-gateway
```

The following example configures a static IP route for the SE:

```
ServiceEngine(config)#ip route 172.16.227.128 255.255.255.0 172.16.227.250
```

The following example negates the static IP route:

```
ServiceEngine(config)#no ip route 172.16.227.128 255.255.255.0 172.16.227.250
```

The following example configures a default domain name for the SE:

```
ServiceEngine(config)#ip domain-name cisco.com
```

The following example negates the default domain name:

```
ServiceEngine(config)#no ip domain-name
```

The following example configures a name server for the SE:

```
ServiceEngine(config)#ip name-server 10.11.12.13
```

The following example disables the name server:

```
ServiceEngine(config)#no ip name-server 10.11.12.13
```

Related Commands

show ip route

ip access-list

To create and modify access lists for controlling access to interfaces or applications, use the **ip access-list standard** or **ip access-list extended** global configuration commands. To remove access control lists, use the **no** form of this command.

```
ip access-list { extended {acl-name | acl-num {delete num | deny { num { ip address | any | host} | gre {ip address | any | host} | icmp{ip address | any | host} | ip {ip address | any | host} | tcp {ip address | any | host} | udp {ip address | any | host}} | insert {num {deny | permit} | list {start-line-num | end-line-num} | move {old-line-num | new-line-num} | permit {num {ip address | any | host} | gre {ip address | any | host} | icmp{ip address | any | host} | ip {ip address | any | host} | tcp {ip address | any | host} | udp {ip address | any | host}} } | {standard {acl-num | acl-name {delete num | deny {num {ip address | any | host} | gre {ip address | any | host} | icmp{ip address | any | host} | ip {ip address | any | host} | tcp {ip address | any | host} | udp {ip address | any | host}} | insert {num {deny | permit} | list {start-line-num | end-line-num} | move {old-line-num | new-line-num} | permit {ip address | any | host}} } }
```

```
no ip access-list {extended {acl-name | acl-num {delete num | deny {num {ip address | any | host} | gre {ip address | any | host} | icmp{ip address | any | host} | ip {ip address | any | host} | tcp {ip address | any | host} | udp {ip address | any | host}} | insert {num {deny | permit} | list {start-line-num | end-line-num} | move {old-line-num | new-line-num} | permit {num {ip address | any | host} | gre {ip address | any | host} | icmp{ip address | any | host} | ip {ip address | any | host} | tcp {ip address | any | host} | udp {ip address | any | host}} } | {standard {acl-num | acl-name {delete num | deny {num {ip address | any | host} | gre {ip address | any | host} | icmp{ip address | any | host} | ip {ip address | any | host} | tcp {ip address | any | host} | udp {ip address | any | host}} | insert {num {deny | permit} | list {start-line-num | end-line-num} | move {old-line-num | new-line-num} | permit {ip address | any | host}} } }
```

Syntax Description

standard	Enables the standard ACL configuration mode.
<i>acl-num</i>	Access list to which all commands entered from access list configuration mode apply, using a numeric identifier. For standard access lists, the valid range is 1 to 99; for extended access lists, the valid range is 100 to 199.
<i>acl-name</i>	Access list to which all commands entered from ACL configuration mode apply, using an alphanumeric string of up to 30 characters, beginning with a letter.
delete	(Optional) Deletes the specified entry.
<i>num</i>	(Optional) Position of condition to delete (1–500).
deny	(Optional) Causes packets that match the specified conditions to be dropped.
<i>num</i>	An IP Protocol Number.
<i>ip address</i>	Source IP address.
<i>any</i>	Any source host.
<i>host</i>	A single host address.
gre	Cisco's GRE Tunneling.
icmp	Internet Control Message Protocol.
ip	Any IP Protocol.
tcp	Transport Control Protocol.

udp	User Datagram Protocol.
insert	(Optional) Inserts the conditions following the specified line number into the access list.
<i>num</i>	Identifies the position at which to insert a new condition.
deny	Specifies packets to deny.
permit	Specifies packets to permit.
list	(Optional) Lists the specified entries (or all entries when none are specified).
<i>start-line-num</i>	(Optional) Line number from which the list begins.
<i>end-line-num</i>	(Optional) Last line number in the list.
move	(Optional) Moves the specified entry in the access list to a new position in the list.
<i>old-line-num</i>	Line number of the entry to move.
<i>new-line-num</i>	New position of the entry. The existing entry is moved to the following position in the access list.
permit	(Optional) Causes packets that match the specified conditions to be accepted for further processing.
extended	Enables the extended ACL configuration mode.

Defaults

An access list drops all packets unless you configure at least one **permit** entry.

Command Modes

Global configuration

Usage Guidelines**Standard ACL Configuration Mode Commands**

To work with a standard access list, enter the **ip access-list standard** command from the global configuration mode prompt. The CLI enters a configuration mode in which all subsequent commands apply to the current access list.

To add a line to the standard IP ACL, enter the following command:

For example, choose a purpose (permit or deny) that specifies whether a packet is to be passed or dropped, enter the source IP address, and enter the source IP wildcard address as follows:

```
[insert line-num] {deny | permit} {source-ip [wildcard] | host source-ip | any}
```

To delete a line from the standard IP ACL, enter the following command:

```
delete line-num
```

To display a list of specified entries within the standard IP ACL, enter the following command:

```
list [start-line-num [end-line-num]]
```

To move a line to a new position within the standard IP ACL, enter the following command:

```
move old-line-num new-line-num
```

To return to the CLI global configuration mode prompt, enter the following command:

exit

To negate a standard IP ACL, enter the following command:

no {deny | permit} {source-ip [wildcard] | host source-ip | any}

Extended ACL Configuration Mode Commands

To work with an extended access list, enter the **ip access-list extended** command from the global configuration mode prompt. The CLI enters a configuration mode in which all subsequent commands apply to the current access list.

To delete a line from the extended IP ACL, enter the following command:

delete line-num

To move a line to a new position within the extended IP ACL, enter the following command:

move old-line-num new-line-num

To display a list of specified entries within the standard IP ACL, enter the following command:

list [start-line-num [end-line-num]]

To return to the CLI global configuration mode prompt, enter the following command:

exit

To add a condition to the extended IP ACL, note that the options depend on the chosen protocol.

For IP, enter the following command to add a condition:

[insert line-num] {deny | permit} {gre | ip | proto-num} {source-ip [wildcard] | host source-ip | any} {dest-ip [wildcard] | host dest-ip | any}

no {deny | permit} {gre | ip | proto-num} {source-ip [wildcard] | host source-ip | any} {dest-ip [wildcard] | host dest-ip | any}

where if you enter *proto-num* is 47 or 0, they represent the equivalent value for GRE or IP.

For TCP, enter the following command to add a condition:

[insert line-num] {deny | permit} {tcp | proto-num} {source-ip [wildcard] | host source-ip | any} [operator port [port]] {dest-ip [wildcard] | host dest-ip | any} [operator port [port]] [established]

no {deny | permit} {tcp | proto-num} {source-ip [wildcard] | host source-ip | any} [operator port [port]] {dest-ip [wildcard] | host dest-ip | any} [operator port [port]] [established]

where *proto-num* can be 6, which is the equivalent value for TCP.

For UDP, enter the following command to add a condition:

[insert line-num] {deny | permit} {udp | proto-num} {source-ip [wildcard] | host source-ip | any} [operator port [port]] {dest-ip [wildcard] | host dest-ip | any} [operator port [port]]

```
no {deny | permit} {udp | proto-num} {source-ip [wildcard] | host source-ip | any} [operator port
[port]] {dest-ip [wildcard] | host dest-ip | any} [operator port [port]]
```

where *proto-num* can be 17, which is the equivalent value for UDP.

For ICMP, enter the following command to add a condition:

```
[insert line-num] {deny | permit} {icmp | proto-num} {source-ip [wildcard] | host source-ip | any}
{dest-ip [wildcard] | host dest-ip | any} [icmp-type [code] | icmp-msg]
```

```
no {deny | permit} {icmp | proto-num} {source-ip [wildcard] | host source-ip | any} {dest-ip
[wildcard] | host dest-ip | any} [icmp-type [code] | icmp-msg]
```

where *proto-num* can be 2, which is the equivalent value for ICMP.

For extended IP ACLs, the **wildcard** keyword is required if the **host** keyword is not specified. For a list of the keywords that you can use to match specific ICMP message types and codes, see [Table 2-10](#). For a list of supported UDP and TCP keywords, see [Table 2-8](#) and [Table 2-9](#).

Use access lists to control access to specific applications or interfaces on an SE. An access control list consists of one or more condition entries that specify the kind of packets that the SE will drop or accept for further processing. The SE applies each entry in the order in which it occurs in the access list, which by default, is the order in which you configured the entry.

The following are some examples of how IP ACLs can be used in environments that have SEs:

- An SE resides on the customer premises and is managed by a service provider, and the service provider wants to secure the device for its management only.
- An SE is deployed anywhere within the enterprise. As with routers and switches, the administrator wants to limit Telnet, SSH, and SE GUI access to the IT source subnets.
- An application layer proxy firewall with a hardened outside interface has no ports exposed. (*Hardened* means that the interface carefully restricts which ports are available for access, primarily for security reasons. With an outside interface, many types of security attacks are possible.) The SE's outside address is Internet global, and its inside address is private. The inside interface has an IP ACL to limit Telnet, SSH, and SE GUI access to the SE.
- An SE is deployed as a reverse proxy in an untrusted environment. The SE administrator wishes to allow only port 80 inbound traffic on the outside interface and outbound connections on the back-end interface.

Within ACL configuration mode, you can use the editing commands (**list**, **delete**, and **move**) to display the current condition entries, to delete a specific entry, or to change the order in which the entries are evaluated. To return to global configuration mode, enter **exit** at the ACL configuration mode prompt.

To create an entry, use a **deny** or **permit** keyword and specify the type of packets that you want the SE to drop or to accept for further processing. By default, an access list denies everything because the list is terminated by an implicit **deny any** entry. You must include at least one **permit** entry to create a valid access list.

After creating an access list, you can include the access list in an access group using the **access-group** command, which determines how the access list is applied. You can also apply the access list to a specific application using the appropriate command. A reference to an access list that does not exist is the equivalent of a **permit any** condition statement.

To work with access lists, enter either the **ip access-list standard** or **ip access-list extended** global configuration command. Identify the new or existing access list with a name up to 30 characters long beginning with a letter or with a number. If you use a number to identify a standard access list, it must be between 1 and 99; for an extended access list, use a number from 100 to 199. You must use a standard access list for providing access to the SNMP server or to the TFTP gateway/server.

After you identify the access list, the CLI enters the appropriate configuration mode and all subsequent commands apply to the specified access list.

ip access-list standard Command

You typically use a standard access list to allow connections from a host with a specific IP address or from hosts on a specific network. To allow connections from a specific host, use the **permit host** *source-ip* option and replace *source-ip* with the IP address of the specific host.

To allow connections from a specific network, use the **permit source-ip wildcard** option. Replace *source-ip* with a network ID or the IP address of any host on the network that you want to specify. Replace *wildcard* with the dotted decimal notation for a mask that is the reverse of a subnet mask, where a 0 indicates a position that must be matched and a 1 indicates a position that does not matter. For instance, the wildcard 0.0.0.255 causes the last eight bits in the source IP address to be ignored. Therefore, the **permit 192.168.1.0 0.0.0.255** entry allows access from any host on the 192.168.1.0 network.

ip access-list extended Command

Use an extended access list to control connections based on the destination IP address or based on the protocol type. You can combine these conditions with information about the source IP address to create more restrictive conditions. [Table 2-8](#) lists the UDP keywords that you can use with extended access lists.

Table 2-8 UDP Keywords and Port Numbers

CLI Keyword	Description	UDP Port Number
bootpc	Bootstrap Protocol (BOOTP) client service	68
bootps	Bootstrap Protocol (BOOTP) server service	67
domain	Domain Name System (DNS) service	53
netbios-dgm	NetBIOS datagram service	138
netbios-ns	NetBIOS name resolution service	137
netbios-ss	NetBIOS session service	139
nfs	Network File System service	2049
ntp	Network Time Protocol settings	123
snmp	Simple Network Management Protocol service	161
snmptrap	SNMP traps	162
tftp	Trivial File Transfer Protocol service	69

[Table 2-9](#) lists the TCP keywords that you can use with extended access lists.

Table 2-9 TCP Keywords and Port Numbers

CLI Keyword	Description	TCP Port Number
domain	Domain Name System	53
exec	Remote process execution	512
ftp	File Transfer Protocol service	21
ftp-data	FTP data connections (used infrequently)	20

Table 2-9 TCP Keywords and Port Numbers (continued)

CLI Keyword	Description	TCP Port Number
nfs	Network File System service applications	2049
rtsp	Real-Time Streaming Protocol applications	554
ssh	Secure Shell login	22
telnet	Remote login using telnet	23
www	World Wide Web (HTTP) service	80

Table 2-10 lists the keywords that you can use to match specific ICMP message types and codes.

Table 2-10 Keywords for ICMP Message Type and Code

Field	Description
administratively-prohibited	Messages that are administratively prohibited from being allowed access.
alternate-address	Messages that specify alternate IP addresses.
conversion-error	Messages that denote a datagram conversion error.
dod-host-prohibited	Messages that signify a Department of Defense (DoD) protocol Internet host denial.
dod-net-prohibited	Messages that specify a DoD protocol network denial.
echo	Messages that are used to send echo packets to test basic network connectivity.
echo-reply	Messages that are used to send echo reply packets.
general-parameter-problem	Messages that report general parameter problems.
host-isolated	Messages that indicate that the host is isolated.
host-precedence-unreachable	Messages that have been received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 3 (Host Unreachable). This is the most common response. Large numbers of this datagram type on the network are indicative of network difficulties or may be indicative of hostile actions.
host-redirect	Messages that specify redirection to a host.
host-tos-redirect	Messages that specify redirection to a host for type of service-based (ToS) routing.
host-tos-unreachable	Messages that denote that the host is unreachable for ToS-based routing.
host-unknown	Messages that specify that the host or source is unknown.
host-unreachable	Messages that specify that the host is unreachable.
information-reply	Messages that contain domain name replies.
information-request	Messages that contain domain name requests.
mask-reply	Messages that contain subnet mask replies.
mask-request	Messages that contain subnet mask requests.
mobile-redirect	Messages that specify redirection to a mobile host.

Table 2-10 **Keywords for ICMP Message Type and Code (continued)**

Field	Description
net-redirect	Messages that are used for redirection to a different network.
net-tos-redirect	Messages that are used for redirection to a different network for ToS-based routing.
net-tos-unreachable	Messages that specify that the network is unreachable for the ToS-based routing.
net-unreachable	Messages that specify that the network is unreachable.
network-unknown	Messages that denote that the network is unknown.
no-room-for-option	Messages that specify the requirement of a parameter, but that no room is unavailable for it.
option-missing	Messages that specify the requirement of a parameter, but that parameter is not available.
packet-too-big	Messages that specify that the ICMP packet requires fragmentation but the Do Not Fragment (DF) bit is set.
parameter-problem	Messages that signify parameter-related problems.
port-unreachable	Messages that specify that the port is unreachable.
precedence-unreachable	Messages that specify that host precedence is not available.
protocol-unreachable	Messages that specify that the protocol is unreachable.
reassembly-timeout	Messages that specify a timeout during reassembling of packets.
redirect	Messages that have been received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 5 (Redirect). ICMP redirect messages are used by routers to notify the hosts on the data link that a better route is available for a particular destination.
router-advertisement	Messages that contain ICMP router discovery messages called router advertisements.
router-solicitation	Messages that are multicast to ask for immediate updates on neighboring router interface states.
source-quench	Messages that have been received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 4 (Source Quench). This datagram may be used in network management to provide congestion control. A source quench packet will be issued when a router is beginning to lose packets due to the transmission rate of a source. The source quench is a request to the source to reduce the rate of a datagram transmission.
source-route-failed	Messages that specify the failure of a source route.
time-exceeded	Messages that specify information about all instances when specified times were exceeded.
timestamp-reply	Messages that contain time-stamp replies.
timestamp-request	Messages that contain time-stamp requests.
traceroute	Messages that specify the entire route to a network host from the source.

Table 2-10 **Keywords for ICMP Message Type and Code (continued)**

Field	Description
ttl-exceeded	Messages that specify that ICMP packets have exceeded the Time-To-Live configuration.
unreachable	Messages that are sent when packets are denied by an access list; these packets are not dropped in the hardware but generate the ICMP-unreachable message.

Examples

The following example shows how to create an access list to allow all web traffic and to only allow a specific host administrative access using Secure Shell (SSH):

```
ServiceEngine(config)#ip access-list extended example
ServiceEngine(config-ext-nacl)#permit tcp any any eq www
ServiceEngine(config-ext-nacl)#permit tcp host 10.1.1.5 any eq ssh
ServiceEngine(config-ext-nacl)#exit
```

The following example shows how to activate the access list for an interface:

```
ServiceEngine(config)#interface gigabitEthernet 1/0
ServiceEngine(config-if)#exit
```

The following example shows how this configuration appears when you enter the **show running-configuration** command:

```
...
!
ip access-list extended example
 permit tcp any any eq www
 permit tcp host 10.1.1.5 any eq ssh
 exit
...

```

Related Commands

```
clear ip access-list counters
show ip access-list
```

ipv6

To specify the default gateway's IPv6 address, use the **ipv6** global configuration command. To disable the IPv6 address, use the **no** form of this command.

ipv6 default-gateway *ip-address*

no ipv6 default-gateway *ip-address*

Syntax Description	default-gateway	Specifies the default gateway's IPv6 address.
	ip-address	IPv6 address of the default gateway.

Defaults	No default behavior or values.

Command Modes	Global configuration

Examples	The following example shows how to configure an IPv6-related address: <pre>ServiceEngine(config)#ipv6 default-gateway fec0::100/64</pre>

Related Commands	show ipv6 traceroute6

kernel kdb

To enable access to the kernel debugger (kdb), use the **kernel kdb** global configuration command. To disable the kernel debugger, use the **no** form of this command.

kernel kdb

no kernel kdb

Syntax Description

This command has no arguments or keywords.

Defaults

kdb is disabled by default.

Command Modes

Global configuration

Usage Guidelines

Once enabled, kdb is automatically activated when kernel problems occur. Once activated, all normal functioning of the CDS device is suspended until kdb is manually deactivated. The kdb prompt looks like this prompt:

```
[0] kdb>
```

To deactivate kdb, enter **go** at the kdb prompt. If kdb was automatically activated because of kernel problems, you must reboot to recover from the issue. If you activated kdb manually for diagnostic purposes, the system resumes normal functioning in whatever state it was when you activated kdb. In either case, if you enter **reboot**, the system restarts and normal operation resumes.

With the Internet Streamer CDS software earlier than Release 2.4, kdb is enabled by default and cannot be disabled. In the Release 2.0.3 and later releases, kdb is disabled by default and you must enter the **kernel kdb** command in global configuration mode to enable it. If kdb has been previously enabled, you can enter the **no kernel kdb** global configuration command to disable it.

When kdb is enabled, you can activate it manually from the local console. With Internet Streamer CDS Release 2.4, you can activate it by pressing **Esc-KDB** (press Escape and then press KDB in capitalization).

Examples

The following example shows how to enable kdb:

```
ServiceEngine(config)#kernel kdb
```

The following example shows how to disable kdb:

```
ServiceEngine(config)#no kernel kdb
```

line

To specify terminal line settings, use the **line** global configuration command. To disable terminal line settings, use the **no** form of this command.

line console carrier-detect

no line console carrier-detect

Syntax Description

console	Configures the console terminal line settings.
carrier-detect	Sets the device to check the carrier detect signal before writing to the console.

Defaults

This feature is disabled by default.

Command Modes

Global configuration

Usage Guidelines

You should enable carrier detection if you connect the SE, SR, or CDSM to a modem for receiving calls. If you are using a null-modem cable with no carrier detect pin, the device might appear unresponsive on the console until the carrier detect signal is asserted. To recover from a misconfiguration, you should reboot the device and set the 0x2000 bootflag to ignore the Carrier Detect (CD) setting.

Examples

The following example shows how to specify terminal line settings:

```
ServiceEngine(config)#line console carrier-detect
```

lls

To view a long list of directory names, use the **lls** EXEC command.

lls [*directory*]

Syntax Description	<i>directory</i> (Optional) Name of the directory for which you want a long list of files.

Defaults	No default behavior or values.

Command Modes	EXEC

Usage Guidelines	This command provides detailed information about files and subdirectories stored in the present working directory (including size, date, time of creation, sysfs name, and long name of the file). This information can also be viewed with the dir command.

Examples	The following example shows how to view a long list of directory names:

```
ServiceEngine#lls
      size      time of last change      name
-----
  4096 Mon Jan 10 14:02:26 2005 <DIR>    WebsenseEnterprise
  4096 Mon Jan 10 14:02:26 2005 <DIR>    Websense_config_backup
10203 Mon Feb 28 04:24:53 2005          WsInstallLog
  4096 Wed Feb 9 00:59:48 2005 <DIR>    core_dir
  4096 Mon Jan 10 13:49:27 2005 <DIR>    crash
   382 Tue Mar 1 03:32:13 2005          crka.log
  1604 Tue Feb 22 03:55:04 2005          dbupgrade.log
  4096 Mon Jan 10 14:02:31 2005 <DIR>    downgrade
  4096 Mon Feb 28 04:17:32 2005 <DIR>    errorlog
53248 Tue Mar 1 03:01:53 2005 <DIR>    logs
16384 Mon Jan 10 13:49:26 2005 <DIR>    lost+found
   438 Tue Jan 11 05:37:57 2005          new_file.xml
  8192 Tue Mar 1 00:00:00 2005 <DIR>    preload_dir
  4096 Tue Mar 1 03:26:00 2005 <DIR>    sa
40960 Tue Mar 1 03:32:15 2005 <DIR>    service_logs
  4096 Tue Feb 22 03:51:25 2005 <DIR>    smartfilter
384802 Mon Feb 28 03:46:00 2005          syslog.txt
16296 Mon Feb 21 04:42:12 2005          test
  4096 Mon Jan 10 14:02:24 2005 <DIR>    var
  4096 Sat Feb 12 07:15:23 2005 <DIR>    wmt_vod
```

Related Commands	dir
	ls

logging

To configure system logging, use the **logging** global configuration command. To disable logging functions, use the **no** form of this command.

logging {**console** {**enable** | **priority** *loglevel*} | **disk** {**enable** | **filename** *filename* | **priority** *loglevel* | **recycle** *size*} | **facility** *facility* | **host** {*hostname* | *ip-address*} [**port** *port_num* | **priority** *loglevel* | **rate-limit** *message_rate*]}

no logging {**console** {**enable** | **priority**} | **disk** [**enable** | **filename** | **priority** | **recycle**] | **facility** | **host** {*hostname* | *ip-address*} [**port** *port_num* | **priority** *loglevel* | **rate-limit** *message_rate*]}

Syntax Description

console	Sets system logging to a console.
enable	Enables system logging to a console.
priority	Sets which priority level messages to send to a syslog file.
<i>loglevel</i>	Use one of the following keywords:
alert	Immediate action needed. Priority 1.
critical	Immediate action needed. Priority 2.
debug	Debugging messages. Priority 7.
emergency	System is unusable. Priority 0.
error	Error conditions. Priority 3.
information	Informational messages. Priority 6.
notice	Normal but significant conditions. Priority 5.
warning	Warning conditions. Priority 4.
disk	Sets system logging to a disk file.
enable	Enables system logging to a disk file.
filename	Sets the name of the syslog file.
<i>filename</i>	Specifies the name of the syslog file.
recycle	Overwrites the <i>syslog.txt</i> when it surpasses the recycle size.
<i>size</i>	Size of the syslog file in bytes (1000000–50000000).
facility	Sets the facility parameter for syslog messages.
<i>facility</i>	Use one of the following keywords:
auth	Authorization system.
daemon	System daemons.
kernel	Kernel.
local0	Local use.
local1	Local use.
local2	Local use.
local3	Local use.
local4	Local use.
local5	Local use.
local6	Local use.
local7	Local use.

mail	Mail system.
news	USENET news.
syslog	Syslog itself.
user	User process.
uucp	UUCP system.
host	Sets the system logging to a remote host.
<i>hostname</i>	Hostname of the remote syslog host. Specifies up to four remote syslog hosts. Note To specify more than one syslog host, use multiple command lines; specify one host per command.
<i>ip-address</i>	IP address of the remote syslog host. Specifies up to four remote syslog hosts. Note To specify more than one syslog host, use multiple command lines; specify one host per command.
port	(Optional) Specifies the port to be used when logging to a host.
<i>port_num</i>	Port to be used when logging to a host. The default port is 514.
priority	(Optional) Sets the priority level for messages when logging messages to a host. The default priority is warning.
<i>loglevel</i>	Use one of the following keywords:
alert	Immediate action needed. Priority 1.
critical	Immediate action needed. Priority 2.
debug	Debugging messages. Priority 7.
emergency	System is unusable. Priority 0.
error	Error conditions. Priority 3.
information	Informational messages. Priority 6.
notice	Normal but significant conditions. Priority 5.
warning	Warning conditions. Priority 4.
rate-limit	(Optional) Sets the rate limit (in messages per second) for sending messages to a host.
<i>message_rate</i>	Rate limit (in messages per second) for sending messages to the host. (0–10000). Setting the rate limit to 0 disables rate limiting.

Defaults

Logging: on
 Priority of message for console: warning
 Priority of message for log file: debug
 Priority of message for a host: warning
 Log file: /local1/syslog.txt
 Log file recycle size: 10,000,000 bytes

Command Modes

Global configuration

Usage Guidelines

Use the **logging** command to set specific parameters of the system log file. System logging is always enabled internally on the SE. The system log file is located on the sysfs partition as /local1/syslog.txt. This file contains the output from many of the CDS components running on the SE, such as authentication entries, privilege levels, administrative details, and diagnostic output during the boot process.

To view information about events that have occurred in all devices in your CDS network, you can use the system message log feature. When a problem occurs in the CDS network, use the system message logs to diagnose and correct such problems.

The syslog.txt file on the CDSM contains information about events that have occurred on the CDSM and not on the registered nodes. The messages written to the syslog.txt file depend on specific parameters of the system log file that you have set using the **logging** global configuration command. For example, a critical error message logged on a registered node does not appear in the syslog.txt file on the CDSM because the problem never occurred on the CDSM but occurred only on the registered node. However, such an error message will be displayed in the syslog.txt file on the registered node.

A disk failure syslog message is generated every time that a failed sector is accessed. Support for filtering multiple syslog messages for a single failed sector on an IDE disk was added. Support for filtering multiple syslog messages for a single failed section for SCSI disks and SATA disks exists.

To configure the SE to send varying levels of event messages to an external syslog host, use the **logging host** option. Logging can be configured to send various levels of messages to the console using the **logging console priority** option.

The **no logging disk recycle size** command sets the file size to the default value. Whenever the current log file size surpasses the recycle size, the log file is rotated. The log file cycles through at most five rotations, and they are saved as [log file name].[1-5] under the same directory as the original log. The rotated log file is the one configured using the **logging disk filename** command.

Configuring System Logging to Remote Syslog Hosts

Cisco Internet Streamer Release 2.4 software, supported logging to only a single remote syslog host, and the following two commands is used to configure a single remote syslog host for an SE:

```
ServiceEngine(config)#logging host hostname
ServiceEngine(config)#logging priority priority
```

You can configure an SE to send varying levels of messages to up to four remote syslog hosts. To accommodate this, **logging host priority priority** global configuration command (shown above) is deprecated, and the **logging host hostname** global configuration command is extended as follows:

```
ServiceEngine(config)#[no] logging host hostname [priority priority-code | port port
| rate-limit limit]
```

where the following is true:

- *hostname* is the hostname or IP address of the remote syslog host. Specify up to four remote syslog hosts. To specify more than one syslog host, use multiple command lines; specify one host per command.
- *priority-code* is the severity level of the message that should be sent to the specified remote syslog host. The default priority-code is “warning” (level 4). Each syslog host can receive a different level of event messages.

**Note**

You can achieve syslog host redundancy by configuring multiple syslog hosts on the SE and assigning the same priority code to each configured syslog host (for example, assigning a priority code of “critical” level 2 to syslog host 1, syslog host 2, and syslog host 3).

- *port* is the destination port of the remote syslog host to which the SE is to send the messages. The default port is port 514. In releases prior to the Internet Streamer CDS Release 2.x software, you could not change the default port. Syslog messages were only sent to port 514 on the specified syslog host.
- *rate-limit* specifies the number of messages that are allowed to be sent to the remote syslog host per second. To limit bandwidth and other resource consumption, messages to the remote syslog host can be rate limited. If this limit is exceeded, messages to the specified remote syslog host are dropped. There is no default rate limit, and by default all syslog messages are sent to all of the configured syslog hosts. If the rate limit is exceeded, a message of the day (MOTD) will be printed for any CLI EXEC shell login.

Mapping syslog Priority Levels to RealProxy Error Codes

The RealProxy system generates error messages and writes them to the RealProxy log file. These error messages are captured by the caching application and passed to the system log file. A one-to-one mapping exists between the RealProxy error codes and the syslog priority levels.

Examples

The following example shows that the SE is configured to send messages that have a priority code of “error” (level 3) to the console:

```
ServiceEngine(config)#logging console priority warnings
```

The following example shows that the SE is configured to disable sending of messages that have a priority code of “error” (level 3) to the console:

```
ServiceEngine(config)#no logging console warnings
```

The following example shows that the SE is configured to send messages that have a priority code of “error” (level 3) to the remote syslog host that has an IP address of 172.31.2.160:

```
ServiceEngine(config)# logging host 172.31.2.160 priority error
```

Related Commands

clear logging
debug
show logging

ls

To view a list of files or subdirectory names within a directory, use the **ls** EXEC command.

ls [*directory*]

Syntax Description	<i>directory</i> (Optional) Name of the directory for which you want a list of files.
Defaults	No default behavior or values.
Command Modes	EXEC
Usage Guidelines	To list the filenames and subdirectories within a particular directory, use the ls <i>directory</i> command; to list the filenames and subdirectories of the current working directory, use the ls command. To view the present working directory, use the pwd command.
Examples	The following example displays a list of files within the current working directory: <pre>ServiceEngine#ls /local1</pre> The following example displays a list of files within the /local1 directory: <pre>ServiceEngine#ls /local1 core_dir crash errorlog logs lost+found service_logs smartfilter syslog.txt</pre>
Related Commands	dir lls pwd

mkdir

To create a directory, use the **mkdir** EXEC command.

mkdir *directory*

Syntax Description	<i>directory</i> Name of the directory to create.
Defaults	No default behavior or values.
Command Modes	EXEC
Usage Guidelines	Use this command to create a new directory or subdirectory in the SE file system.
Examples	The following example shows how to create a new directory under local1: <pre>ServiceEngine#mkdir /local1/mydir</pre>
Related Commands	dir lls ls pwd rmdir

mkfile

To create a new file, use the **mkfile** EXEC command.

mkfile *filename*

Syntax Description

<i>filename</i>	Name of the file that you want to create.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Use this command to create a new file in any directory of the SE.

Examples

The following example shows how to create a new file:

```
ServiceEngine#mkfile traceinfo
```

Related Commands

lls
ls
mkdir

movie-streamer

To enable and configure the Movie Streamer server, use the **movie-streamer** global configuration command. To disable the Movie Streamer, use the **no** form of this command.

movie-streamer accelerate vod enable

movie-streamer advanced {**client** {**idle-timeout** *num* | **rtp-timeout**} | **origin server idle-interval** *num*}

movie-streamer broadcast port-list *num port num*

movie-streamer cache {**age-multiplier** *num* | **enable** | **max-ttl** {**days** *num* | **hours** *num* | **minutes** *num* | **seconds** *num*} | **reval-each-request**}

movie-streamer enable

movie-streamer max-concurrent-sessions *num*

movie-streamer proxy outgoing rtsp host *ip address port num*

movie-streamer transport-src-address *ip address*

no movie streamer {**accelerate vod enable** | **advanced** {**client** {**idle-timeout** *num* | **rtp-timeout**} | **origin server idle-interval** *num*} | **broadcast port-list** *num port num* | **cache** {**age-multiplier** *num* | **enable** | **max-ttl** {**days** *num* | **hours** *num* | **minutes** *num* | **seconds** *num*} | **reval-each-request**} | **enable** | **max-concurrent-sessions** *num* | **proxy outgoing rtsp host** *ip address port num* | **transport-src-address** *ip address*}

Syntax Description

accelerate	Configures Movie Streamer kernel streaming acceleration.
vod	Configures kernel streaming acceleration for VOD.
enable	Enables kernel streaming acceleration.
advanced	Configures Movie Streamer Advanced features.
client	Configures advanced client features.
idle-timeout	Sets the RTSP timeout.
<i>num</i>	Client idle timeout in seconds (0-300).
rtp-timeout	Sets the RTP timeout.
origin-server	Configures the advanced origin server.
idle-interval	Sets the origin server idle interval.
<i>num</i>	Server idle interval in seconds (1-10).
broadcast	Configures the Movie Streamer live broadcast.
port-list	Specifies a port list.
<i>num</i>	Broadcast list number (1-1024).
<i>port num</i>	Broadcast port number.
cache	Configures the Movie Streamer cache.
age-multiplier	Sets the Movie Streamer cache heuristic modifier.
<i>num</i>	Expiration time as a percentage of their age (0-100).

enable	Enables the Movie Streamer media cache.
max-ttl	Sets the maximum time to live for objects in the cache
days	Specifies the maximum time to live units in days.
<i>num</i>	Maximum time to live (1-1825).
hours	Specifies the maximum time to live units in hours.
<i>num</i>	Maximum time to live (1-43800).
minutes	Specifies the maximum time to live units in minutes.
<i>num</i>	Maximum time to live (1-2628000).
seconds	Specifies the maximum time to live units in seconds.
<i>num</i>	Maximum time to live (1-157680000).
reval-each-request	Sets the scope of revalidation for the request.
enable	Enables the Movie Streamer.
max-concurrent-sessions	Specifies the Movie Streamer maximum concurrent sessions.
<i>num</i>	The maximum concurrent sessions (1-16000).
proxy	Configures the Movie Streamer proxy.
outgoing	Configures the Outgoing proxy.
rtsp	Configures the Outgoing RTSP proxy.
host	Specifies the outgoing proxy server.
<i>ip address</i>	IP address of outgoing proxy server.
<i>port num</i>	Port number of outgoing proxy server (1-65535).
transport-src-address	Specifies the source IP address to be set in transport header (useful if behind NAT).
<i>ip address</i>	Source IP address in transport header.

Defaults

days: 1 day
hours: 72 hours
minutes: 4320 minutes
seconds: 259200 seconds

Command Modes

Global configuration

Usage Guidelines

The **movie-streamer accelerate vod enable** command enables kernel streaming acceleration for VOD. The **movie-streamer advanced client** command sets the RTSP or RTP timeout value.

The **movie-streamer advanced origin-server** command sets the origin-server idle-interval value, which can determine the origin-server RTP timeout value.

The Idle Timeout field and the **movie-streamer advanced client idle-timeout** command (as well as the **movie-streamer advanced client rtp-timeout** command), are only intended for performance testing when using certain testing tools that do not have full support of the RTCP receiver report. Setting these timeouts to high values causes inefficient tear-down of client connections when the streaming sessions have ended.

For typical deployments, it is preferable to leave these parameters set to their defaults. The default is 60. The **movie-streamer advanced client idle-timeout** command has a range from 0 to 300, whereas the Idle Timeout field has a range from 30-180. This is by design.

Examples

The following example shows how to set the original server interval:

```
ServiceEngine(config)#movie-streamer advanced origin-server idle-interval 5
```

The following example shows how to set the broadcast port list:

```
ServiceEngine(config)#movie-streamer broadcast port-list 1 5000 5002
```

The following example shows how to set the expiration time as a percentage of the age:

```
ServiceEngine(config)#movie-streamer cache age-multiplier 50
```

The following example shows how to set the content cache maximum TTL:

```
ServiceEngine(config)#movie-streamer cache max-ttl days 100
```

The following example shows how to set the maximum concurrent sessions:

```
ServiceEngine(config)#movie-streamer max-concurrent-sessions 7000
```

The following example shows how to set the outgoing proxy:

```
ServiceEngine(config)#movie-streamer proxy outgoing rtsp host 10.74.61.98 554
```

The following example shows how to set the source IP of the transport header while behind NAT:

```
ServiceEngine(config)#movie-streamer transport-src-address 10.74.61.99
```

The following example shows how to set the client timeout:

```
ServiceEngine(config)#movie-streamer advanced client idle-timeout 150
```

The following example shows how to set the RPT time out:

```
ServiceEngine(config)#movie-streamer advanced client rtp-timeout 150
```

Set original server interval is 5 second

```
ServiceEngine(config)#movie-streamer advanced origin-server idle-interval 5
```

Set broadcast port list

```
SPCDN-QA-35(config)#movie-streamer broadcast port-list 1 5000 5002
```

Set Expiration time as a percentage of their age's 50%

```
SPCDN-QA-35(config)#movie-streamer cache age-multiplier 50
```

Set cache content max ttl is 100 days

```
SPCDN-QA-35(config)#movie-streamer cache max-ttl days 100
```

Set max con-current sessions is 7000

```
SPCDN-QA-35(config)#movie-streamer max-concurrent-sessions 7000
```

Set out going proxy

```
SPCDN-QA-35(config)#movie-streamer proxy outgoing rtsp host 10.74.61.98 554
```

Set the source Ip of transport header while behind NAT

```
SPCDN-QA-35(config)#movie-streamer transport-src-address 10.74.61.99
```

Related Commands

show movie-streamer
show statistics movie-streamer

mtu

To set the interface maximum transmission unit (MTU) packet size, use the `mtu` interface configuration command. Use the `no` form of this command to reset the MTU packet size.

mtu **mtusize**

no mtu **mtusize**

Syntax Description	<i>mtusize</i> MTU packet size in bytes (576-1500).
Command Default	The default MTU packet size for an Ethernet interface is 1500 bytes.
Command Modes	Interface configuration
Usage Guidelines	The MTU is the largest size of IP datagram that can be transferred using a specific data link connection. Use the <code>mtu</code> command to set the maximum packet size in bytes.
Examples	The following example sets the MTU packet size as 1500 bytes: <pre>ServiceEngine(config-if)#mtu 1500</pre> The following example resets the MTU packet size: <pre>ServiceEngine(config-if)#no mtu 1500</pre>
Related Commands	<pre>show interface show running-config show startup-config</pre>

no (global configuration)

To undo a global configuration command or set its defaults, use the **no** form of a global configuration command.

no *command*



Note

The commands you can use with a CDS device (including the **no** form of each command) vary based on whether the device is configured as a CDSM, SE, or SR. See [Table 2-1 on page 2-2](#) to identify the commands available for a specific device.

Syntax Description

<i>command</i>	Specifies the command type; see the “ Usage Guidelines ” section for valid values.

Defaults

No default behavior or values.

Command Modes

Global configuration

Usage Guidelines

Valid values for *command* are as follows:

aaa	Configures authentication, authorization, and accounting (AAA).
access-lists	Configures access control list entries.
acquirer	Configures acquisition parameters.
asset	Configures the asset tag name string.
authentication	Configures the authentication.
bandwidth	Configures bandwidth controls.
bitrate	Configures the bit rate.
cdsm	Configures the CDSM settings.
clock	Configures the time-of-day clock.
cms	Configures the Centralized Management System (CMS).
device	Configures the device mode.
dns	Configures the SE DNS cache.
exec-timeout	Configures the EXEC timeout.
external-ip	Configures up to eight external (NAT) IP addresses.
ftp	Configures FTP caching-related parameters.
help	Configures the assistance for the command-line interface.
hostname	Configures the system’s network name.
http	Configures HTTP-related parameters.
icap	Configures the ICAP feature for the HTTP protocol.

interface	Configures a Gigabit Ethernet interface.
ip	Configures IP parameters.
ip access-list	Configures IP access lists.
kernel	Enables access to the kernel debugger.
ldap	Configures Lightweight Directory Access Protocol (LDAP) parameters.
logging	Configures the system logging (syslog).
network-filesystem	Configures the network file system server and client.
ntp	Configures the Network Time Protocol (NTP).
offline-operation	Configures the offline service operation.
pace	Configures the HTTP pacing bandwidth and bit rate.
port-channel	Configures port-channel global options.
primary-interface	Configures a primary interface.
radius-server	Configures RADIUS server authentication.
rtsp	Configures Real-Time Streaming Protocol (RTSP)-related parameters.
rule	Configures the Rules Template.
snmp-server	Configures the SNMP server.
sshd	Configures the Secure Shell (SSH) service.
tcp	Configures global TCP parameters.
telnet enable	Configures Telnet services.
transaction-logs	Configures the transaction logging.
username	Establishes username authentication.
wmt	Configures Windows Media Technologies (WMT) parameters .

Use the **no** command to disable functions or negate a command. If you need to negate a specific command, such as the default gateway IP address, you must include the specific string in your command, such as **no ip default-gateway *ip-address***.

no (interface configuration)

To negate a Gigabit Ethernet or port-channel interface configuration command or set its defaults, use the **no** interface configuration command.

no interface { **GigabitEthernet** *slot/port* | **PortChannel** { **1** | **2** } | **Standby** *group num* }

Syntax Description	GigabitEthernet	Selects a Gigabit Ethernet interface to configure.
	<i>slot/port</i>	Slot and port number for the selected interface. The slot range is 0–2; the port range is 0–3. The slot number and port number are separated with a forward slash character (/).
	PortChannel	Selects the EtherChannel of interfaces to configure.
	1	Sets the port-channel interface number to 1.
	2	Sets the port-channel interface number to 2.
	Standby	Sets the standby group for the interface.
	<i>group num</i>	Group number for the selected interface. The group number range is 1-4.

Defaults No default behavior or values.

Command Modes Interface configuration

Related Commands

- interface**
- show interface**
- show running-config**
- show startup-config**

ntp

To configure the Network Time Protocol (NTP) server and to allow the system clock to be synchronized by a time server, use the **ntp** global configuration command. To disable this function, use the **no** form of this command.

ntp server {*ip-address* | *hostname*} [*ip-addresses* | *hostnames*]

no ntp server {*ip-address* | *hostname*} [*ip-addresses* | *hostnames*]

Syntax Description

server	Sets the NTP server IP address.
<i>ip-address</i>	NTP server IP address.
<i>hostname</i>	NTP server hostname.
<i>ip-addresses</i>	(Optional) IP address of the time server providing the clock synchronization (maximum of four).
<i>hostnames</i>	(Optional) Hostname of the time server providing the clock synchronization (maximum of four).

Defaults

No default behavior or values.

Command Modes

Global configuration

Usage Guidelines

Use this command to synchronize the SE, SR or CDSM clock with the specified NTP server. The **ntp server** command enables NTP servers for timekeeping purposes and is the only way to synchronize the system clock with a time server.

When you synchronize the CDSM clock with an NTP server, there is a possibility of all devices registered with the CDSM being shown as offline and then reverted to online status. This situation can occur when synchronization with the NTP server sets the CDSM clock forward in time by an interval greater than at least two polling intervals or when the software clock on the CDSM is changed by a similar value using the **clock EXEC** command. The CDSM determines the status of devices in the CDS network depending on when it was last contacted by the devices for a getUpdate request. If you set the CDSM clock ahead in time, you have added that amount of time to the period since the CDSM received the last getUpdate request. However, it is only a transient effect. Once the devices contact the CDSM for their next getUpdate request after the clock setting change, the CDSM GUI reports the status of all devices correctly.

Examples

The following example configures the IP address of the time server providing the clock synchronization:

```
ServiceEngine(config)#ntp 172.16.22.44
```

The following example resets the time server providing the clock synchronization:

```
ServiceEngine(config)#no ntp 172.16.22.44
```

Related Commands

clock
show clock
show ntp status

ntpdate

To set the software clock (time and date) using a Network Time Protocol (NTP) server, use the **ntpdate** EXEC command.

ntpdate {*hostname* | *ip-address*}

Syntax Description

<i>hostname</i>	NTP hostname.
<i>ip-address</i>	NTP server IP address.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Use NTP to find the current time of day and set the SE current time to match. The **ntpdate** command synchronizes the software clock with the hardware clock.

Examples

The following example sets the software clock of the SE using an NTP server:

```
ServiceEngine#ntpdate 10.11.23.40
```

Related Commands

clock set
show clock

ping

To send echo packets for diagnosing basic network connectivity on networks, use the **ping** EXEC command.

ping {*hostname* | *ip-address*}

Syntax Description

<i>hostname</i>	Hostname of system to ping.
<i>ip-address</i>	IP address of system to ping.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

To use this command with the *hostname* argument, be sure that DNS functionality is configured on your SE. To force the timeout of a nonresponsive host or to eliminate a loop cycle, press **Ctrl-C**.

Following are sample results of the **ping** command:

- Normal response—The normal response occurs in 1 to 10 seconds, depending on network traffic.
- Destination does not respond—If the host does not respond, a “no answer from host” appears in 10 seconds.
- Destination unreachable—The gateway for this destination indicates that the destination is unreachable.
- Network or host unreachable—The SE found no corresponding entry in the route table.

Examples

The following example shows how to test the basic network connectivity with a host:

```
ServiceEngine#ping 172.19.131.189
PING 172.19.131.189 (172.19.131.189) from 10.1.1.21 : 56(84) bytes of
data.
64 bytes from 172.19.131.189: icmp_seq=0 ttl=249 time=613 usec
64 bytes from 172.19.131.189: icmp_seq=1 ttl=249 time=485 usec
64 bytes from 172.19.131.189: icmp_seq=2 ttl=249 time=494 usec
64 bytes from 172.19.131.189: icmp_seq=3 ttl=249 time=510 usec
64 bytes from 172.19.131.189: icmp_seq=4 ttl=249 time=493 usec

--- 172.19.131.189 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/mdev = 0.485/0.519/0.613/0.047 ms
ServiceEngine#
```


ping6

To ping the IPv6 address, use the **ping6** EXEC command.

ping6 *line ip-address*

Syntax Description	<i>line</i>	Destination Host or IP Address.
	<i>ip-address</i>	IP address of system to ping.

Defaults	No default behavior or values.

Command Modes	EXEC

Examples	The following example shows how to ping the IPv6 address: ServiceEngine(config) # pingv5 fec0::100/64

Related Commands	ping

port-channel

To configure the port-channel load-balancing options, use the **port-channel** global configuration command. To disable load-balancing options, use the **no** form of this command.

port-channel load-balance {dst-ip | dst-mac | round-robin}

no port-channel load-balance

Syntax Description

load-balance	Configures the load-balancing method.
dst-ip	Specifies the load-balancing method using destination IP addresses.
dst-mac	Specifies the load-balancing method using destination Media Access Control (MAC) addresses.
round-robin	Specifies the load-balancing method using round-robin sequential, cyclical resource allocation.

Defaults

Round-robin is the default load-balancing method.

Command Modes

Global configuration

Usage Guidelines

The **port-channel load-balance** command configures one of three load-balancing algorithms and provides flexibility in choosing interfaces when an Ethernet frame is sent. The **round-robin** option allows evenly balanced usage of identical network interfaces in a channel group. Because this command takes effect globally, if two channel groups are configured, they must use the same load-balancing option.

Because the Internet Streamer CDS software normally initiates IP packets or Ethernet frames, it does not support hashing based on the source IP address and source MAC address. Cisco Internet Streamer Release 2.4 software adds the round-robin option, which is the default load-balancing algorithm, to evenly distribute traffic among several identical network interfaces.

Examples

The following example shows how to configure the round-robin load-balancing method on an SE:

```
ServiceEngine(config)#port-channel load-balance round-robin
```

Related Commands

interface

primary-interface

To configure the primary interface for the CDS network, use the **primary-interface** global configuration command. Use the **no** form of the command to remove the configured primary interface.

primary-interface { **GigabitEthernet** *1-2/port* | **PortChannel** *1-2* | **Standby** *group_num* }

no primary-interface { **GigabitEthernet** *1-2/port* | **PortChannel** *1-2* | **Standby** *group_num* }

Syntax Description		
GigabitEthernet		Selects a Gigabit Ethernet interface as the CDS network primary interface.
<i>1-2/</i>		Gigabit Ethernet slot numbers 1 or 2.
<i>port</i>		Port number of the Gigabit Ethernet interface.
PortChannel		Selects a port-channel interface as the CDS network primary interface.
<i>1-2</i>		Port channel number 1 or 2.
Standby		Selects a standby group as the CDS network primary interface.
<i>group_num</i>		Standby group number.

Defaults

The default primary interface is the first operational interface on which a link beat is detected. Interfaces with lower-number IDs are polled first (for example, GigabitEthernet 0/0 is checked before 1/0). Primary interface configuration is required for the proper functioning of the Centralized Management System (CMS). After devices are registered to the CDSM, the CDSM uses the configured primary interface to communicate with the registered devices.

You cannot enable the CDS network without specifying the primary interface. Also, you must have chosen the primary interface before you enable the CMS. The primary interface can be changed without disabling the CDS network. The primary interface specifies the default route for an interface. To change the primary interface, choose a different interface as the primary interface.

In Cisco Internet Streamer Release 2.4 software and later releases, you can select a standby interface as the primary interface (you can enter the **primary-interface Standby group_num** command) to specify a standby group as the primary interface on an SE.

Command Modes

Global configuration

Usage Guidelines

The **primary-interface** global configuration command allows the administrator to specify the primary interface for the CDS network.

The primary interface can be changed without disabling the CDS network. To change the primary interface, re-enter the command string and specify a different interface.



Note

If you use the **restore factory-default preserve basic-config** command, the configuration for the primary interface is not preserved. On a device in a CDS network, if you want to re-enable the CDS network after using the **restore factory-default preserve basic-config** command, make sure to reconfigure the primary interface after the factory defaults are restored.

Examples

The following example shows how to specify the GigabitEthernet slot 1 port 0 as the primary interface on an SE:

```
ServiceEngine(config)#primary-interface GigabitEthernet 1/0
```

The following example shows how to specify the GigabitEthernet slot 2 port 0 as the primary interface on an SE:

```
ServiceEngine(config)#primary-interface GigabitEthernet 2/0
```

pwd

To view the present working directory, use the **pwd** EXEC command.

pwd

Syntax Description	This command has no arguments or keywords.

Defaults	No default behavior or values.

Command Modes	EXEC

Usage Guidelines	Use this command to display the present working directory of the SE.

Examples	The following example shows how to view the present working directory:

```
ServiceEngine#pwd  
/local1
```

Related Commands	cd dir lls ls

qos

To globally enable QoS functionality on the switch, use the **qos** command. To globally disable QoS functionality, use the no form of this command.

```
qos {device-policy-service {config-file url | enable} | dsvc num name name fqdn icap ip address
num list request-type {all num num name redirect-url {no-redirect list num | url list num} |
```

```
http-download num num name{no-redirect list num | url list num} | wmt-streaming num num
name redirect-url {no-redirect list num | url list num}}
```

```
no qos {device-policy-service {config-file url | enable} | dsvc num name name fqdn icap ip
address num list request-type {all num num name redirect-url {no-redirect list num | url list
num} | http-download num num name{no-redirect list num | url list num} | wmt-streaming
num num name redirect-url {no-redirect list num | url list num}}
```

Syntax Description

device-policy-service	Configures Camiant qos cdn-am policy service.
config-file	Specifies the policy service configuration file.
<i>url</i>	URL or local configuration file.
enable	Enables Camiant policy service.
dsvc	Configures PCMM QoS details for the delivery service.
<i>num</i>	the delivery service ID, which is obtained from the CDSM (1-4294967295).
<i>name</i>	Delivery Service Name as obtained from the CDSM.
<i>name</i>	Service Routed Domain for delivery service.
<i>fqdn</i>	Service FQDN for delivery service
icap	Specifies that authorization needed using ICAP.
<i>ip address</i>	IP address of the Policy Server.
<i>num</i>	Port of the Policy Server for authorization (1-65535).
<i>list</i>	List of URI extension separated by commas for which Authorization is to be done.
request-type	Configures the QoS setting needed for Windows Media Streaming or download.
all	Configures the QoS setting for Windows Media Streaming and download.
<i>num</i>	Signature details as key ID.
<i>num</i>	Signature details as key ID.
<i>name</i>	Signature details as key.
redirect-url	Specifies the redirect URL string on signature validation failure.
no-redirect	Always returns forbidden if validation fails.
<i>url</i>	Redirect URL String on signature validation failure.
<i>list</i>	List of URI extensions separated by commas for which Signature validation is to be done.
<i>num</i>	(1) Enable or (0) Disable the setting given.
http-download	Specifies the QoS setting for download.
wmt-streaming	Specifies the QoS setting for Windows Media Streaming.

Defaults

QoS functionality is disabled.

Command Modes

Global configuration

Usage Guidelines

If QoS functionality is globally enabled, it is enabled on all interfaces, except on the interfaces where QoS has been disabled. If QoS functionality is globally disabled, all traffic is passed in QoS pass-through mode.

Examples

This example shows how to enable QoS functionality globally on the switch:

```
ServiceEngine(config)#qos device-policy-service enable
```

Related Commands

show qos
show statistics qos

radius-server

To configure RADIUS authentication parameters, use the **radius-server** global configuration command. To disable RADIUS authentication parameters, use the **no** form of this command.

radius-server {**enable** | **host** {*hostname* | *hostipaddr*} [**auth-port** *port*] | **key** *keyword* | **redirect** {**enable** | **message** *reply* *location* *url*} | **retransmit** *retries* | **timeout** *seconds*}

no radius-server {**enable** | **host** {*hostname* | *hostipaddr*} | **key** | **redirect** {**enable** | **message** *reply* *location* *url*} | **retransmit** | **timeout**}

Syntax Description

enable	Enables HTTP RADIUS authentication.
host	Specifies a RADIUS server.
<i>hostname</i>	Hostname of the RADIUS server.
<i>hostipaddr</i>	IP address of the RADIUS server.
auth-port	(Optional) Sets the UDP port for the RADIUS authentication server.
<i>port</i>	UDP port number (1–65535). The default is 1645.
key	Specifies the encryption key shared with the RADIUS servers.
<i>keyword</i>	Text of the shared key (15 characters maximum).
redirect	Redirects the response if an authentication request fails.
enable	Enables the redirect feature.
message	Replies with an authentication failure message.
<i>reply</i>	Reply message text string (24 characters maximum).
location	Sets the HTML page location, for example, http://www.cisco.com .
<i>url</i>	URL destination of authentication failure instructions.
retransmit	Specifies the number of transmission attempts to an active server.
<i>retries</i>	Number of transmission attempts for a transaction (1–3).
timeout	Time to wait for a RADIUS server to reply.
<i>seconds</i>	Wait time in seconds (1–20).

Defaults

auth-port *port*: UDP port 1645

retransmit *retries*: 2

timeout *seconds*: 5

Command Modes

Global configuration

Usage Guidelines

RADIUS is a client/server authentication and authorization access protocol used by an CDS network device to authenticate users attempting to connect to a network device. The CDS network device functions as a client, passing user information to one or more RADIUS servers. The CDS network device

permits or denies network access to a user based on the response that it receives from one or more RADIUS servers. RADIUS uses the User Datagram Protocol (UDP) for transport between the RADIUS client and server.

You can configure a RADIUS key on the client and server. If you configure a key on the client, it must be the same as the one configured on the RADIUS servers. The RADIUS clients and servers use the key to encrypt all RADIUS packets transmitted. If you do not configure a RADIUS key, packets are not encrypted. The key itself is never transmitted over the network.

**Note**

For more information about how the RADIUS protocol operates, see RFC 2138, *Remote Authentication Dial In User Service (RADIUS)*.

RADIUS authentication usually occurs in these instances:

- Administrative login authentication—When an administrator first logs in to the SE to configure the SE for monitoring, configuration, or troubleshooting purposes. For more information, see the [“Enabling and Disabling Administrative Login Authentication and Authorization Through RADIUS”](#) section on page 2-169.
- HTTP request authentication—When an end user sends a service request that requires privileged access to content that is served by the SE. For more information, see the [“Configuring RADIUS Authentication of HTTP Requests”](#) section on page 2-170.

RADIUS authentication is disabled by default. You can enable RADIUS authentication and other authentication methods at the same time. You can also specify which method to use first.

To configure RADIUS parameters, use the **radius-server** command in global configuration mode. To disable RADIUS authentication parameters, use the **no** form of this command.

The **redirect** option of the **radius-server** command redirects an authentication response to a different authentication server if an authentication request using the RADIUS server fails.

**Note**

The following **rule** command is relevant to RADIUS authentication only if the **redirect** option has been configured.

To exclude domains from RADIUS authentication, use the **rule no-auth domain** command. RADIUS authentication takes place only if the site requested does not match the specified pattern.

Enabling and Disabling Administrative Login Authentication and Authorization Through RADIUS

When configuring an SE to use RADIUS to authenticate and authorize administrative login requests, follow these guidelines:

- By default, RADIUS authentication and authorization is disabled on an SE.
- Before enabling RADIUS authentication on the SE, you must specify at least one RADIUS server for the SE to use.
- You can enable RADIUS authentication and other authentication methods at the same time. You can specify which method to use first using the **primary** keyword. When local authentication is disabled, if you disable all other authentication methods, local authentication is re-enabled automatically.
- You can use the SE GUI or the CLI to enable RADIUS authentication and authorization on an SE.

**Tip**

From the SE GUI, choose **Devices > General Settings > Authentication**. Use the displayed Authentication Configuration window.

To use the SE CLI to enable RADIUS authentication and authorization on an SE, enable RADIUS authentication for normal login mode by entering the **authentication login radius** global configuration command as follows:

```
ServiceEngine(config)# authentication login radius enable [primary] [secondary]
```

Use the **authentication configuration radius** global configuration command to enable RADIUS authorization as follows:

```
ServiceEngine(config)# authentication configuration radius enable [primary] [secondary]
```

**Note**

To disable RADIUS authentication and authorization on an SE, use the **no radius-server enable** command.

Configuring RADIUS Authentication of HTTP Requests

To configure RADIUS authentication for HTTP requests on an SE, configure the RADIUS server settings on the SE and enable RADIUS authentication for HTTP requests on the SE using the **radius-server** global configuration command.

Examples

The following example enables the RADIUS client, specifies a RADIUS server, specifies the RADIUS key, accepts retransmit defaults, and excludes the domain name, mydomain.net, from RADIUS authentication. You can verify the configuration with the **show radius-server** and **show rule all** commands.

```
ServiceEngine(config)#radius-server enable
ServiceEngine(config)#radius-server host 172.16.90.121
ServiceEngine(config)#radius-server key myradiuskey
ServiceEngine(config)#rule action no-auth pattern-list 2
ServiceEngine(config)#rule pattern-list 2 domain mydomain.net
```

```
ServiceEngine#show radius-server
Login Authentication for Console/Telnet/Ftp/SSH Session: enabled
Configuration Authentication for Console/Telnet/Ftp/SSH Session: enabled (secondary)
```

```
Radius Configuration:
-----
Radius Authentication is on
Timeout = 5
Retransmit = 2
Key = ****
Radius Redirect is off
There is no URL to authentication failure instructions
Servers
-----
IP 172.16.90.121 Port = 1645
```

```
ServiceEngine#show rule all
Rules Template Configuration
-----
Rule Processing Enabled
rule no-auth domain mydomain.net
```

The following example disables RADIUS authentication on the SE:

```
ServiceEngine(config)#no radius-server enable
```

The following example shows how to force the SE to try RADIUS authentication first:

```
ServiceEngine(config)# authentication login radius enable primary
```

Related Commands

debug authentication user
rule
show radius

rcp

To enable the Remote Copy Program (RCP), use the **rcp** global configuration command. To disable RCP, use the **no** form of this command.

rcp enable

no rcp enable

Syntax Description	enable Enables RCP services.

Defaults	No default behavior or values.

Command Modes	Global configuration

Examples	The following example shows how to enable RCP: <code>ServiceEngine(config)# rcp enable</code>

Related Commands	show rcp

rea

To initiate the remote execution agent, use the **rea** EXEC command.

rea {start | stop}

Syntax Description	start	Starts the remote execution agent services.
	stop	Stops the remote execution agent services.
Defaults	No default behavior or values.	
Command Modes	EXEC	
Examples	The following example shows the remote execution agent services being started. ServiceEngine(config)# rea start	
Related Commands	show rea	

reload

To halt and perform a cold restart on the SE, use the **reload** EXEC command.

reload [force]

Syntax Description	force (Optional) Forces a reboot without further prompting.
Defaults	No default behavior or values.
Command Modes	EXEC
Usage Guidelines	To reboot the SE, use the reload command. If the current running configuration is different from the startup configuration and if the configuration changes are not saved to flash memory, you are prompted to save the current running configuration parameters to the startup configuration. To save any file system contents to disk from memory before a restart, use the cache synchronize command.
Examples	The following example reloads the SE after you have saved the configuration changes. <pre>ServiceEngine#reload System configuration has been modified. Save?[yes]:yes Proceed with reload?[confirm]yes Shutting down all services, will timeout in 15 minutes. reload in progress</pre> The following example forces a reboot on the SE: <pre>ServiceEngine#reload force</pre>
Related Commands	cache synchronize write write erase

rename

To rename a file on the SE, use the **rename** EXEC command.

rename *oldfilename newfilename*

Syntax Description	<i>oldfilename</i>	Original filename.
	<i>newfilename</i>	New filename.

Defaults	No default behavior or values.

Command Modes	EXEC

Usage Guidelines	Use this command to rename any sysfs file without making a copy of the file.

Examples	The following example renames a file named errlog.txt as old_errlog.txt: ServiceEngine# rename errlog.txt old_errlog.txt

Related Commands	cpfile

restore

To restore the device to its manufactured default status, removing the user data from the disk and flash memory, use the **restore EXEC** command. This command erases all existing content on the device.

restore factory-default [preserve basic-config]

Syntax Description

factory-default	Resets the device configuration and data to their manufactured default status.
preserve	(Optional) Preserves certain configurations and data on the device.
basic-config	Selects basic network configurations.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Use this command to restore data on disk and in flash memory to the factory default, while preserving particular time-stamp evaluation data. You need to enter this command from the root directory, or else the following error message is displayed:

```
ServiceEngine#restore factory-default
```

```
Need to cd to / before issuing this command
```

```
Command aborted.
SERVICEENGINE#
```

Be sure to back up the CDSM database and copy the backup file to a safe location that is separate from that of the CDSM, or change over from the primary to a standby CDSM before you use the **restore factory-default** command on your primary CDSM. The primary CDSM operation must be halted before proceeding with backup and restore commands.



Caution

This command erases user-specified configuration information stored in the flash image and removes the data on the disk, the user-defined disk partitions, and the entire CDSM database. User-defined disk partitions that are removed include the sysfs and cdnfs partitions. The configuration being removed includes the starting configuration of the device.

By removing the CDSM database, all configuration records for the entire CDS network are deleted. If you do not have a valid backup file or a standby CDSM, you must use the **cms deregister force** command and reregister every SE and SR after you have reconfigured the CDSM, because all previously configured data is lost.

If you used your standby CDSM to store the database while you reconfigured the primary, you can simply register the former primary as a new standby CDSM.

If you created a backup file while you configured the primary CDSM, you can copy the backup file to this newly reconfigured CDSM and use the **cms database restore** command.

**Caution**

If you upgraded your software after you received your software recovery CD-ROM, using the CD-ROM software images may downgrade your system.

Cisco Internet Streamer CDS software consists of three basic components:

- Disk-based software
- Flash-based software
- Hardware platform cookie (stored in flash memory)

All of these components must be correctly installed for Cisco Internet Streamer CDS software to work properly.

Examples

The following two examples show the results of using the **restore factory-default** and **restore factory-default preserve basic-config** commands. Because configuration parameters and data are lost, if prompts are given before initiating the restore operation to ensure that you want to proceed.

**Note**

If you use the **restore factory-default preserve basic-config** command, the configuration for the primary interface is not preserved. On a device running the Internet Streamer CDS Release 2.x software, if you want to re-enable the CDS network after using the **restore factory-default preserve basic-config** command, make sure to reconfigure the primary interface after the factory defaults have been restored.

CDSM# **restore factory-default**

This command will wipe out all of data on the disks and wipe out CDS CLI configurations you have ever made. If the box is in evaluation period of certain product, the evaluation process will not be affected though.

It is highly recommended that you stop all active services before this command is run.

Are you sure you want to go ahead?[yes/no]

CDSM# **restore factory-default preserve basic-config**

This command will wipe out all of data on the disks and all of CDS CLI configurations except basic network configurations for keeping the device online. The to-be-preserved configurations are network interfaces, default gateway, domain name, name server and hostname. If the box is in evaluation period of certain product, the evaluation process will not be affected.

It is highly recommended that you stop all active services before this command is run.

Are you sure you want to go ahead?[yes/no]

**Note**

You can enter basic configuration parameters (such as the IP address, hostname, and name server) at this point or later through entries in the command-line interface.

The following example shows that entering the **show disk** command after the **restore** command verifies that the **restore** command has removed data from the partitioned file systems (sysfs and cdnfs):

```
ServiceEngine#show disk
```

```
SYSFS      0.0GB      0.0%
CDNFS      0.0GB      0.0%
FREE       29.9GB     100.0%
```

Because flash memory configurations were removed after the **restore** command was used, the **show startup-config** command does not return any flash memory data. The **show running-config** command returns the default running configurations.

The **show wmt** commands continue to display the same license evaluation periods as before the **restore factory-default** command was invoked, because the evaluation period is not affected by this **restore** command. For example, if there were 21 days remaining in the evaluation period before the **restore factory-default** command was used, there would continue to be 21 days remaining in the evaluation period.

Related Commands

- cms database backup
- cms database restore
- show disks
- show rtsp server real-subscriber
- show running-config
- show startup-config
- show wmt

rmdir

To delete a directory, use the **rmdir** EXEC command.

rmdir *directory*

Syntax Description	<i>directory</i> Name of the directory that you want to delete.
Defaults	No default behavior or values.
Command Modes	EXEC
Usage Guidelines	Use this command to remove any directory from the SE file system. The rmdir command removes only empty directories.
Examples	The following example removes the oldfiles directory under /local1: ServiceEngine# rmdir /local1/oldfiles
Related Commands	lls ls mkdir

rtsp

To configure the Real-Time Streaming Protocol (RTSP)-related parameters, use the **rtsp** global configuration command. To disable individual options, use the **no** form of this command.

rtsp {**advanced** *ip address* {**bypass-gateway** **movie-streamer** | **max-initial-setup-delay** *time_delay* | **max-request-rate** *num*} | **ip-address** *ip address*}

no rtsp {**advanced** *ip address* {**bypass-gateway** **movie-streamer** | **max-initial-setup-delay** *time_delay* | **max-request-rate** *num*} | **ip-address** *ip address*}

Syntax Description

advanced	Performs advanced configuration of the RTSP gateway.
<i>ip address</i>	The IP address of RTSP gateway.
bypass-gateway	Allows bypassing the RTSP gateway for RTSP requests.
movie-streamer	Allows bypassing the RTSP gateway for Movie Streamer RTSP requests.
max-initial-setup-delay	Specifies the maximum delay in seconds between the TCP accept and first RTSP message from the client. The default is 10 seconds.
<i>time_delay</i>	The RTSP advanced maximum initial setup delay in seconds (0-2147483647).
max-request-rate	Specifies the maximum incoming requests allowed by the RTSP Gateway per second.
<i>num</i>	The maximum requests per second (1-2147483647).
ip-address	Configures the IP address for the RTSP gateway.
<i>ip-address</i>	The IP address of the RTSP gateway.

Defaults

max-initial-setup-delay *time_delay*: 10 seconds

max-request-rate *num*: 40 requests

Command Modes

Global configuration

Usage Guidelines

RTSP is a standard Internet streaming control protocol (RFC 2326). It is an application-level protocol that controls the delivery of data with real-time properties, such as video and audio. Apple QuickTime, Real Networks, and the Cisco Streaming Engine use RTSP as the streaming control protocol.

Live Streaming with the Cisco Streaming Engine

The Internet Streamer CDS software supports live streaming content with many kinds of network topologies and deployment scenarios. This feature allows the integration of streaming content from Cisco IP/TV Servers and QuickTime live broadcast servers with the CDS network. Support for broadcast of playlists is included (except for SEs at the network edge), allowing you to convert one or more disk files into a playlist and to send them out through simulated live streaming.

An RTSP source is a fully qualified RTSP URL that references an external streaming server, such as a parent SE, which provides the corresponding RTSP request point.

RTSP Gateway

The RTSP gateway is a process that runs on the SE. The RTSP gateway accepts an RTSP request and performs the initial RTSP handshake with RTSP-based clients (for example, Windows Media 9 players) on behalf of the back-end RTSP servers (for example, the WMT RTSP server) that are running on the SE.

For every RTSP request, the RTSP gateway examines the following properties of the request:

- The URL and its position in the Unified Name Space (UNS)
- The user agent
- The IP address of the final destination
- The media type

After the successful completion of uniformity checks, the RTSP gateway tunnels the request to the appropriate back-end RTSP server that is running on the SE. The RTSP gateway can tunnel the request to RealProxy, RealSubscriber, or the Cisco Streaming Engine on the SE, depending on the requested media type, the back-end RTSP servers that are currently enabled on the SE, and the media player that is requesting the content.

After the RTSP gateway tunnels the request to a particular back-end RTSP server that is running on the SE and the back-end server and the client negotiate the UDP ports, the RTSP gateway continues with RTSP message passing (SETUP). When the RTSP client issues a PLAY request, the streaming server starts streaming the data to the client over UDP.

Based on the properties of the incoming request, including user agent, final destination, and media file type, the RTSP gateway performs the following tasks with SEs:

- Forwards the incoming request to the appropriate back-end RTSP server that is running on the SE. The incoming request goes to the WMT RTSP server if the client is a Windows Media 9 player. The SE uses the IETF standard RTSP protocol and proprietary Microsoft extensions to serve the content to Windows Media 9 players.
- Redirects the incoming request.
- Rejects the incoming request.

If the SE is registered with a CDSM, the RTSP gateway also redirects the incoming requests to other content distributors (for example, RealSubscriber or Cisco Streaming Engine) that are configured on the SE.

Network Address Translation (NAT) is designed for IP address simplification and conservation because it enables private IP internetworks that use nonregistered IP addresses to connect to the Internet. NAT operates on a router, usually connecting two networks together, and translates the private addresses in the internal network into legal addresses before packets are forwarded onto another network. As part of this functionality, NAT can be configured to advertise only one external address for the entire network. This configuration provides additional security, effectively hiding the entire internal network from the world behind that address. NAT has the dual functionality of security and address conservation and is typically implemented in remote access environments.



Note

If the SE is behind a NAT-enabled router, you must specify the IP address of the RTSP gateway that is running on the SE. By default, no IP address is specified.

Default RTSP Gateway Settings

The RTSP gateway is automatically enabled on the SE and cannot be disabled with a command.

[Table 2-11](#) lists the default settings for the RTSP gateway.

Table 2-11 *Default Settings for the RTSP Gateway*

RTSP Gateway Setting	Default Setting
IP address of RTSP gateway	Not specified
Incoming RTSP port	Port 554
Incoming RTSP request rate	40 requests per second
Layer 4 switching	Not enabled
Maximum initial setup delay	10 seconds
Maximum request rate	40 requests per second

By default, the RTSP gateway is always enabled on an SE and cannot be disabled by entering a CLI command. As [Table 2-11](#) shows, the RTSP gateway has a set of default settings. You only need to change these default settings under the following conditions:

- You want to configure the RTSP gateway to listen for incoming RTSP requests on a port other than the default port (port 554).
- The SE is behind a NAT-enabled router. In this case, you must specify the IP address of the RTSP gateway. By default, an IP address for the RTSP gateway is not specified.

**Note**

A description of the Real-Time Streaming Protocol (RTSP) is available as IETF RFC 2326.

Examples

The following example shows how to set up the Movie Streamer RTSP bypass gateway:

```
ServiceEngine(config)#rtsp advanced bypass-gateway movie-streamer
```

The following example shows how to establish the maximum initial setup delay:

```
ServiceEngine(config)#rtsp advanced max-initial-setup-delay 15
```

The following example shows how to establish the maximum request rate:

```
ServiceEngine(config)#rtsp advanced max-request-rate 50
```

The following example shows how to assign the RTSP IP address:

```
ServiceEngine(config)#rtsp ip-address 10.74.61.1
```

Related Commands

show rtsp

rule

To set the rules by which the SE filters HTTP, HTTPS, and RTSP traffic, use the **rule** global configuration command. To disable individual options, use the **no** form of this command.

The general **rule** command is as follows:

```
rule {action action-type pattern-list list_num [protocol {all | protocol-type}] | enable |
pattern-list list_num pattern-type}
```

The specific **rule** commands are as follows:

```
rule action allow pattern-list list_num [protocol {all | http | rtmp | rtsp}]
```

```
rule action block pattern-list list_num [protocol {all | http | rtmp | rtsp}]
```

```
rule action generate-url-signature {include-client-src-ip | key-id-owner 1-32 {key-id-number
1-16} {pattern-list 1-512} [protocol {all | http}]}
```

```
rule action no-cache pattern-list list_num [protocol {all | http | rtmp | rtsp}]
```

```
rule action redirect url pattern-list list_num [protocol {all | http | rtmp | rtsp}]
```

```
rule action refresh pattern-list list_num [protocol {all | http }]
```

```
rule action replace pattern-list list_num [protocol {all | http | rtmp | rtsp}]
```

```
rule action rewrite pattern-list list_num [protocol {all | http | rtmp | rtsp}]
```

```
rule action use-icap-service service-name pattern-list list_num [protocol {all | http}]
```

```
rule action validate-url-signature {error-redirect-url url | exclude {all error-redirect-url url
pattern-list num [protocol {all | http | rtmp | rtsp}]} | client-ip error-redirect-url url
pattern-list num [protocol {all | http | rtmp | rtsp}]} | expiry-time error-redirect-url url
pattern-list num [protocol {all | http | rtmp | rtsp}]}]}
```

```
rule enable
```

```
rule pattern-list list-num domain dn_regexp
```

```
rule pattern-list list-num group-type {and | or}
```

```
rule pattern-list list-num header-field {referer ref_regexp | request-line req_regexp | user-agent
ua_regexp}
```

```
rule pattern-list list-num src-ip s_ipaddress s_subnet
```

```
rule pattern-list list-num url-regex url_regexp
```

```
rule pattern-list list-num url-regexsub url_regexp url_sub
```

```
no rule action {allow pattern-list list_num [protocol {all | http | https | rtsp}]} | block pattern-list
list_num [protocol {all | http | https | rtsp}]} | generate-url-signature {include-client-src-ip
| key-id-owner 1-32 {key-id-number 1-16} {pattern-list 1-512} [protocol {all | http}]} |
no-cache pattern-list list_num [protocol {all | http | https}]} | redirect url pattern-list
list_num [protocol {all | http | https | rtsp}]} | refresh pattern-list list_num [protocol {all |
```

```

http | https}} | replace pattern-list list_num [protocol {all | http | https | rtsp}} | rewrite
pattern-list list_num [protocol {all | http | https | rtsp}} | use-icap-service service-name
pattern-list list_num [protocol {all | http | https}} | validate-url-signature pattern-list
error-redirect-url url | exclude {all error-redirect-url url pattern-list num [protocol {all |
http | rtmp | rtsp}} | client-ip error-redirect-url url pattern-list num [protocol {all | http |
rtmp | rtsp}} | expiry-time error-redirect-url url pattern-list num [protocol {all | http | rtmp
| rtsp}}}}

```

no rule enable

```

no rule pattern-list list-num {domain dn_regexp | group-type {and | or} | header-field {referer
ref_regexp | src-ip s_ipaddress s_subnet | url-regex url_regexp | url-regex url_regexp
url_sub}}

```

Syntax Description

action	Describes the action that the rule is to take.
<i>action-type</i>	Types of actions that you can associate with a defined pattern list.
pattern-list	Configures the pattern list.
<i>list_num</i>	Pattern list number (1–512).
protocol	Specifies the protocol for which this rule is to be matched.
all	Matches this rule with all applicable protocols for this action.
<i>protocol-type</i>	Protocol types that support rule actions, namely, http , https , and rtsp . Note The term http traffic is used to refer to requests over HTTP including HTTP, FTP over HTTP, and HTTPS over HTTP. The Rules Template is not supported for FTP native requests.
enable	Enables rules processing on the SE.
<i>pattern-type</i>	Types of rule patterns that you can add to a pattern list.
allow	Allows the incoming request that matches the pattern list. This can be used in combination with block actions to allow selective types of requests. Allow does not carry any meaning as a standalone action.
http	Matches this rule with HTTP.
rtmp	Matches this rule with RTMP.
rtsp	Matches this rule with RTSP.
block	Blocks this request and allows all others.
generate-url-signature	Specifies that the SE generates a signed URL that is included in the autogenerated ASX file when content routing is in use and the pattern matches.
include-client-src-ip	Specifies the client IP to be included in the signed URL.
key-id-owner	Specifies the owner of the key (1-32). The key is a shared secret string.
<i>1-32</i>	Specifies the owner of the key.
key-id-number	Specifies the identification number of the key (1-16).
<i>1-16</i>	Specifies the identification number of the key.
pattern-list	Specifies the number of the pattern list (1-512). Valid patterns are domain, url-regex, or dst-ip.
<i>1-512</i>	Specifies the number of the pattern list.
no-cache	Does not cache the object.

redirect	Redirects the request to the rewritten URL.
<i>url</i>	Redirect URL.
refresh	Revalidates the object with the web server.
replace	Replaces the text string in the object.
rewrite	Rewrites the original request as a specified URL and fetches the rewritten URL on a cache miss.
use-icap-service	Uses a specific ICAP server.
<i>service-name</i>	Service name used for handling a request through an ICAP server.
validate-url-signature	Validates a signed URL.
error-redirect-url	Specifies the error URL.
exclude	Specifies what field in the URL signature must be validated.
all	Specifies both client-ip and expiry time fields will be excluded in validation.
client-ip	Specifies that the client-ip field will be excluded in validation.
expiry-time	Specifies that the expire-time field will be excluded in validation.
domain	Specifies the regular expression to match the domain name.
<i>dn_regex</i>	Regular expression to be matched with the domain name.
group-type	Specifies whether the pattern list is an AND or OR type.
and	Specifies an AND pattern to the pattern list.
or	Specifies an OR pattern to the pattern list.
header-field	Pattern type—Specifies the header field pattern of the request and substitute replacement pattern.
referer	Specifies the referer request header.
<i>ref_regex</i>	Regular expression to be matched with the referer request header.
request-line	Specifies the request method line.
<i>req_regex</i>	Regular expression to be matched with the request method line.
user-agent	Specifies the user agent request header.
<i>ua_regex</i>	Regular expression to be matched with the User Agent request header.
src-ip	Specifies the source IP address of the request.
<i>s_ipaddress</i>	Source IP address of the request.
<i>s_subnet</i>	Source IP subnet mask.
url-regex	Specifies the regular expression to match a substring of the URL.
<i>url_regex</i>	Regular expression to be matched with the URL string.
url-regsub	Sets the regular expression to match the URL and replacement pattern.
<i>url_sub</i>	URL string replacement pattern.

Defaults

The default is rule processing disabled.

The **group-type** pattern is OR by default.

Command Modes

Global configuration

Usage Guidelines

The Rules Template allows you to specify a set of rules, each clearly identified by an action and a pattern. The Rules Template allows you to configure an SE to use specific rules to filter HTTP, HTTPS, and RTSP traffic. A common use of this feature is to configure an SE to block the spread of Internet worms and viruses within an organization by checking whether a requested web page matches the pattern of a known Internet worm and if so then automatically blocking the request.

If you have enabled rules processing on an SE (enabled the Rules Template feature on the SE and configured rules for the SE), the SE checks each incoming client request to determine if a rule pattern matches the requested content. If a rule pattern matches the given request, the SE uses the specified action (policy) to handle this incoming traffic.

The SE can match incoming requests against the following:

- Patterns in the IP address of the client requesting the content (source IP address), including the IP address, the network mask, and the port list
- Patterns in the IP address of the origin web or media server (destination IP addresses), including the IP address, the network mask, and the port list
- Regular expression of the URL
- Regular expression of the domain portion of the URL
- MIME types of the web object that the client is requesting
- Regular expressions symbolizing domain names
- Headers that are sent in the request, including the following:
 - User-agent of the request, which indicates which client software is issuing the request
 - Referer, which indicates the web page from which the browser jumped to this link
 - Request line, which indicates the request line itself

You can apply the policies defined in the Rules Template to HTTP (including FTP over HTTP) and HTTPS and to RTSP for streaming media objects. Policies that can be applied include the following:

- Allowing a request to be completed
- Blocking the request
- Overriding the HTTP response header and caching the object
- Caching the object depending on the HTTP response header
- Bypassing authentication for the request
- Replacing the text string
- Not caching an object
- Bypassing an upstream proxy for the request
- Redirecting the request to a different URL
- Revalidating the object with the origin server
- Rewriting the URL
- No URL filtering for the specified HTTP and HTTPS requests
- Using a specific ICAP server
- Using a specific upstream proxy
- Using a specific server for the request

**Note**

To enter a question mark (?) in a rule regular expression from the command-line interface, use the escape character followed by a question mark (?). Use of the escape sequence prevents the command-line interface from displaying context-sensitive help.

Supported Rule Actions per Protocol

For RTSP, the `redirect` and the `redirect_url_for_cdn` rule actions are supported for RTSP requests from RealMedia players. These two rule actions are not supported for RTSP requests from Windows Media Players. For example, Windows Media Services 9 (WMS 9) supports the `block`, `rewrite`, and `allow` rule actions for RTSP requests, but does not support the `redirect` and `redirect_url_for_cdn` rule actions for RTSP requests.

Supported Action and Pattern Combinations

Not all actions support all patterns for request matching because some patterns do not make sense for some actions.

Understanding Actions and Patterns

A *rule* is specified by an action and a pattern list. An action is performed on a request if this request matches the pattern list specified in the **rule pattern-list** command.

An *action* is something that the SE performs when processing a request; for instance, an action could be blocking the request, using an alternative proxy, and so forth.

A *pattern list* defines the limits of a request; for instance, a pattern list may specify that the source IP address falls in the subnet range 172.16.*.*.

Rules can be dynamically added, displayed, or deleted from the SE. The rules are preserved across reboots because they are written into persistent storage, such as NVRAM, using the appropriate CLI commands, the SE GUI, or the CDSM GUI. Only the system resources limit the number of rules that the SE can support. Because rules consume resources, the more rules that you define can greatly impact how the SE performs.

**Note**

The number of actions is limited only by available resources. The maximum number of pattern lists is 512. The maximum number of patterns per action is 128. A single pattern list can contain up to 128 patterns of a particular pattern type.

Actions

The Rules Template supports the following types of actions:

- **Allow**—Allows incoming requests that match the pattern list.
This rule action can be used in combination with block actions to allow selective types of requests. Allow does not carry any meaning as a standalone action.
- **Block**—Blocks this request and allows all others.
- **No-cache**—Does not cache this object.
- **Redirect**—Redirects the original request to a specified URL. Redirect is relevant to the RADIUS server only if the RADIUS server has been configured for **redirect**.
- **Refresh**—For a cache hit, forces an object freshness check with the server.
- **Replace**—Replaces the text string in the object.

- **Rewrite**—Rewrites the original request as a specified URL. The SE searches for the rewritten URL in the cache, and then on a cache miss, fetches the rewritten URL and returns the object transparently to the client. You should use a **redirect** rule instead of a **rewrite** rule because of possible performance impacts. The reason for the performance impact is that, for a **redirect** rule, the SE sends a 302 (Found) message to the client with the new redirect URL. The client issues a separate request to the redirected URL. However, for a **rewrite** action, the original request URL is rewritten as the specified URL. The URL rewrite could change the domain name of the URL, which necessitates a Domain Name Server (DNS) lookup to find the destination IP address of the new rewritten server to which the request must be sent.
- **Use-icap-service**—Uses a specified ICAP server.
- **Validate-url-signature**—Validates a signed URL.

Actions can be applied to specific protocols or to a set of protocols. If no protocol is configured, then the specified action will be taken for all the traffic that goes through the SE.

Patterns

The Rules Template supports the following pattern types:

- **Domain**—Matches the domain name in the URL or the Host header against a regular expression. For example, `.*ibm.*` matches any domain name that contains the `ibm` substring. The `\.foo\.com$` domain name matches any domain name that ends with the `.foo.com` substring.



Note In regular expression syntax, the dollar sign (\$) metacharacter directs that a match is made only when the pattern is found at the end of a line.

- **Group-type**—Specifies whether the pattern list is an AND or OR type. The default is OR.
- **Src-ip**—Matches the request's source IP address and netmask. Specify an IP address and a netmask.
- **URL-regex**—Matches the URL against a regular expression. The match is case insensitive. Specify a regular expression.
- **Header-field**—Matches the header field pattern of the request.

Request header field patterns **referer**, **request-line**, and **user-agent** are supported for the actions **block**, **redirect**, and **rewrite**. The **referer** pattern is matched against the Referer header in the request, the **request-line** pattern is matched against the first line of the request, and the **user-agent** pattern is matched against the User-Agent header in the request.

- **URL-regexsub**—Matches the URL against a regular expression to form a new URL per pattern substitution specification for the **rewrite** and **redirect** actions. The match is case insensitive. The valid substitution index range is from 1 to 9.

If an empty string is given as a replacement pattern, the Referer header is stripped. Stripping of the Referer header occurs in the **user-agent** pattern.

Multiple patterns can be entered on the same pattern list. If any of them matches the incoming request, the corresponding action is taken.

Multiple patterns for the same pattern list must be entered on different lines.

Rules Template Processing Considerations

Actions and patterns have a predefined order of execution. A group of rules with the same action is always executed either before or after another group of rules with a different action. The **block**, **rewrite**, and **redirect** rule actions support the following additional patterns: **request-line**, **referer**, and **user-agent** regular expressions. The **request-line** regular expression matches the first line of the

request. The **user-agent** regular expression matches the User-Agent header value of the request. The **referer** regular expression matches the Referer header value of the request. The order is not affected by the order in which the rules are entered using CLI commands.

Allow and **block** carry the same precedence. The order of execution depends on the order of configuration between **allow** and **block** actions. Other actions always take precedence over **allow**.

Among rules of the same action, a predefined execution order exists among the rule patterns, which means that within a group of rules of the same action, one group of rules with the same pattern is always executed either before or after another group of rules with a different pattern.

Among all rules of the same action and of the same rules pattern, the rules are evaluated in a Last-Entered-First-Examined fashion (the reverse of the order in which the rules were entered). This order is not affected by the order in which the rules are entered using CLI commands.

Most actions do not have any parameters.

Service Rules for URLs

There are three cases for service rules:

1. If allow rules are configured, then it is an implicit deny.
2. If deny rules are configured then it is implicit allow.
3. If both allow and deny are configured, then it is an implicit allow.

For example, if all URL requests that match HTML are blocked, implicitly, all requests that match other URL requests are allowed.

If all URL requests that match WMV are allowed, implicitly, all request that match other URL requests are blocked.

If both of the above rules are configured, then HTML URL requests are blocked, and all other URL requests are allowed.

Examples

The following example shows that the SE is configured to replace the internal.domain.com string in a request to the server named dummy:

```
ServiceEngine(config)# rule action rewrite header-field referer internal.domain.com dummy
```

The following example shows that if an empty string is given as a replacement pattern, then the referer header is stripped. This rule states that all requests, which have a referer header that indicates a corporate internal server in ABCBigCorp, strip the referer field so that the outside web server does not see the name of the corporate internal server.

```
ServiceEngine(config)# rule action rewrite header-field referer internal.abcbigcorp.com ""
```

The following example shows that the **rule pattern-list** command is configured to add a pattern to an existing pattern list to perform an action to be defined on destination IP address 172.16.25.25 using the dst-ip pattern:

```
ServiceEngine#show rule pattern-list 10 all
```

```
Rules Template Configuration
```

```
-----
```

```
Rule Processing Enabled
```

```
Pattern-Lists :
```

```
rule pattern-list 11 dst-ip 172.16.25.25 255.255.255.0
```

```
rule pattern-list 11 domain foo.com
```

The following example shows that the **rule action block** command is configured and associated with an existing pattern list:

```
ServiceEngine(config)#rule action block pattern-list 10 protocol all
ServiceEngine#show rule action block
Rules Template Configuration
-----
Rule Processing Enabled

Actions :

rule action block pattern-list 10 protocol all
```

The following example shows that the **rule action block** command is configured and associated with an existing pattern list, which lists as its pattern the domain yahoo.com:

```
ServiceEngine(config)#rule pattern-list 10 domain yahoo.com
ServiceEngine#show rule pattern-list 10 all
Rules Template Configuration
-----
Rule Processing Enabled

Pattern-Lists :

rule pattern-list 10 domain yahoo.com
ServiceEngine(config)#rule action block pattern-list 10 protocol all
```

In this example, the request (using HTTP) to yahoo.com was denied three times.

The following example shows that the **rule action block** command (action) blocks all patterns specified with the **rule pattern-list 12** command:

```
ServiceEngine(config)#rule pattern-list 12 domain \.foo.com
ServiceEngine(config)#rule action block pattern-list 12
ServiceEngine(config)#
```

The following example prevents caching of requests that match a URL request that contains the ***cgi-bin*** string:

```
ServiceEngine(config)#rule pattern-list 13 url-regex \.*cgi-bin.*
ServiceEngine(config)#rule action no-cache pattern-list 13
ServiceEngine(config)#
```

The actions that are to be taken by the rules are configured through the **rule action** commands. Patterns that are to be matched to a particular pattern that you specify are configured through **rule pattern-list** commands.

The following example shows how patterns use AND by configuring patterns with the same pattern list number and applying that pattern list to an action:

```
ServiceEngine(config)#rule action block pattern-list 1
ServiceEngine(config)#rule pattern-list 1 url-regex yahoo
ServiceEngine(config)#rule pattern-list 1 dst-port 80
```

Other options of the **rule** command work similarly to the preceding examples.

The following example redirects a request for old-domain-name that has been changed to new-domain-name:

```
Cache(config)#rule action redirect http://old-domain-name/ pattern-list 1 protocol http
Cache(config)#rule pattern-list 1 url-regex http://old-domain-name/
http://new-domain-name/
```

The following example redirects requests from an IETF site to a site that is locally mirrored:

```
Cache(config)#rule action redirect http://www.ietf.org/rfc/(.*) pattern-list 2 protocol http
```

The following example shows that if the request URL is `http://www.ietf.org/rfc/rfc1111.txt`, the SE rewrites the URL as `http://wwwin-eng.cisco.com/RFC/RFC/rfc1111.txt` and sends a 302 Temporary Redirect response with the rewritten URL in the Location header to the client. The browser automatically initiates a request to the rewritten URL.

```
Cache(config)#rule pattern-list 2 url-regex http://www.ietf.org/rfc/(.*)  
http://wwwin-eng.cisco.com/RFC/RFC/\1
```

The following example redirects all requests for `linux.org` to a local server in India that is closer to where the SE is located:

```
Cache(config)#rule action redirect http://linux.org/(.*) pattern-list 3 protocol http
```

The following example shows that two URLs are to be matched if the pattern is **url-regex**. If the URLs that are given in the action configuration are invalid, a warning is displayed during the configuration of this rule. The action URL is taken when the header field patterns are configured.

```
Cache(config)#rule pattern-list 3 url-regex http://linux.org/(.*) http://linux.org.in/\1
```

The following example bypasses requests with `cisco.com` as the domain from URL filtering:

```
ServiceEngine(config)#rule action no-url-filtering pattern-list 6 protocol all  
ServiceEngine(config)#rule pattern-list 6 domain cisco.com
```

Related Commands

clear
show rule

script

To execute a script provided by Cisco or check the script for errors, use the **script** EXEC command.

script {**check** | **execute**} *file_name*

Syntax Description	check	Checks the validity of the script.
	execute	Executes the script. The script file must be a sysfs file in the current directory.
	<i>file_name</i>	Name of the script file.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines The **script** EXEC command opens the script utility, which allows you to execute Cisco-supplied scripts or check errors in those scripts. The script utility can read standard terminal input from the user if the script you run requires inputs from the user.



Note

The script utility is designed to run only Cisco-supplied scripts. You cannot execute script files that lack Cisco signatures or that have been corrupted or modified.

Examples The following example checks for errors in the script file foo.script:

```
ServiceEngine#script check foo.script
```

```
Script file foo.script is valid.
```


service-router

To configure service routing, use the **service-router** global configuration command. To disable last-resort routing, use the **no** form of this command.

On the SE:

```
service-router {keepalive-interval num | service-monitor {number-of-samples {all num | cpu
num | disk num | fms num | kmemory num | memory num | wmt num | nic num} | sample-period
{all num | cpu num | disk num | fms num | kmemory num | memory num | movie-streamer num
| nic num | wmt num} | threshold {all num | cpu num | disk num | failcntdisk num | fms num |
kmemory num | memory num | nic num | wmt num} | type {all | cpu | disk | failcntdisk | fms
| kmemory | memory | nic | wmt}}}
```

no service-router

On the SR:

```
service-router {access-policy enable | content-based-routing {enable | redundant} | dns-ttl num
| lastresort {domain name {allow all | alternate name} | error-domain name error-file} |
location-based-routing { enable | geo-location-server {primary ip address num | secondary
ip address num}} | proximity-based-routing {enable | proximity-cache timeout num |
proximity-server ip address num} | redirect-mode { ip-redirect} | service-monitor
{number-of-samples {all num | cpu num | disk num | kmemory num | memory num}} |
sample-period {cpu num | disk num | failcntdisk num| kmemory num | memory num} |
threshold {all num | cpu num | disk num | kmemory num | memory num} | type {all | cpu |
disk | kmemory | memory}}
```

no service-router

Syntax Description

keepalive-interval	Specifies the SR keepalive interval in seconds.
<i>num</i>	Number of seconds (1-120).
service-monitor	Configures Service Monitor related parameters.
number-of-samples	Counts the latest sampled values to be used when calculating average.
all	Sets to all monitor types.
<i>num</i>	Count of latest sampled values to be used when calculating average (1-120).
cpu	Enables the monitor CPU load.
disk	Sets the disk monitor type.
fms	Sets the Flash Media Server (FMS) monitor type.
kmemory	Sets the monitor kernel memory type.
memory	Sets the monitor memory type.
wmt	Sets the Windows Media Technology (WMT) monitor type.
nic	Sets the Network Interface Card monitor type.
sample-period	Configures the time interval between two consecutive samples.
<i>num</i>	Time interval between two consecutive samples in seconds (1-160).
threshold	Configures threshold values.
failcntdisk	Sets the disk failure monitor type.

<i>num</i>	The disk FailureCnt threshold value.
movie-streamer	Sets the Movie Streamer monitor type.
type	Configures the type to be monitored.
access-policy	Configures the service-router access-policy.
enable	Enables access-policy.
content-based-routing	Configures content based routing.
enable	Enables content based routing.
redundant	Specifies the number of redundant copies of the content.
<i>num</i>	Number of redundant copies of the content (1-4).
dns-ttl	Configures Time to Live (TTL) of Domain Name Server (DNS) records issued by SR.
<i>num</i>	Number of seconds (1-60).
lastresort	Configures the lastresort domain.
domain	Configures the domain.
<i>name</i>	Domain name.
allow	Allows the client to be routed through an alternate domain or origin server.
all	Allows all requests.
alternate	Configures an alternate domain.
<i>name</i>	Alternate domain name.
error-domain	Configures error domain.
<i>name</i>	Error domain name.
error-file	Configures error file name.
<i>name</i>	Error file name.
location-based-routing	Configures location-based routing.
enable	Enables location-based routing.
geo-location-server	Configures geo location server IP address and port.
primary	Configures the primary geographical (geo) location server IP address and port.
<i>ip address</i>	IP address of primary geo location server.
<i>num</i>	Port number of primary geo location server.
secondary	Configures the secondary geo location server IP address and port.
<i>ip address</i>	IP address of secondary geo location server.
<i>num</i>	Port number of secondary geo location server.
proximity-based-routing	Configures proximity-based routing.
enable	Enables proximity-based routing.
proximity-cache	Configures proximity cache.
timeout	Configures proximity cache timeout.
<i>num</i>	Proximity cache timeout in seconds (1-86400).
proximity-server	Configures proximity server IP address and port.
<i>ip address</i>	IP address of proximity server.
<i>num</i>	Port number of proximity server (1-65535).

redirect-mode	Configures the service router redirect mode.
ip-redirect	Enables IP redirection.
service-monitor	Configures service monitor parameters.
number-of-samples	Counts the latest sampled values to be used when calculating average.
all	Allows all monitor types.
<i>num</i>	Count of latest sampled values to be used when calculating average (1-120).
cpu	Sets the CPU monitor type.
disk	Sets the disk monitor type.
kmemory	Sets the monitor kernel memory.
memory	Sets the monitor memory.
failcntdisk	Sets the disk failure monitor type.
sample-period	Configures the time interval between two consecutive samples.
threshold	Configures threshold values.
type	Configures the type to be monitored.

Defaults

keepalive-interval: 2 seconds
redundant copies: 1 copy
dns-ttl: 60 seconds
proximity cache timeout: 1800 seconds
sample-period: 1 second
nic sample-period: 3 seconds
number of samples: 2 samples

Command Modes

Global configuration

Usage Guidelines

To configure last-resort routing, use the **service-router** global configuration command, where domain is the service routing domain name, and alternate is where to route requests.

Last-resort routing is applicable when load-based routing is enabled and all SEs have exceeded their thresholds or all SEs in the domain are offline. The SR can redirect requests to a configurable alternate domain when all SEs serving a client network region are overloaded.



Note

If the last-resort domain is not configured and the SE thresholds are exceeded, requests are redirected to the origin server.

Crossdomain Support

When a client requests the content from a portal and the content then makes a request to a different remote domain (or origin server), the request cannot be served unless the origin server or the remote domain has a crossdomain.xml that grants access to the original portal to continue with the streaming.

For example, a client request for abc.com/streaming.html (which has the content), makes a request for cds-origin.com/vod/sample.flv (which is a different domain), then the client must request a crossdomain.xml. The crossdomain.xml allows access to abc.com and can then stream sample.flv. If the cds-origin.com does not have crossdomain.xml, then the request is denied.

**Note**

In the case of Flash, the request is made for crossdomain.xml. In the case of Silverlight the request is made for clientaccesspolicy.xml.

Instead of directly going to cds-origin.com, the request first comes to the service router. So when the request for crossdomain.xml comes to the service router, it is served to the client. This xml grants access to the portal for the file requested. So the client then sends the request for the file which is served.

**Note**

For Silverlight the client access policy is requested only when web service calls are made. Depending on the client player, for both Silverlight and Flash applications, the clientaccesspolicy.xml and crossdomain.xml need to be provisioned on the origin server.

FLVPlaybackComponent does not currently crossdomain requests for video files. The crossdomain request is issued only when a query string is present. In such cases, the video gets downloaded but does not play.

The number of the HTTP Requests (normal) in Request Received (“show statistics service-router summary”) should increase.

Examples

The following example shows how to configure the keepalive interval:

```
ServiceRouter(config)#service-router keepalive-interval 2
```

The following example shows how to configure the service monitor type:

```
ServiceRouter(config)#service-router service-monitor type all
```

Crossdomain Support

The following example shows how to enable crossdomain support:

```
ServiceEngine(config)#service-router access-policy enable
```

The following example shows how to disable crossdomain support:

```
ServiceEngine(config)#no service-router access-policy enable
```

Related Commands

show service-router

setup

To configure basic configuration settings (general settings, device network settings, and disk configuration) on the SE and a set of commonly used caching services, use the **setup** EXEC command. You can also use the **setup** EXEC command to complete basic configuration after upgrading.

setup

Syntax Description	This command has no arguments or keywords.

Defaults	No default behavior or values.

Command Modes	EXEC

Examples	The following example shows the part of the output when you enter the setup EXEC command on an SE running the Internet Streamer CDS software:

```
ServiceEngine#setup
```

```
Here is the current profile of this device
```

```
CDN device                : Yes
```

```
Do you want to change this (y/n) [n]:
```

```
Press the ESC key at any time to quit this session
```

show access-lists

To display the access control list (ACL) configuration, use the **show access-lists 300** EXEC command.

show access-lists 300

Syntax Description None

Command Default No default behavior or values.

Command Modes EXEC

Examples [Table 2-12](#) describes the fields shown in the **show access-lists 300** display.

Table 2-12 *show access-lists Field Descriptions*

Field	Description
Access Control List Configuration	
Access Control List is enabled	Configuration status of the access control list option.
Groupname and username-based List	Lists the group name-based access control lists.

Related Commands access-lists

show acquirer

To display the acquirer information and progress of content acquisition for a specified channel number or name, use the **show acquirer** EXEC command.

show acquirer [**delivery-service** {**delivery-service-id** *delivery-service-id* | **delivery-service-name** *delivery-service-name*} | **progress** {**delivery-service-id** *delivery-service-id* | **delivery-service-name** *delivery-service-name*} | **proxy authentication**]

Syntax Description	
delivery-service	Displays acquirer information for the delivery service.
delivery-service-id	(Optional) Displays the ID for the delivery service.
<i>delivery-service-id</i>	Delivery service ID.
delivery-service-name	(Optional) Displays the name for the delivery service.
<i>delivery-service-name</i>	Delivery service name.
progress	(Optional) Displays the acquisition progress for the specified channel.
proxy	(Optional) Displays the proxy information for the acquirer.
authentication	Displays the proxy authentication details for the acquirer.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines The **show acquirer progress** command displays information for all channels for which the SE is the root SE. It displays the number of acquired objects in relation to the total number of objects for both a single item or crawler jobs. When an acquisition is in progress, it displays the number of data bytes currently being downloaded in relation to the total size of the object and its URL. The **show acquirer progress** command also displays information about the authentication that allows the acquirer to access content through a transparent or nontransparent proxy server.

The **show acquirer proxy authentication** command displays the proxy authentication configuration for the acquirer if you have enabled content acquisition through a proxy server and proxy authentication is configured. Use the **acquirer proxy authentication outgoing** global configuration command to configure authentication when you enable content acquisition through a proxy server. You must first configure the proxy host and the port using the **http proxy outgoing host** global configuration command.

When you enable content acquisition through a proxy server, you can provide the proxy configuration and proxy authentication information in the manifest file. If the proxy and proxy authentication are configured in the manifest file, the **show acquirer proxy authentication** command does not display any proxy details.

Examples The **show acquirer progress** EXEC command displays the progress of the acquirer for a specified channel. If a specific channel is not mentioned, the display shows the progress for all the channels for which the SE is the root.

Table 2-13 describes the fields shown in the **show acquirer progress** display.

Table 2-13 *show acquirer progress Field Descriptions*

Field	Description
Channel-id	Numerical identifier for the channel.
Channel-Name	Name for the channel.
Acquired Single Items	Total number of single items completed out of all of the single items specified in the manifest. For example, 200/301 shows that all 200 items out of a total of 301 items have been acquired.
Acquired Crawl Items	Total number of links with crawling completed out of the total crawlable items for each crawling task specified in the manifest, along with the starting URL.
Download Size (Bytes)	Current URL fetched by the acquirer for the channel, if applicable, along with the file size details.

The following example shows the output from the **show acquirer proxy authentication** command when there are no proxies configured using the **acquirer proxy authentication** global configuration command:

```
ServiceEngine#show acquirer proxy authentication
No proxy authentication information configured
```

The following example shows the output from the **show acquirer proxy authentication** command after configuring the proxy using the **acquirer proxy authentication** global configuration command:

```
ServiceEngine#show acquirer proxy authentication
acquirer proxy authentication outgoing 172.28.225.29 8080 admin password **** My-Domain
basic-auth-disable
acquirer proxy authentication transparent admin password **** My-Domain basic-auth-disable
```

Related Commands

acquirer (global configuration)
http
show statistics acquirer

show alarms

To display information on various types of alarms, their status, and history, use the **show alarms** EXEC command.

```
show alarms [critical [detail [support]] | detail [support] | history [[start_num [end_num [detail
[support]] | detail [support]]] | critical [start_num [end_num [detail [support]] | detail
[support]]] | detail [support] | major [start_num [end_num [detail [support]] | detail
[support]]] | minor [start_num [end_num [detail [support]]] | detail [support]]] | major
[detail [support]] | minor [detail [support]] | status]
```

Syntax Description

critical	(Optional) Displays critical alarm information.
detail	(Optional) Displays detailed information for each alarm.
support	(Optional) Displays additional information about each alarm.
history	(Optional) Displays information about the history of various alarms.
<i>start_num</i>	(Optional) Alarm number that appears first in the alarm history.
<i>end_num</i>	(Optional) Alarm number that appears last in the alarm history.
major	(Optional) Displays information about major alarms.
minor	(Optional) Displays information about minor alarms.
status	(Optional) Displays the status of various alarms and alarm overload settings.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

The Node Health Manager enables CDS applications to raise alarms to draw attention to error or significant conditions. The Node Health Manager, which is the data repository for such alarms, aggregates the health and alarm information for the applications, services (for example, the cache service), and resources (for example, disk drives) that are being monitored on the SE. For example, the Node Health Manager gives you a mechanism to determine if a monitored application (for example, the HTTP proxy caching service) is alive on the SE. These alarms are referred to as Internet Streamer CDS software alarms.

The Internet Streamer CDS software uses SNMP to report error conditions by generating SNMP traps. In the Internet Streamer CDS software, the following SE applications can generate an Internet Streamer CDS software alarm:

- Node Health Manager (alarm overload condition and Node Manager aliveness)
- Node Manager for service failures (aliveness of monitored applications)
- System Monitor (sysmon) for disk failures

The three levels of alarms in the Internet Streamer CDS software are as follows:

- **Critical**—Alarms that affect the existing traffic through the SE and are considered fatal (the SE cannot recover and continue to process traffic).
- **Major**—Alarms that indicate a major service (for example, the cache service) has been damaged or lost. Urgent action is necessary to restore this service. However, other node components are fully functional and the existing service should be minimally impacted.
- **Minor**—Alarms that indicate that a condition that will not affect a service has occurred but corrective action is required in order to prevent a serious fault from occurring.

You can configure alarms using the **snmp-server enable traps alarm** global configuration command.

Use the **show alarms critical** EXEC command to display the current critical alarms being generated by the Internet Streamer CDS software applications. Use the **show alarms critical detail** EXEC command to display additional details for each of the critical alarms being generated. Use the **show alarms critical detail support** EXEC command to display an explanation about the condition that triggered the alarm and how you can find out the cause of the problem. Similarly, you can use the **show alarms major** and **show alarms minor** EXEC commands to display the details of major and minor alarms.

Use the **show alarms history** EXEC command to display a history of alarms that have been raised and cleared by the Internet Streamer CDS software on the SE. The Internet Streamer CDS software retains the last 100 alarm raise and clear events only.

Use the **show alarm status** EXEC command to display the status of current alarms and the SE's alarm overload status and alarm overload configuration.

Examples

[Table 2-14](#) describes the fields shown in the **show alarms history** display.

Table 2-14 *show alarms history Field Descriptions*

Field	Description
Op	Operation status of the alarm. Values are R—Raised or C—Cleared.
Sev	Severity of the alarm. Values are Cr—Critical, Ma—Major, or Mi—Minor.
Alarm ID	Type of event that caused the alarm.
Module/Submodule	Software module affected.
Instance	Object that this alarm event is associated with. For example, for an alarm event with the Alarm ID disk_failed, the instance would be the name of the disk that failed. The Instance field does not have pre-defined values and is application specific.

[Table 2-15](#) describes the fields shown in the **show alarms status** display.

Table 2-15 *show alarms status Field Descriptions*

Field	Description
Critical Alarms	Number of critical alarms.
Major Alarms	Number of major alarms.
Minor Alarms	Number of minor alarms.
Overall Alarm Status	Aggregate status of alarms.

Table 2-15 *show alarms status Field Descriptions (continued)*

Field	Description
Device is NOT in alarm overload state.	Status of the device alarm overload state.
Device enters alarm overload state @ 999 alarms/sec.	Threshold number of alarms per second at which the device enters the alarm overload state.
Device exits alarm overload state @ 99 alarms/sec.	Threshold number of alarms per second at which the device exits the alarm overload state.
Overload detection is enabled.	Status of whether overload detection is enabled on the device.

Related Commands

alarm overload-detect
snmp-server enable traps

show arp

To display the Address Resolution Protocol (ARP) table, use the **show arp** EXEC command.

show arp

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes EXEC

Examples The **show arp** command displays the Internet-to-Ethernet address translation tables of the Address Resolution Protocol. Without flags, the current ARP entry for the hostname is displayed.

[Table 2-16](#) describes the fields shown in the **show arp** display.

Table 2-16 *show arp Field Descriptions*

Field	Description
Protocol	Type of protocol.
Address	Ethernet address of the hostname.
Flags	Current ARP flag status.
Hardware Addr	Hardware Ethernet address given as six hexadecimal bytes separated by colons.
Type	Type of wide-area network.
Interface	Type of Ethernet interface.

show authentication

To display the authentication configuration, use the **show authentication** EXEC command.

show authentication user

Syntax Description	user Displays the authentication configuration for the user login to the system.
Defaults	No default behavior or values.
Command Modes	EXEC
Related Commands	authentication authentication clear show statistics authentication

show authsvr

To display the status of the Authorization server, use the **show authsvr** EXEC command.
show authsvr [unknown-server]

Syntax Description	unknown-server (Optional) Shows the allow and deny rule for unknown configured servers or domains.
Defaults	No default behavior or values.
Command Modes	EXEC
Examples	The following example shows the status of the Authorization server: <pre>ServiceEngine#show authsvr Authserver is Enabled</pre>
Related Commands	authsvr

show bandwidth

To display the bandwidth allocated to a particular device, use the **show bandwidth** EXEC command.

show bandwidth [**flash-media-streaming** | **movie-streamer** | **wmt**]

Syntax Description	flash-media-streaming (Optional) Displays the Flash media streaming bandwidth settings.
	movie-streamer (Optional) Displays the Movie Streamer bandwidth settings.
	wmt (Optional) Displays Windows Media Technology (WMT) bandwidth settings.

Defaults No default behavior or values.

Command Modes EXEC

Examples [Table 2-17](#) describes the fields shown in the **show bandwidth** display.

Table 2-17 *show bandwidth Field Descriptions*

Field	Description
Module	Types of application servers for which bandwidth allocation is displayed: • wmt incoming is for incoming WMT streaming content requests from end users. • wmt outgoing is for outgoing WMT media from SEs. • movie-streamer incoming is for incoming Movie Streamer content requests from end users. • movie-streamer outgoing is for outgoing Movie Streamer media from SEs. • flash-media-streaming is for Flash Media Streaming.
Bandwidth Kbps	Maximum amount of bandwidth that you want allowed in kilobits per second (kbps) for a particular period of time. Incoming and outgoing bandwidth enforced is 8000000 kbps.
Start Time	Time of the day for the bandwidth rate setting to begin, using a 24-hour clock in local time on the SE (hh:mm).
End Time	Time of the day for the bandwidth rate setting to end, using a 24-hour clock in local time on the SE (hh:mm).
Default Bandwidth Kbps	Amount of default bandwidth (in kbps). The default bandwidth is the amount of bandwidth associated with each content service type when there is no scheduled bandwidth.
Max Bandwidth Kbps	Maximum bandwidth (in kbps) permitted by the system license. This bandwidth specifies the upper limit of allowable bandwidth.

■ show bandwidth

Related Commands bandwidth (global configuration)

show banner

To display information on various types of banners, use the **show banner** EXEC command.

show banner

Syntax Description	This command has no arguments or keywords.

Defaults	No default behavior or values.

Command Modes	EXEC

Examples	Table 2-18 describes the fields shown in the show banner display.

Table 2-18 *show banner Field Descriptions*

Field	Description
Banner is enabled.	Configuration status of the banner feature.
MOTD banner is: abc	Displays the configured message of the day.
Login banner is: acb	Displays the configured login banner.
Exec banner is: abc	Displays the configured EXEC banner.

Related Commands	banner

show bitrate

To display the bit rate allocated to a particular device, use the **show bitrate** EXEC command.

show bitrate [**movie-streamer** | **wmt**]

Syntax Description	movie-streamer	(Optional) Displays the Movie Streamer bit rate settings.
	wmt	(Optional) Displays Windows Media Technology (WMT) bit rate settings.

Defaults No default behavior or values.

Command Modes EXEC

Examples [Table 2-19](#) describes the fields shown in the **show bitrate** display.

Table 2-19 *show bitrate Field Descriptions*

Field	Description
Module	Types of application servers for which the bit rate is displayed: • wmt outgoing is the maximum bit rate per WMT stream that can be served by the SE. • wmt incoming is the maximum bit rate per WMT stream that can be received by the SE. • movie-streamer outgoing is the maximum bit rate per streamer that can be served by the SE. • movie-streamer incoming is the maximum bit rate per streamer that can be received by the SE.
Default Bitrate Kbps	Bit rate associated with the application servers when the bit rate has not been configured on the SE.
Configured Bitrate Kbps	Bit rate configured on the SE in kilobits per second.

Related Commands **bitrate**

show cache

To display a list of cached contents, use the **show cache** EXEC command.

show cache [**content num**]

Syntax Description	content	Displays a list of cached contents in order of decreasing priority.
	num	Specifies number of cached contents to be displayed (1-1000).

Defaults Number of cached contents is 100.

Command Modes EXEC

Usage Guidelines The **show cache** command allows users to check the cached content in an SE. Users can also view the priority, size, and URL information through this command.

Examples The following example shows the cached contents:

```
ServiceEngine#show cache content 1000
Max-cached-entries is set as 1000
Number of cal cached assets: 12
-----
Priority      Size      URL
-----
1.09887e+00  16      rtsp://72.163.255.118/c.wmv
1.04340e+00  416     rtsp://72.163.255.118/c.wmv.Ui4HeLMPgB5lLH_+bo2d.03.bmp
6.71782e-01  957     rtsp://72.163.255.118/c.wmv.hdr
5.74964e-01  16      rtsp://72.163.255.118/4.wmv
5.60340e-01  664997  rtsp://72.163.255.118/c.wmv.Ui4HeLMPgB5lLH_+bo2d.03
3.15230e-01  665107  http://72.163.255.118/c.wmv
2.39938e-01  5409    rtsp://72.163.255.118/4.wmv.hdr
2.02040e-01  35256   rtsp://72.163.255.118/4.wmv.rPgfTr1Lo0dT6FJWaxDs.03.bmp
1.59027e-01  873664  http://72.163.255.118/4.flv
1.45368e-01  3603032 http://72.163.255.118/b.wmv
1.23161e-01  70517409 rtsp://72.163.255.118/4.wmv.rPgfTr1Lo0dT6FJWaxDs.03
7.88076e-02  29180088 http://72.163.255.118/4.wmv
```

Related Commands cache

show capability

To display the capabilities of the Cap-X profile ID, use the **show capability** EXEC command.

show capability profile ID *profile ID*

Syntax Description	profile ID	Displays information for the Cap-X profile.
	<i>profile ID</i>	Profile ID number. The range is 1-65535.

Defaults	No default behavior or values.

Command Modes	EXEC

Related Commands	capability

show cdnfs

To display CDS network file system (cdnfs) information, use the **show cdnfs** EXEC command.

show {cdnfs volumes | usage}

Syntax Description	volumes	Displays CDS network file system volumes.
	usage	Displays Content Delivery Network (CDN) current usage.

Defaults	No default behavior or values.

Command Modes	EXEC

Examples	Table 2-20 describes the fields shown in the show cdnfs volumes display.

Table 2-20 *show cdnfs volumes Field Descriptions*

Field	Description
cdnfs 00–04	CDS network file system and disk number.
nnnnnnKB	Size of the volume in kilobytes.

Related Commands	cdnfs disk (EXEC) show disks show statistics cdnfs

show clock

To display the system clock, use the **show clock** EXEC command.

show clock [**detail** | **standard-timezones** {**all** | **details** *timezone* | **regions** | **zones** *region-name*}]

Syntax Description		
detail	(Optional) Displays detailed information; indicates the Network Timing Protocol (NTP) clock source and the current summer time setting (if any).	
standard-timezones	(Optional) Displays information about the standard time zones.	
all	Displays all of the standard time zones (approximately 1500 time zones). Each time zone is listed on a separate line.	
details	Displays detailed information for the specified time zone.	
<i>timezone</i>	Name of the time zone.	
regions	Displays the region name of all the standard time zones. All 1500 time zones are organized into directories by region.	
zones	Displays the name of every time zone that is within the specified region.	
<i>region-name</i>	Name of the region.	

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines The CDS has several predefined standard time zones. Some of these time zones have built-in summertime information while others do not. For example, if you are in an eastern region of the United States (US), you must use the US/Eastern time zone that includes summertime information and will adjust the clock automatically every April and October. There are about 1500 standard time zone names.

The **clock summertime** command is disabled when a standard time zone is configured. You can only configure summertime if the time zone is not a standard time zone (if the time zone is a customized zone).

In addition, CLI commands exist to enable you to display a list of all the standard time zones. The **show clock standard-timezones all** EXEC command enables you to browse through all standard time zones and choose from these predefined time zones. You can choose a customized name that does not conflict with the predefined names of the standard time zones. Most predefined names of the standard time zones have two components, a region name and a zone name. You can list time zones by several criteria, such as regions and zones.

Examples

Table 2-21 describes the field in the **show clock** display.

Table 2-21 *show clock Field Description*

Field	Description
Local time	Day of the week, month, date, time (hh:mm:ss), and year in local time relative to the UTC offset.

Table 2-22 describes the fields shown in the **show clock detail** display.

Table 2-22 *show clock detail Field Descriptions*

Field	Description
Local time	Local time relative to UTC.
UTC time	Coordinated Universal Time (UTC) date and time.
Epoch	Number of seconds since Jan. 1, 1970.
UTC offset	UTC offset in seconds, hours, and minutes.

The following example shows an excerpt of the output from the **show clock standard-timezones all** EXEC command. As the following example shows, all of the standard time zones (approximately 1500 time zones) are listed. Each time zone is listed on a separate line.

```
ServiceEngine # show clock standard-timezones all
Africa/Abidjan
Africa/Accra
Africa/Addis_Ababa
Africa/Algiers
Africa/Asmera
Africa/Bamako
Africa/Bangui
Africa/Banjul
Africa/Bissau
Africa/Blantyre
Africa/Brazzaville
Africa/Bujumbura
Africa/Casablanca
Africa/Ceuta
Africa/Conakry
Africa/Dakar
Africa/Dar_es_Salaam
Africa/Djibouti
.
.
.
```

The following example shows an excerpt of the output from the **show clock standard-timezones region** EXEC command. As the example shows, all first level time zone names or directories are listed. All 1500 time zones are organized into directories by region.

```
ServiceEngine # show clock standard-timezones regions
Africa/
America/
Antarctica/
Arctic/
Asia/
Atlantic/
Australia/
```

show clock

```
Brazil/
CET
.
.
.
```

The following example shows an excerpt of the output from the **show clock standard-timezones zones** EXEC command. As the following example shows, this command lists the name of every time zone that is within the specified region (for example, the US region).

```
ServiceEngine # show clock standard-timezones zones US
Alaska
Aleutian
Arizona
Central
East-Indiana
Eastern
Hawaii
Indiana-Starke
Michigan
Mountain
Pacific
Samoa
```

The following example shows an excerpt of the output from the **show clock standard-timezones details** EXEC command. This command shows details about the specified time zone (for example, the US/Eastern time zone). The command output also includes the standard offset from the Greenwich mean time (GMT).

```
ServiceEngine # show clock standard-timezones details US/Eastern
US/Eastern is standard timezone.
Getting offset information (may take a while) ...
Standard offset from GMT is -300 minutes (-5 hour(s)).
It has built-in summertime.
Summer offset from GMT is -240 minutes. (-4 hour(s)).
```

Related Commands**clock (EXEC)****clock (global configuration)**

show cms

To display the Centralized Management System (CMS) embedded database content and maintenance status and other information, use the **show cms** EXEC command.

```
show cms {database {content {dump filename | text | xml} | maintenance [detail]} | info |
processes}
```

Syntax Description	
database	Displays embedded database maintenance information.
content	Writes the database content to a file.
dump	Dumps all database content to a text file.
<i>filename</i>	Name of the file to be saved under local1 directory.
text	Writes the database content to a file in text format.
xml	Writes the database content to a file in XML format.
maintenance	Shows the current database maintenance status.
detail	(Optional) Displays database maintenance details and errors.
info	Displays CMS application information.
processes	Displays CMS application processes.

Defaults No default behavior or values.

Command Modes EXEC

Examples [Table 2-23](#) describes the fields shown in the CDSM **show cms info** display.

Table 2-23 show cms Field Descriptions for the CDSM

Field	Description
CDN information	
Model	Model name of the device.
Node Id	Unique identifier given to the device by the CDSM at registration, which is used to manage the device.
Device Mode	Configured mode of device used during registration.
Current CDSM role	Role of the current CDSM: Primary or Standby.
CMS services information	
Service cms_httpd is running	Status of the cms_httpd management service (running or not running). This field is specific to the CDSM only.
Service cms_cdsd is running	Status of the cms_cdsd management service (running or not running). This field is specific to the CDSM only.

Table 2-24 describes the fields shown in the SE **show cms info** display.

Table 2-24 *show cms Field Descriptions for the SE*

Field	Description
CDN information	
Model	Model name of the device.
Node Id	Unique identifier given to the device by the CDSM at registration, which is used to manage the device.
Device Mode	Configured mode of device used during registration.
Current CDSM address	Address of the CDSM as currently configured in the cdsm ip global configuration command. This address may differ from the registered address if a standby CDSM is managing the device instead of the primary CDSM with which the device is registered.
Registered with CDSM	Address of the CDSM with which the device is registered.
Status	Connection status of the device to the CDSM. This field may contain one of three values: Online, Offline, or Pending.
Time of last config-sync	Time when the device management service last contacted the CDSM for updates.

The following example writes the database content to a file in text format:

```
CDSM# show cms database content text
Database content can be found in /local1/cms-db-12-12-2002-17:06:08:070.txt.
```

The following example writes the database content to a file in XML format:

```
CDSM# show cms database content xml
Database content can be found in /local1/cms-db-12-12-2002-17:07:11:629.xml.
```

The following example shows the output of the **show cms database maintenance detail** on an SE:

```
ServiceEngine#show cms database maintenance detail
Database maintenance is not running.
Regular database maintenance is enabled.
Regular database maintenance schedule is set on Sun, Mon, Tue, Wed, Thu, Fri, Sat at 02:00
Full database maintenance is enabled.
Full database maintenance schedule is set on Sun, Mon, Tue, Wed, Thu, Fri, Sat at 04:00
Disk usage for STATE partition: Total: 1523564K, Available: 1443940K, Use: 6%

DATABASE VACUUMING DETAILS AND ERRORS
-----
Database Vacuuming never performed or it did not complete due to error.
Latest Vacuuming status :No Error
Last Vacuum Error : No Error
Last Reindex Time : Thu Jul 15 02:02:49 2004
Latest Reindexing status :No Error
Last Reindex Error: No Error
ServiceEngine#
```

Related Commands

cms (EXC)
cms (global configuration)

show content

To display all content entries in the CDS, use the **show content** EXEC command.

show content {**all** [**background** | **brief**] | **url** *url* [**brief**]}

Syntax Description	all	Displays all cached content into a file.
	<i>name</i>	The output file to log cache content query results.
	background	(Optional) Run this command in background.
	brief	(Optional) Using brief display mode.
	url	Displays the cached content object with original URL.
	<i>url</i>	The original URL for cache content object query.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines This command allows users to check the cached or pre-positioned content in an SE. Through this command, users can view content attributes such as status and file size.

Examples The following example displays the RTSP URL in the CDS:

```
ServiceEngine#show content url rtsp://www.cht.com/CHT_2M.wmv
CAL content object attributes:
URL: rtsp://www.cht.com/CHT_2M.wmv
Status is 2 (Servable)
File size is 16 Bytes
Playable by WMT
Authorization is Not Required
Content is CACHED with priority 0.574964
```

The following example displays all content entries in the CDS:

```
ServiceEngine#show content all name background
Command running in background...
ServiceEngine#USER INFO: Your 'show content all' command finished
```

show debugging

To display the state of each debugging option, use the **show debugging** EXEC command.

show debugging

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

This command displays only the type of debugging enabled, not the specific subset of the command.

Examples

In the following example, the **debug icp client** command coupled with the **show debugging** command shows that Internet Cache Protocol (ICP) debugging is enabled:

```
ServiceEngine#debug icp client
ServiceEngine#show debugging
Debug icp (client) is on
```

Related Commands

debug
undebug

show device-mode

To display the configured or current mode of a device, use the **show device-mode** EXEC command.

show device-mode {configured | current}

Syntax Description	configured	Displays the configured device mode.
	current	Displays the current device mode.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines If the configured and current device modes differ, a reload is required for the configured device mode to take effect.

Examples The configured device mode field in the **show device-mode configured** display shows the device mode that has been configured, but has not yet taken effect. The current device mode field in the the **show device-mode current** display shows the current mode in which the CDS device is operating.

The following example shows how to use the **show device-mode** command to show the device mode when you change the device from an SE to an SR using the **device mode** command:

```
Acmehost# show device-mode current
Current device mode: service-engine
Acmehost# show device-mode configured
Configured device mode: service-engine
Acmehost(config)#device mode service-router
The new configuration will take effect after a reload
Acmehost(config)#exit
Acmehost# show device-mode current
Current device mode: service-engine
Note: The configured and current device modes differ,
a reload is required for the configured device mode to
take effect.
Acmehost# show device-mode configured
Configured device mode: service-router
Note: The configured and current device modes differ,
a reload is required for the configured device mode to
take effect.
Acmehost# write memory
Acmehost# reload force
...reload...

Acmehost# show running-config
device mode service-router
!
hostname Acmehost
..
```

show device-mode

```
Acmehost# show device-mode configured
Configured device mode: service-router
Acmehost# show device-mode current
Current device mode: service-router
```

Related Commands **device**

show direct-server-return

To display the Direct Server return information, use the **show direct-server-return** EXEC command.

show direct-server-return

Syntax Description	This command has no keywords or arguments.

Defaults	No default behavior or values.

Command Modes	EXEC

Examples	The following example displays the Direct Server return information:

```
ServiceEngine#show direct-server-return
direct-server-return vip 11.11.11.11
```

Related Commands	direct-server-return

show disks

To view information about your disks, use the **show disks** EXEC command.

show disks [**current** | **details** | **raid-state** | **SMART-info** [**details**]]

Syntax Description	current	(Optional) Displays currently effective configurations.
	details	(Optional) Displays currently effective configurations with more details.
	raid-state	(Optional) Shows the volume and progress information for the RAID disks.
	SMART-info	(Optional) Displays hard drive diagnostic information and information about impending disk failures.
	details	(Optional) Displays more detailed SMART disk-monitoring information.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines The **show disks** command displays the names of the disks currently attached to the SE.

Proactively Monitoring Disk Health with SMART

The ability to proactively monitor the health of disks with Self Monitoring, Analysis, and Reporting Technology (SMART) was added. SMART provides you with hard drive diagnostic information and information about impending disk failures.

SMART is supported by most disk vendors and is a standard method used to determine the health of a disk. SMART has several read-only attributes (for example, the power-on hours attribute, the load and unload count attribute) that provide the CDS software with information regarding the operating and environmental conditions that may indicate an impending disk failure.

To display more detailed information, enter the **show disks SMART-info details** EXEC command. The output from the **show disks SMART-info** and the **show disks SMART-info details** commands will differ based on the disk vendor and the type of drive technology (Integrated Drive Electronics [IDE], Small Computer Systems Interface [SCSI], and Serial Advanced Technology Attachment [SATA] disk drives).

Even though SMART attributes are vendor dependent, there is a common way of interpreting most SMART attributes. Each SMART attribute has a normalized current value and a threshold value. When the current value exceeds the threshold value, the disk is considered as failed. The CDS software monitors the SMART attributes and reports any impending failure through syslog messages, SNMP traps, and alarms.

The output from the **show tech-support** EXEC command also includes SMART information.

Filter Out Multiple Syslog Messages for a Single Failed Sector on SCSI, IDE, and SATA Disk Drives

Many disk failure messages were generated when a single disk sector failed, which caused an unnecessary alarm. Changes for suppressing multiple syslog messages on a single sector failure have been implemented for IDE disk drives. This fix has also been extended to SCSI and SATA disk drives.

Examples

Table 2-25 describes the fields shown in the **show disks details** display.

Table 2-25 *show disks details Field Descriptions*

Field	Description
disk00	Availability of the disk: Present, Not present or Not responding, Not used, or (*). Note Disk drives that are currently marked as bad are shown as “Not used” in the output. Future bad disk drives (drives that will not be used after the next time that the SE is reloaded) are shown with an asterisk (*). Disk identification number and type. Disk size in megabytes and gigabytes.
disk01	Same type of information is shown for each disk.
System use	Amount of disk space being used for system use.
Free	Amount of unused disk space available.

SMART support is vendor dependent; each disk vendor has a different set of supported SMART attributes. The following example shows the output from the **show disks SMART-info EXEC** command that was entered on two different SEs (Service Engine A and Service Engine B). These two SEs contain hard disks that were manufactured by different vendors.

```
ServiceEngine#show disks SMART-info
=== disk00 ===
smartctl version 5.38 [i686-spcdn-linux-gnu] Copyright (C) 2002-8 Bruce Allen
Home page is http://smartmontools.sourceforge.net/

=== START OF INFORMATION SECTION ===
Device Model: ST3500320NS
Serial Number: 5QM19RKR
Firmware Version: SN04
User Capacity: 500,107,862,016 bytes
Device is: Not in smartctl database [for details use: -P showall]
ATA Version is: 6
ATA Standard is: ATA/ATAPI-6 T13 1410D revision 2
Local Time is: Thu May 21 14:09:19 2009 UTC
SMART support is: Available - device has SMART capability.
SMART support is: Enabled

=== START OF READ SMART DATA SECTION ===
SMART overall-health self-assessment test result: PASSED

RUNNING: /usr/sbin/smartctl /dev/sda -H -i

=== disk01 ===
smartctl version 5.38 [i686-spcdn-linux-gnu] Copyright (C) 2002-8 Bruce Allen
Home page is http://smartmontools.sourceforge.net/

=== START OF INFORMATION SECTION ===
Device Model: ST3500320NS
Serial Number: 5QM19B0B
Firmware Version: SN04
User Capacity: 500,107,862,016 bytes
Device is: Not in smartctl database [for details use: -P showall]
ATA Version is: 6
```

■ show disks

```

ATA Standard is: ATA/ATAPI-6 T13 1410D revision 2
Local Time is: Thu May 21 14:09:19 2009 UTC
SMART support is: Available - device has SMART capability.
SMART support is: Enabled

=== START OF READ SMART DATA SECTION ===
SMART overall-health self-assessment test result: PASSED

RUNNING: /usr/sbin/smartctl /dev/sdb -H -i

=== disk02 ===
smartctl version 5.38 [i686-spcdn-linux-gnu] Copyright (C) 2002-8 Bruce Allen
Home page is http://smartmontools.sourceforge.net/

=== START OF INFORMATION SECTION ===
Device Model: ST3500320NS
Serial Number: 5QM19SK9
Firmware Version: SN04
User Capacity: 500,107,862,016 bytes
Device is: Not in smartctl database [for details use: -P showall]
ATA Version is: 6
ATA Standard is: ATA/ATAPI-6 T13 1410D revision 2
Local Time is: Thu May 21 14:09:19 2009 UTC
SMART support is: Available - device has SMART capability.
SMART support is: Enabled

=== START OF READ SMART DATA SECTION ===
SMART overall-health self-assessment test result: PASSED

RUNNING: /usr/sbin/smartctl /dev/sdc -H -i

```

Table 2-26 describes some typical fields in the **show disks SMART-info** display.

Table 2-26 *show disks SMART-info Field Descriptions*

Field	Description
disk00—disk05	Shows information for disk drives.
Device Model	Vendor number and version number of the disk.
Serial Number	Serial number for the disk.
Device type	Type of device.
Transport protocol	Physical layer connector information, for example: Parallel SCSI (SPI-4).
Local time is	Day of the week, month, date, time (hh:mm:ss), year, clock standard.
Device supports SMART and SMART is Enabled	Status of SMART support: Enabled or Disabled.
Temperature Warning Enabled	Temperature warning status: Enabled or Disabled.
SMART Health Status:	Health status of the disk: OK or Failed.

Related Commands

disk (EXEC)

show distribution

To display the distribution information for a specified delivery service and to probe a remote SE for the liveness of its associated delivery service, use the **show distribution** EXEC command.

```
show distribution [delivery-services {delivery-service-id delivery-service-num |  
delivery-service-name delivery-service-name}]
```

```
show distribution [forwarder-list {delivery-service-id delivery-service-num |  
delivery-service-name delivery-service-name} | detail]
```

```
show distribution [location {forwarder-load-weight | live-load-weight |  
location-leader-preference} {delivery-service-id delivery-service-num |  
delivery-service-name delivery-service-name}]
```

```
show distribution [object-status object-url]
```

```
show distribution [processes]
```

```
show distribution [remote ip-address {metadata-sender delivery-service-id  
delivery-service-num [start-generation-id gen-id end-generation-id gen-id] | unicast-sender  
delivery-service-id delivery-service-num {cdn-url cdn_url | probe | relative-cdn-url  
cdn_url}}]
```

```
show distribution [remote traceroute {forwarder-next-hop delivery-service-id  
delivery-service-num {max-hop maxhop_num | trace-till-good | trace-till-root} |  
unicast-sender delivery-service-id delivery-service-num {cdn-url cdn_url | probe |  
relative-cdn-url cdn_url} {max-hop maxhop_num | trace-till-good | trace-till-root}}]
```

Syntax Description

delivery-services	(Optional) Displays information about the specified delivery service.
delivery-service-id	(Optional) Specifies the delivery service ID.
<i>delivery-service-num</i>	Delivery service number (64-bit number).
delivery-service-name	(Optional) Specifies the delivery service name.
<i>delivery-service-name</i>	Delivery service name.
forwarder-list	(Optional) Displays the forwarder lists for all delivery services subscribed to by the SE.
detail	(Optional) Displays detailed forwarder lists for all delivery services subscribed to by the SE.
location	(Optional) Displays delivery service routing-related parameters for the SEs in the location (specified by the delivery service ID).
forwarder-load-weight	Displays the forwarder load weight value of the SEs in the location (specified by the delivery service ID). For more information, see the “Forwarder Probability” section on page 2-229 .
live-load-weight	Displays the live load weight value of the SEs in the location (specified by the delivery service ID). For more information, see the “Live Splitting Probability” section on page 2-231 .
location-leader-preference	Displays the location leader preference value of the SEs in the location (specified by the delivery service ID). For more information, see the “Location Leader Preference” section on page 2-230 .

show distribution

object-status	(Optional) Displays information on the status of a pre-positioned object.
<i>object-url</i>	URL of the pre-positioned object.
processes	(Optional) Displays information on distribution processes.
remote	(Optional) Displays delivery service information about a remote SE.
<i>ip-address</i>	IP address of the remote SE.
metadata-sender	Displays the metadata from a remote SE.
start-generation-id	(Optional) Specifies the beginning database value of the current version of the multicast cloud.
<i>gen_id</i>	Beginning database value.
end-generation-id	Specifies the ending database value of the current version of the multicast cloud.
<i>gen_id</i>	Ending database value.
unicast-sender	Displays the unicast data from a remote SE.
cdn-url	Checks the object on a remote SE using the specified URL.
<i>cdn_url</i>	CDS network URL used to check the object on a remote SE.
probe	Probes the remote unicast sender.
relative-cdn-url	Checks the object on a remote SE using the specified URL.
traceroute	Displays the traceroute for the delivery service routing status.
forwarder-next-hop	Displays the next forwarder in the path for the SE. Note This keyword lets you display the forwarding SEs to the root SE in a manner similar to the traceroute command.
delivery-service-id	Specifies the delivery service ID with which the unicast sender is associated.
<i>delivery-service-num</i>	Delivery service number of the delivery service with which the unicast sender is associated.
max-hop	Displays the maximum number of hops needed to reach the unicast sender.
<i>maxhop_num</i>	Maximum number of hops (1–1024).
trace-till-good	Allows the device to trace the route of an object until the object is found.
trace-till-root	Allows the device to trace the route of an object until the device reaches the root SE.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Use the **show distribution remote *ip-address* metadata-sender delivery-service-id *delivery-service-num* [start-generation-id *gen_id* end-generation-id *gen_id*]** command option to retrieve the metadata from a remote SE assigned to a specified delivery service ID. The start and end generation IDs specify the beginning and ending database values representing the current version of the multicast cloud stored in the local database.

**Note**

Generation IDs must be greater than zero. Also, you must specify both the start and the end generation IDs, or neither ID.

The **show distribution remote** *ip-address unicast-sender delivery-service-id delivery-service-num relative-cdn-url cdn-url* command shows the status of the relative CDS network URL of an object at a remote SE assigned to a specified delivery service ID. A relative CDS network URL is one that lacks the prefix of the protocol and hostname. For example, the relative CDS network URL for <http://www.mycompany.com/abc.def.html> is [abc.def.html](#).

Use the **show distribution remote** *ip-address unicast-sender delivery-service-id delivery-service-num probe* command to probe a remote SE for the liveness of the delivery service to which it is assigned.

The **show distribution object-status** *object-url* command can be used to display the properties of a pre-positioned object.

You can view the location leader preference and forwarder weight for the SE using the **show distribution** command. However, you can configure the location leader preference and forwarder weight only using the CDSM GUI for each SE. Default values are assumed if you do not manually configure them.

The **show distribution location forwarder-load-weight** command displays the probability of SEs assigned to the delivery service within the location being selected as a forwarder. The **show distribution location location-leader-preference** command displays the location leader preference value of SEs that are assigned to the delivery service within the location.

Use the **show distribution delivery-services** command to view the forwarder for the SEs. If a receiver SE is unable to find its forwarder SE, one of the following reasons is displayed in the Status/Reason column of the output of the **show distribution delivery-services** command:

- LLMT—The home SE cannot find the forwarder because the home SE has a limit on the forwarder lookup level.
- FAIL—The home SE cannot find the forwarder because there is a failed SE along the path within the specified forwarder lookup level.
- NGWT—The home SE cannot find the forwarder because there is an SE with a negative forwarder-load-weight along the path within the specified forwarder lookup level.

Forwarder Probability

When an SE (location leader) selects its forwarder from an upstream location, it uses the *forwarderLoad-weight* value configured for each SE in its upstream location. The weight value of each SE corresponds to the probability of the SE being selected as the forwarder.

Each SE generates a unique random number. When an SE needs to select an inter-location forwarder, it views all the SEs in one remote location as a collection, with the size corresponding to their weight. It uses the generated random number to select an SE as a forwarder. SEs with a higher weight are more likely to be selected as forwarders.

**Note**

The *forwarderLoad-weight* value represents a probabilistic value. When a large number of children SEs select a forwarder from a location, the load on the forwarder represents the weight.

The load on the forwarder is the replication load per delivery service on the SE because all SEs subscribed to the delivery service will select a forwarder to balance the load. However, as the number of SEs assigned to different delivery services might differ, a forwarder might receive requests for

content from SEs in other delivery services, which increases the load. Therefore, it is possible that the total load (of replicating content) on the forwarder does not reflect the weight but depends on the number of SEs assigned to a delivery service.

For each SE, you can specify the probability of each SE acting as a forwarder to SEs from downstream locations using the CDSM GUI. You can also specify whether certain SEs should never serve as a forwarder to downstream SEs. The specification is delivery service independent.

If you choose not to configure settings using the Location Leader and Forwarder Settings for SE window, the delivery service routing algorithm uses the random number method to generate one permutation of the SE ID ordered list.

Location Leader Preference

For intra-location (list of SEs in an SE's own location) forwarder selection, the delivery service routing algorithm first creates an ordered list of the SEs based on their *location leader-preference* in a descending order. Next, the delivery service routing algorithm will select the first SE in the ordered list as the location leader.

When multiple SEs have the same *location leader-preference*, the delivery service routing algorithm guarantees that all the SEs assigned to each delivery service in the location still generate the same ordered list, which avoids routing loops. A routing loop is a deadlock situation in which the forwarder selection among multiple SEs within the loop prevents the SEs from receiving the content from upstream locations. For example, SE1 uses SE2 as the forwarder and SE2 uses SE1 as the forwarder for the same delivery service.

However, for two different delivery services, the ordered list could be different (when multiple SEs have the same location leader probability value) even if the subscribed SEs are the same. When multiple SEs have the highest *location leader-preference*, although each SE has an equal chance of acting as the location leader (for different delivery services), only one SE always acts as the location leader for one particular delivery service. If you configure all the SEs in your network to have the same *location leader-preference* value, then each SE has an equal chance of acting as a location leader. When each SE has an equal probability of being selected as the location leader for any particular delivery service, only one particular SE is always selected as the location leader.



Note

If there are two SEs in the same location (SE1, SE2) and both of them are assigned to two delivery services (CH1, CH2), and if you want SE1 to be the location leader for CH1 and SE2 to be the location leader for CH2, you cannot configure them using *location leader-preference* and *forwarderLoad-weight*.

In a location, you can specify the probability for each SE acting as the location leader. The specification is delivery service independent.

The following limitations are associated with specifying a location leader preference:

- When multiple SEs are configured with the same *location leader-preference* value and assigned to a delivery service, they have an equal probability of being selected as the location leader. In such a case, you do not have a control mechanism to decide which SE should be selected as the location leader.
- Only the order among the SEs with the highest preference is randomized to determine the location leader preference and not other SEs with the same preference value. It is possible that if the SE(s) with the highest preference failed and there are several other SEs with the second highest preference value, they will not be balanced across the different delivery services. The same SE will be the location leader for all delivery services.
- If an SE with a high *location leader-preference* is assigned to many delivery services, it is possible that the SE can be selected as the location leader for all these delivery services.

Live Splitting Probability

Similar to the delivery service routing application used for content replication that assigns weight and priority to SEs to tune location leader and forwarder selections, you can specify a configuration parameter *liveSplit-load-weight* for each SE. This parameter represents the relative probability that an SE is likely to receive live stream splitting traffic as compared to other SEs. The specification is delivery service independent. If you do not configure *liveSplit-load-weight*, the algorithm should work as it currently does.

A weighted load balancing scheme splits the live stream load on the SEs according to the *liveSplit-load-weight* value because SEs of different types have an equal probability of being selected as the splitting SE on the location path.

The *liveSplit-load-weight* is used when the delivery service routing generates the ordered list of SEs for each location. The SEs are ordered in a way that the higher the weight, the greater probability that the SEs are being ordered at the beginning of the list.

The weight represents a relative value. The *liveSplit-load-weight* assigned to one SE is compared against the weights of other SEs in the same location.

The weight is a probabilistic value. For one particular URL, all SEs generate the same ordered list for a location.

It is possible that an SE with a lower weight is being ordered at the beginning while an SE with a higher weight is being ordered at the end of the list. The weighted load balancing is useful only when there are multiple live stream URLs.

The *liveSplit-load-weight* parameter applies both within the home location and upstream locations. This setting is different from the distribution settings where *locationLeader-priority* controls how you choose SEs from the home location, while *forwarderLoad-weight* controls how you choose SEs from upstream locations.

Examples

The following examples show various ways of using the **show distribution remote** commands.

The following example shows the status of the object at a remote SE with the IP address 172.16.2.160 and delivery service ID 631. The URL of the content object specified in the command must not be the complete source URL. Instead, it must be the relative CDS network URL of the object.

```
ServiceEngine#show distribution remote 172.16.2.160 unicast-sender delivery-service-id 631
relative-cdn-url 101files/100.txt
```

```
Forwarder-Name : AD-SE08
Forwarder-ID : 140
Forwarder IP : 2.43.10.70
Forwarder Location : default-location

Relative CDN URL : 101files/100.txt
Actual Size : 58
Size Transferred : 58
Resource-ID : roVe2aMzp+YhmbhGUfMPpQ
Content-ID : 7LC5xOlMp4YvkBJlHaQucQ
Last Modified Time : 10:52:38 Jan 04 2005
```

The following example retrieves the metadata from a remote SE with the IP address 172.16.2.160 assigned to delivery service ID 4999:

```
ServiceEngine#show distribution remote 172.16.2.160 metadata-sender delivery-service-id
4999
```

```
Getting meta data for delivery service(4999) from genid -1 to 2
Connecting to 2.43.10.101
Remote SE replied with the following headers:
  Action : Processing metadata records
  Latest Gen id is : 2
  Have more records to process : No
  Is metadata still in full reload: No
add-size: 2, del-size: 0

Add Logs: 1 to 2
  add #1: UBsSUMwbTdJzzpqDvxSdYg..., basic_auth/public.html
  add #2: NJyVL9CZwpnyCfw+Is26yw..., index.txt
```

The following example probes the remote SE with the IP address 172.16.2.160 for the liveness of its assigned delivery service ID 153:

```
ServiceEngine#show distribution remote 172.16.2.160 unicast-sender delivery-service-id 153
probe
Probe Successful
```

The following example shows the beginning database value of the current version of the multicast cloud at a remote SE with the IP address 10.43.10.101 and delivery service ID 4999:

```
ServiceEngine# show distribution remote 10.43.10.101 metadata-sender delivery-service-id
4999 start-generation-id 0 end-generation-id 5
Getting meta data for delivery service(4999) from genid -1 to 5
Connecting to 10.43.10.101
Remote SE replied with the following headers:
  Action : Processing metadata records
  Latest Gen id is : 2
  Have more records to process : No
  Is metadata still in full reload: No
add-size: 2, del-size: 0

Add Logs: 1 to 2
  add #1: UBsSUMwbTdJzzpqDvxSdYg..., basic_auth/public.html
  add #2: NJyVL9CZwpnyCfw+Is26yw..., index.txt
```


**Note**

When start and end generation IDs are not specified in the **show distribution remote** command, the current maximum generation ID of -100 will be the start generation ID. The end generation ID is equal to the sum of the start generation ID and 100.

The following example shows the list of forwarders in the path toward the root SE:

```
ServiceEngine#show distribution remote traceroute forwarder-next-hop delivery-service-id
4999 trace-till-root
```

Hop	NextHop_SEId	NextHop_SEName	NextHop_SEIp	GenID	Status/Reason
1	5884	AD-SE07	192.168.1.69	1	REGULAR
2	6035	AD-SE13	2.43.10.101	1	LOC-LEAD
3	5683	AD-SE12	2.43.10.100	1	LOC-LEAD
4	6026	gnadaraj-507	2.43.27.2	1	LOC-LEAD
5	5638	devi-507	2.43.27.36	1	LOC-LEAD (Reached RootSE)

The following example shows output from the **show distribution object-status** command:

```
ServiceEngine#show distribution object-status http://www.cisco.com/index.txt
```

```
===== Website Information =====
```

```
Name                : cisco-crawl
Origin Server FQDN   : www.cisco.com
Request Routed FQDN  : N/A
Content UNS Reference # : 1
```

```
===== delivery services Information =====
```

```
*** delivery service 4999 (name = headercheck) ***
```

Object Replication

```
-----
Replication           : Done
File State            : Ready for distribution
Multicast for delivery service : Not Enabled
Replication Lock      : Received by Unicast-Receiver/Acquirer
Reference Count       : 1
Total Size            : 2208640
Transferred Size      : 2208640
MD5 of MD5            : zwhJagyCmRAE4UmTwc0EtA..
Source Url            : http://liqq-linux.cisco.com/index.txt
Source Last Modified Time : Sun Jul 11 03:23:33 2004
```

Object Properties

```
-----
Redirect To Origin    : Yes
Requires Authentication : No
Alternative URL       :
Serve Start Time      : N/A
Serve End Time        : N/A
Play servers          : HTTP HTTPS
Content Metadata       : None
Content uns_id         : yhzR3VZ96MDz5FVHwmGD+A..
Content gen-id         : 5638:1108022220:1
```

```
===== CDNFS Information =====
```

show distribution

```

Internal File Name      :
/disk00-04/d/http-liqq-linux.cisco.com-azk2lrqzsytweswexham5w/32/326cf0278da48aac82d796cb1
19b1caa.0.data.txt
Actual File Size        : 2208640 bytes
MD5 of MD5 (Re-calculated): zwhJagyCmRAE4UmTwc0EtA..
Content metadata        : None
Metadata match with     : delivery service 4999
Number of Source-urls   : 1

```

Source-url to CDN-object mapping:

```

Source-url              : http://liqq-linux.cisco.com/index.txt
Used by CDN object      : ---- Yes ----
Internal File Name      :
/disk00-04/d/http-liqq-linux.cisco.com-azk2lrqzsytweswexham5w/32/326cf0278da48aac82d796cb1
19b1caa.0.data.txt
Actual File Size        : 2208640 bytes

```

===== CDNFS lookup output =====

CDNFS File Attributes:

```

Status                  3 (Ready)
File Size                2208640 Bytes
Start Time              null
End Time                null
Allowed Playback via    HTTP HTTPS
Last-modified Time      Sun Jul 11 03:23:33 2004
cdn_uns_id              yhzR3VZ96MDz5FVHwmGD+A..
last-modified           Sun, 11 Jul 2004 03:23:33 GMT

```

Internal path to data file:

```

/disk00-04/d/http-liqq-linux.cisco.com-azk2lrqzsytweswexham5w/32/326cf0278da48aac82d796cb1
19b1caa.0.data.txt

```

The **show distribution delivery-services** output and the **show distribution forwarder-list** output display additional delivery service routing information. The newly added Status/Reason field displays whether the SE is a location leader and the reason for not having a forwarder SE.

The following example shows the delivery service distribution information:

ServiceEngine#**show distribution delivery-services**

Delivery Service Name	ID	Priority	Root	Forwarder	Status/Reason
00-AD	527	500	No	Rack89-SE-11	REGULAR N/A
01-AD	586	500	Yes	N/A	N/A
00-Live	588	500	Yes	N/A	LIVE N/A

```

LOC-LEAD: This SE is the location leader for this delivery service
REGULAR:  This SE is not the location leader for this delivery service
LLMT:     This SE cannot find forwarder because this SE has limit on
           the forwarder lookup level
FAIL:     This SE cannot find forwarder because there is failed SE along
           the path within specified forwarder lookup level
NGWT:     This SE cannot find forwarder because there is SE with negative
           forwarder-load-weight along the path within the specified
           forwarder lookup level
LIVE:     The specified delivery service is live delivery service, forwarder not
applicable
*:        MetaData forwarder and Unicast forwarder are different

```

The following example provides delivery service distribution information for delivery service ID 527:

```
ServiceEngine#show distribution delivery-services delivery-service-id 527
```

```
Delivery service Configuration
```

```
-----
Delivery service ID           :           527
Delivery service Name        :           00-AD
Website Name                  :           Test1
Website Origin FQDN          :           www.test.com
Delivery service Priority     :           500
Configured Distribution Type  :           Multicast only
```

```
Root SE Information
```

```
-----
ID of Configured Root SE     :           462
Name of Configured Root SE   :           Rack89-SE-11
IP of Configured Root SE     :           2.43.27.38
ID of Effective Root SE      :           462
Current root-ce-uid          :           1110247321
This SE's Role                :           Not a Root SE
This SE in Full Reload       :           No
```

```
Root SE Failover/Fallback Information
```

```
-----
Root SE Failover/Fallback Interval :           120 Mins
```

```
Metadata Information
```

```
-----
Metadata-Forwarder ID       :           462
Metadata-Forwarder Name     :           Rack89-SE-11
Metadata-Forwarder Primary IP :           2.43.27.38
Metadata-Forwarder NAT IP/Port :           N/A
Address to Poll Metadata-Forwarder :           Primary IP
Metadata-Forwarder Status    :           REGULAR
Last gen-id Switch          :           Never
Current low-water-marker     :           1
Current max-gen-id           :           0
Current max-del-gen-id       :           0
Last poll                   :           13 Secs ago
Next poll                   :           107 Secs from now
Idle poll interval          :           120 Secs
Poll interval multiplier     :           1
```

```
Unicast Information
```

```
-----
Ucast-Forwarder ID         :           462
Ucast-Forwarder Name       :           Rack89-SE-11
Ucast-Forwarder Primary IP :           2.43.27.38
Ucast-Forwarder NAT IP/Port :           N/A
Address to Poll Ucast-Forwarder :           Primary IP
Ucast-Forwarder Status     :           REGULAR
```

```
Multicast Information
```

```
-----
```

```
QoS Configuration
```

```
-----
MetaData QoS (system config) :           16 (Effective)
```

```
Progress Information
```

```
-----
Number of jobs completed     :           0
Has incomplete jobs          :           No
```

show distribution

LOC-LEAD: This SE is the location leader for this delivery service
 REGULAR: This SE is not the location leader for this delivery service
 LLMT: This SE cannot find forwarder because this SE has limit on
 the forwarder lookup level
 FAIL: This SE cannot find forwarder because there is failed SE along
 the path within specified forwarder lookup level
 NGWT: This SE cannot find forwarder because there is SE with negative
 forwarder-load-weight along the path within the specified
 forwarder lookup level
 LIVE: The specified delivery service is live delivery service, forwarder not
 applicable
 *: MetaData forwarder and Unicast forwarder are different



Note

The Has Unfinished Job line is only available if the SE is *not* a root SE. It is only available on a receiver SE.

Related Commands

show statistics distribution

show flash

To display the flash memory version and usage information, use the **show flash** EXEC command.

show flash

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

If a new software image has been installed and is waiting to be run after a reboot, the **show flash** command displays this information and the version of Internet Streamer CDS software that will run on the device after reload.

Examples

The following example displays the flash information:

```
ServiceEngine#show flash
CDS software version (disk-based code): CDS-2.4.0-b328

System image on flash:
Version: 2.4.0.328

System flash directory:
System image: 274 sectors
Bootloader, rescue image, and other reserved areas: 59 sectors
512 sectors total, 179 sectors free.
```

[Table 2-27](#) describes the fields shown in the **show flash** display.

Table 2-27 *show flash Field Descriptions*

Field	Description
Internet Streamer CDS software version (disk-based code)	Internet Streamer CDS software version and build number that is running on the device.
System image on flash:	
Version	Version and build number of the software that is stored in flash memory.
System flash directory:	
System image	Number of sectors used by the system image.
Bootloader, rescue image, and other reserved areas	Number of sectors used by the bootloader, rescue image, and other reserved areas.
XX sectors total, XX sectors free	Total number of sectors. Number of free sectors.

show flash-media-streaming

To display the Flash Media Streaming information, use the **show flash-media-streaming** EXEC command.

On the SE:

```
show flash-media-streaming [license | logging name | mtrack | stream-status {dvrcast [all name]
| live [all name]}]
```

On the SR:

```
show flash-media-streaming
```

Syntax Description

license	Shows the Flash Media Streaming licenses.
logging	Sets the Tar Flash Media Streaming transaction logs to /local/local1/filename.tar.gz.
<i>name</i>	Filename.
mtrack	Displays the Flash Media Streaming memory usage.
stream-status	Displays the Flash Media Streaming stream status.
dvrcast	Displays dvrcast stream status.
all	(Optional) Dumps detail statistics into /local/local1/filename.
live	Displays the live stream status.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

When you execute the **show flash-media-streaming stream-status live** command and the Forwarder is a Content Origin server running Linux, the **show** command does not show statistics for the Content Origin server.

Examples

The following example displays the Flash media streaming information:

```
ServiceEngine#show flash-media-streaming
Flash Media Streaming is disabled.
Max. Allowed concurrent sessions are 200.
Flash Media Streaming Monitoring is enabled.
Admin list allow: 1.1.1.1
Total number of wholesale licenses is 0.
Bandwidth Details:
Non wholesale bandwidth (Perpetual) is 200000 kbps.
Configured max bandwidth is 10000 kbps.
Total wholesale bandwidth (Term Based) is 0 kbps.
Allowed bandwidth is 10000 kbps.
```

Related Commands

flash-media-streaming
show statistics flash-media-streaming

show ftp

To display the caching configuration of the File Transfer Protocol (FTP), use the **show ftp** EXEC command.

show ftp

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes EXEC

Examples This example lists the caching configuration of FTP:

```
ServiceEngine#show ftp
```

```
FTP heuristic age-multipliers: directory-listing 30% file 60%
Maximum Time To Live in days : directory-listing 3 file 7
Minimum Time To Live in minutes: 60
No objects are revalidated on every request.
Serve-IMS without revalidation if...
Directory listing object is less than 50% of max age
File object is less than 80% of max age
Incoming Proxy-Mode:
Servicing Proxy mode FTP connections on ports: 22 23 88 66 48 488 449 90
Outgoing Proxy-Mode:
Not using outgoing proxy mode.
Maximum size of a cacheable object is unlimited.
```


show hardware

To display the system hardware status, use the **show hardware** EXEC command.

show hardware

Syntax Description	This command has no arguments or keywords.

Defaults	No default behavior or values.

Command Modes	EXEC

Usage Guidelines	In Internet Streamer CDS Release 2.4, the output of the show hardware EXEC command displays the version of the TV-out hardware that the SE is equipped with. In the following excerpt of the sample output from the show hardware command, this particular information is highlighted in bold. Rev 3 in the command output indicates that the TV-out hardware uses the newer Revision 3 MPEG decoder PCI part. The Vela II Revision D and Revision E cards use the Revision 3 part.

```
ServiceEngine#show hardware
.
.
.
Total 1 CPU.
1024 Mbytes of Physical memory.
1 CD ROM drive (CD-224E)
1 AV card (Vela II)
2 GigabitEthernet interfaces
1 Console interface
2 USB interfaces [Not supported in this version of software]

The following PCI cards were found:
PCI-Slot-1 MPEG-Decoder-AV [1105:8476 (Sigma Designs, Inc.) (rev 3)]
PCI-Slot-2 SCSI
Manufactured As: Pre-FCS 565 [867383Z]
.
.
.
```

The output of the **show hardware** EXEC command notifies you if the SE is running a version of the CDS software that does not support the TV-out hardware contained in the SE. In the following example, you are notified that the SE has a Vela II audio-video (AV) card that is not supported by the version of the CDS software that is running on the SE. In the following excerpt of the sample output from the **show hardware** command, this particular information is highlighted in bold:

```
ServiceEngine # show hardware

CPU 0 is GenuineIntel Intel(R) Celeron(R) CPU 1.70GHz (rev 1) running at 1699MHz
.
Total 1 CPU.
1024 Mbytes of Physical memory.
1 CD ROM drive (CD-224E)
1 AV card (Vela II) [***Revision not supported in this version of software***]
2 GigabitEthernet interfaces
1 Console interface
```

show hardware

2 USB interfaces [Not supported in this version of software]

The following PCI cards were found:

.
.
.

Examples

Table 2-28 describes the fields shown in the **show hardware** display.

Table 2-28 *show hardware Field Descriptions*

Field	Description
Compiled hour:minute:second month day year by cnbuild	Compile information for the software build.
System was restarted on day of week month day hour:minute:second year	Date and time that the system was last restarted.
The system has been up for X hours, X minutes, X seconds	Length of time the system has been running since the last reboot.
CPU 0 is	CPU manufacturer information.
Total X CPU	Number of CPUs on the device.
XXXX Mbytes of Physical memory	Number of megabytes of physical memory on the device.
X CD ROM drive	Number of CD-ROM drives on the device.
X Console interface	Number of console interfaces on the device.
Cookie info	
SerialNumber	Serial number of the device.
SerialNumber (raw)	Serial number of the device as an ASCII value.
TestDate	Date that the device was tested.
ModelNum (text)	Hardware model of the device.
ModelNum (raw)	Internal model number (ASCII value) that corresponds to the ExtModel number.
HWVersion	Number of the current hardware version.
PartNumber	Not implemented.
BoardRevision	Number of revisions for the current system board.
ChipRev	Number of revisions for the current chipset.
VendID	Vendor ID of the cookie.
CookieVer	Version number of the cookie.
Chksum	Checksum of the cookie showing whether the cookie is valid.
List of all disk drives	
Physical disk information	Lists the disks by number.
disk00	Availability of the disk: Present, Not present or Not responding, or Not used (*). Disk identification number and type. Disk size in megabytes and gigabytes.

Table 2-28 *show hardware Field Descriptions (continued)*

Field	Description
disk01	Same type of information is shown for each disk.
Mounted filesystems	
Device	Path to the partition on the disk.
Type	Type of the file system. Values include PHYS-FS, SYSFS, or cdnfs.
Size	Total size of the file system in megabytes and gigabytes.
Mount point	Mount point for the file system. For example, the mount point for SYSFS is /local/local1.
System use	Amount of disk space being used for system use.
Free	Amount of unused disk space available.

Related Commands**show version**

show hosts

To view the hosts on your SE, use the **show hosts** EXEC command.

show hosts

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes EXEC

Examples The **show hosts** command lists the name servers and their corresponding IP addresses. It also lists the hostnames, their corresponding IP addresses, and their corresponding aliases (if applicable) in a host table summary.

[Table 2-29](#) describes the fields shown in the **show hosts** display.

Table 2-29 *show hosts Field Descriptions*

Field	Description
Domain names	Domain names used by the device to resolve the IP address.
Name Server(s)	IP address of the Domain Name Server (DNS) name server or servers.
Host Table	
hostname	Fully Qualitified Domain Name (FQDN) (that is, hostname and domain) of the current device.
inet address	IP address of the current host device.
aliases	Name configured for the current device based on the host global configuration command.

show http

To display HTTP caching parameters, use the **show http** EXEC command.

show http {age-mult | all | cache-cookie | cache-fill-range | cache-on-abort | object | proxy | reval-each-request | ttl}

Syntax Description		
age-mult		Displays HTTP/1.0 caching heuristic modifiers.
all		Displays all HTTP-related caching configurations.
cache-cookie		Displays the configuration for caching of web objects with associated cookies.
cache-fill-range		Displays the configuration for cache-fill, for a range request starting from 0.
cache-on-abort		Displays the cache-on-abort configuration.
object		Displays the configuration of HTTP objects.
proxy		Displays the proxy mode configuration.
reval-each-request		Displays the revalidation configuration for every request.
ttl		Displays the Time To Live for objects in the cache.

Defaults

No default behavior or values.

Command Modes

EXEC

Examples

The following example lists the configuration and status of HTTP:

```
ServiceEngine#show http all
Basic authenticated objects are not cached.
HTTP heuristic age-multipliers: text 30% binary 60%
Serve-IMS without revalidation if...
  Text object is less than 50% of max age
  Binary object is less than 80% of max age
Objects with associated cookies are not cached
Client no-cache requests are retrieved from the origin server
Cache on abort feature is disabled
Objects will always continue to be cached on a client abort
  Maximum threshold is disabled
  Minimum threshold is disabled
  Percent threshold is disabled
Maximum time to live in days: text 3 binary 7
Minimum time to live for all objects in minutes: 5
Objects are not revalidated on each request
Incoming Proxy-Mode:
  Not servicing incoming proxy mode connections.
Outgoing Proxy-Mode:
  Not using outgoing proxy mode.

Monitor Interval for Outgoing Proxy Servers is 60 seconds

Timeout period for probing Outgoing Proxy Servers is 300000 microseconds
```

show http

Use of Origin Server upon Proxy Failures is disabled.
Persistent connection is enabled and set to all
Persistent connection timeout is 600 seconds
WWW-Authenticate headers containing
No host configured to receive Proxy-Authorization header
No host configured to receive WWW-Authorization header
Maximum size of a cacheable object is unlimited
Requested Object URL validation is enabled
Healing client is disabled

Timeout for responses = 0 seconds
Max number of misses allowed before stop healing mode = 0
Port number for healing request/response = 14333
Http-port to forward http request to healing server = 80

The following example shows the IP address and port numbers of the HTTP incoming and outgoing proxy modes:

```
ServiceEngine#show http proxy
Incoming Proxy-Mode:
  Servicing Proxy mode HTTP connections on port: 8080
Outgoing Proxy-Mode:
  Directing request to proxy server at 10.1.1.1 port 7777
```

Related Commands

http
show statistics http

show icap

To display Internet Content Adaptation Protocol (ICAP) configuration details, use the **show icap** EXEC command.

show icap [*service service_name*]

Syntax Description

service	(Optional) Displays the configurations for the specified service.
<i>service_name</i>	Name of the service.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Use the **show icap** EXEC command to display the current ICAP configuration for the SE. The command output shows the status of the enabled ICAP features, the service definitions, a list of vectoring points, and an ordered list of ICAP services.

To display the definition and status of a specific ICAP service that is configured on the SE, use the **show icap service service_name** EXEC command.

Examples

The following example displays the ICAP configuration for the SE:

```
ServiceEngine#show icap
ICAP global configurations
=====
ICAP apply: RULES
ICAP logging: DEFAULT

ICAP bypass Streaming content: ENABLED
ICAP rescan cached objects on service update: ENABLED

ICAP service configurations
=====
-----
Configurations for service test
-----
Enabled Status: ENABLED
Load Balancing Scheme: Weighted-load
Error handling scheme: Send client error

Vectoring points registered:
reqmod-precachereqmod-postcacherespmod-precache

Servers configured:

server URL:          icap://10.1.1.1:1344/test-icap
```

show icap

```
-----
Configurations for service service
-----
Enabled Status: DISABLED
Load Balancing Scheme: round-robin
Error handling scheme: Bypass

Vectoring points registered:
None

Servers configured:
None

-----
Configurations for service servforicap
-----
Enabled Status: ENABLED
Load Balancing Scheme: round-robin
Error handling scheme: Bypass

Vectoring points registered:
None

Servers configured:

server URL:      icap://1.2.3.4/servforicap
```

Related Commands**icap service**

show interface

To display the hardware interface information, use the **show interface** EXEC command.

show interface { **GigabitEthernet** *slot/port* | **PortChannel** { **1** | **2** } | **standby** *group num* }

Syntax Description		
GigabitEthernet		Selects a Gigabit Ethernet interface to configure.
<i>slot/port</i>		Slot and port number for the selected interface. The slot range is 0 to 2; the port range is 0 to 3. The slot number and port number are separated with a forward slash character (/).
PortChannel		Selects the EtherChannel of interfaces to configure.
1		Sets the port channel interface number to 1.
2		Sets the port channel interface number to 2.
standby		Sets the standby group for the interface.
<i>group num</i>		Group number for the selected interface. The group number range is 1 to 4.

Defaults No default behavior or values.

Command Modes EXEC

Examples [Table 2-30](#) describes the fields shown in the **show interface GigabitEthernet** display.

Table 2-30 *show interface GigabitEthernet Field Descriptions*

Field	Description
Type	Type of interface. Always Ethernet.
Ethernet address	Layer 2 MAC address.
Maximum Transfer Unit Size	Current configured MTU value.
Metric	Metric setting for the interface. The default is 1. The routing metric is used by the routing protocol to determine the most favorable route. Metrics are counted as additional hops to the destination network or host; the higher the metric value, the less favorable the route.
Packets Received	Total number of packets received by this interface.
Input Errors	Number of incoming errors on this interface.
Input Packets Dropped	Number of incoming packets that were dropped on this interface.
Input Packets Overruns	Number of incoming packet overrun errors.
Input Packets Frames	Number of incoming packet frame errors.
Packet Sent	Total number of packets sent from this interface.

Table 2-30 *show interface GigabitEthernet Field Descriptions (continued)*

Field	Description
Output Errors	Number of outgoing packet errors.
Output Packets Dropped	Number of outgoing packets that were dropped by this interface.
Output Packets Overruns	Number of outgoing packet overrun errors.
Output Packets Carrier	Number of outgoing packet carrier errors.
Output Queue Length	Output queue length in bytes.
Collisions	Number of packet collisions at this interface.
Flags	Interface status indicators. Values include Up, Broadcast, Running, and Multicast.
Mode	Setting, transmission mode, and transmission for this interface.

Table 2-31 describes the fields shown in the **show interface PortChannel** display.

Table 2-31 *show interface PortChannel Field Descriptions*

Field	Description
Description	Description of the device, as configured by using the description option of the interface global configuration command.
Type	Type of interface. Always Ethernet.
Ethernet address	Layer 2 MAC address.
Internet Address	Internet IP address configured for this interface.
Broadcast Address	Broadcast address configured for this interface.
Netmask	Netmask configured for this interface.
Maximum Transfer Unit Size	Current configured MTU value.
Metric	Metric setting for the interface. The default is 1. The routing metric is used by the routing protocol. Higher metrics have the effect of making a route less favorable; metrics are counted as addition hops to the destination network or host.
Packets Received	Total number of packets received by this interface.
Input Errors	Number of incoming errors on this interface.
Input Packets Dropped	Number of incoming packets that were dropped on this interface.
Input Packets Overruns	Number of incoming packet overrun errors.
Input Packets Frames	Number of incoming packet frame errors.
Packet Sent	Total number of packets sent from this interface.
Output Errors	Number of outgoing packet errors.
Output Packets Dropped	Number of outgoing packets that were dropped by this interface.
Output Packets Overruns	Number of outgoing packet overrun errors.

Table 2-31 *show interface PortChannel Field Descriptions*

Field	Description
Output Packets Carrier	Number of outgoing packet carrier errors.
Output Queue Length	Output queue length in bytes.
Collisions	Number of packet collisions at this interface.
Flags	Interface status indicators. Values include Up, Broadcast, Running, and Multicast.

[Table 2-32](#) describes the fields shown in the **show interface standby** display.

Table 2-32 *show interface standby Field Descriptions*

Field	Description
Standby Group	Number that identifies the standby group.
Description	Description of the device, as configured by using the description option of the interface global configuration command.
IP address, netmask	IP address and netmask of the standby group.
Member interfaces	Member interfaces of the standby group. Shows which physical interfaces are part of the standby group. Shows the interface definition, such as GigabitEthernet 1/0.
Active interface	Interfaces that are currently active in the standby group.

Related Commands

interface
show running-config
show startup-config

show inventory

To display the system inventory information, use the **show inventory** EXEC command.

show inventory

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

The **show inventory** command allows you to view the unique device identifier information (UDI) for an SE. Typically, Cisco SEs contain the following three identification items, which make up the UDI:

- Product ID (PID)
- Version ID (VID)
- Serial number (SN)

This identity information is stored in the SE nonvolatile memory. Each SE has a unique device identifier (UDI). The UDI shows PID, VID and SN.

The UDI is electronically accessed by the product operating system or network management application to enable identification of unique hardware devices. The data integrity of the UDI is vital to customers. The UDI that is programmed into the SE's nonvolatile memory is equivalent to the UDI that is printed on the product label and on the carton label. This UDI is also equivalent to the UDI that can be viewed through any electronic means and in all customer-facing systems and tools. Currently, there is only CLI access to the UDI; there is no SNMP access to the UDI information.

On newer SE models, you can use the **show inventory** EXEC command to display the SE's UDI. On older SE models, use the **show tech-support** EXEC command to display the SE's UDI.

Examples

The following example shows the inventory information for one of the newer SE models (SE-565):

```
ServiceEngine#show inventory
```

```
PID: SE-565-K9 VID: 0 SN: serial_number
```

In the preceding example, *serial number* is the serial number of the SE. The version ID is displayed as "0" because the version number is not available.

[Table 2-33](#) describes the fields shown in the **show inventory** display.

Table 2-33 *show inventory Field Descriptions*

Field	Description
PID	Product identification (ID) number of the device.
VID	Version ID number of the device. Displays as 0 if the version number is not available.
SN	Serial number of the device.

The following example shows that you must use the **show tech-support** EXEC command to display the inventory information on an older SE model:

```
ServiceEngine# show inventory
Please look at 'sh tech-support' for information!
ServiceEngine# show tech-support
```

Related Commands **show tech-support**

show ip access-list

To display the access lists that are defined and applied to specific interfaces or applications, use the **show ip access-list** EXEC command.

show ip access-list [*acl-name* | *acl-num*]

Syntax Description

<i>acl-name</i>	(Optional) Information for a specific access list, using an alphanumeric identifier up to 30 characters, beginning with a letter.
<i>acl-num</i>	(Optional) Information for a specific access list, using a numeric identifier (0 to 99 for standard access lists and 100 to 199 for extended access lists).

Defaults

Displays information about all defined access lists.

Command Modes

EXEC

Usage Guidelines

Use the **show ip access-list** EXEC command to display the access lists that have been defined on the current system. Unless you identify a specific access list by name or number, the system displays information about all the defined access lists, including the following sections:

- Available space for new lists and conditions
- Defined access lists
- References by interface and application

Examples

The following example shows sample output from the **show ip access-list** command:

```
ServiceEngine#show ip access-list
Space available:
  47 access lists
  492 access list conditions

Standard IP access list 1
  1 permit 10.1.1.2
  2 deny 10.1.2.1
    (implicit deny any: 2 matches)
  total invocations: 2
Extended IP access list 100
  1 permit tcp host 10.1.1.1 any
  2 permit tcp host 10.1.1.2 any
  3 permit tcp host 10.1.1.3 any
    (implicit fragment permit: 0 matches)
    (implicit deny ip any any: 0 matches)
  total invocations: 0
Standard IP access list test
  1 permit 1.1.1.1 (10 matches)
  2 permit 1.1.1.3
  3 permit 1.1.1.2
    (implicit deny: 2 matches)
  total invocations: 12
```

```
Interface access list references:  
  GigabitEthernet 0/0  inbound  100
```

```
Application access list references:  
  tftp_server                standard  1  
  UDP ports:                 69
```

The following example shows sample output from the **show ip access-list** command for the access list named test:

```
ServiceEngine#show ip access-list test  
Standard IP access list test  
  1 permit 1.1.1.1 (10 matches)  
  2 permit 1.1.1.3  
  3 permit 1.1.1.2  
    (implicit deny: 2 matches)  
total invocations: 12
```

**Note**

The system displays the number of packets that have matched a condition statement only if the number is greater than zero.

Related Commands

clear
ip access-list

show ip routes

To display the IP routing table, use the **show ip routes** EXEC command.

show ip routes

Syntax Description	This command has no arguments or keywords.

Defaults	No default behavior or values.

Command Modes	EXEC

Examples	The show ip routes command displays the IP routing table. Table 2-34 describes the fields shown in the show ip routes display.

Table 2-34 *show ip routes Field Descriptions*

Field	Description
Destination	Destination address IP route mask.
Gateway	IP address or IP alias of the gateway router.
Netmask	Subnet mask of the gateway router.

Related Commands	ip

show ldap

To display the Lightweight Directory Access Protocol (LDAP) parameters, use the **show ldap** EXEC command.

show ldap

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes EXEC

Examples [Table 2-35](#) describes the fields shown in the **show ldap** display.

Table 2-35 *show ldap Field Descriptions*

Field	Description
LDAP Authentication	State of LDAP authentication (enabled or disabled).
Allow mode	Access to users when the LDAP server is unavailable.
Base DN	Base distinguished name.
Filter	LDAP filter for authentication group.
Retransmits	Number of retransmissions.
Timeout	Wait time in seconds for an LDAP server to reply.
UID Attribute	User ID attribute on the LDAP server.
Group Attribute	Authentication group attribute: - distinguished name (dn), - unique name (un), - organizational unit (ou) for native LDAP groups, and - member of (memberOf) Active Directory group.
organizationUnit	Group name obtained from the <i>ou</i> attribute of the user account.
Custom Attribute	Group name obtained from the <i>custom</i> attribute of the user account.
Active Directory	Group name obtained from the <i>memberOf</i> attribute of the user account. Note An Active Directory database is a user database that resides on a Windows 2000 server that is running the Microsoft Active Directory program.

Table 2-35 *show ldap Field Descriptions (continued)*

Field	Description
Static Groups	Status of whether the static group query for user membership has been enabled. A static group defines each member individually using the object class attribute of <i>groupOfNames</i> or <i>groupOfUniqueNames</i> .
Group Attribute	Group attribute that the LDAP server uses to search the direct or nested static group configurations.
Group Member	Group member attribute that the LDAP server uses to search the direct or nested static group configurations.
Nested Groups	Any static groups that are nested under the parent group, which the LDAP server searches for user account information.
Nested Level	Number of levels down the LDAP directory from the starting point of the search that the LDAP server searches.
Administrative DN	Administrator distinguished name for the LDAP database search. There is no default value for this field and none is specified if it is not configured.
Administrative Password	Password of administrator for the LDAP database search. There is no default value for this field and none is specified if it is not configured.
LDAP version	LDAP software release version.
LDAP port	TCP port for the LDAP authentication server.
Policy redirect feature	Status of whether the support for acceptable use policy redirection has been configured.
Policy redirect append request URL	Status of whether the SE is enabled to append the request URL (original destination URL) to the LDAP (Acceptable Use Policy) AUP redirect URL.
Policy redirection URL	URL to redirect to if the user still has accepted the usage policy.
Policy redirection LDAP attribute name	Name of the LDAP attribute that is to be queried for the version that the user has accepted.
Policy redirection LDAP attribute value	Value of the LDAP attribute that is to be queried for the version that the user has accepted.
Password Expiry feature	Status of whether support for expiry of authorization passwords has been configured.
Password Expiry redirection URL	URL to redirect to if the user password has expired.
Server	LDAP server IP address.
Status	Status of whether the server is the primary or secondary host.
Primary	Primary host.
Secondary	Secondary host.

show logging

To display the system message log configuration, use the **show logging** EXEC command.

show logging

Syntax Description	This command has no arguments or keywords.

Defaults	No default behavior or values.

Command Modes	EXEC

Usage Guidelines	The following is an example of a syslog message for proxy-mode native FTP support:

```
SE-FTP_PROXY-3-252009:  Failed to configure FTP Proxy-mode listener on port
                        '[port]'.
```

Explanation: Could not start proxy-mode listener for FTP control connection for the specified port. The port is temporarily in an un-bindable state, or is in use by some other application.

Action: Check whether the port has been configured for use by a different application. If not, retry the incoming proxy command after 2 minutes. If this error repeats frequently, contact Cisco TAC.

To view information about events that have occurred in all devices in your CDS network, you can use the system message log in the CDSM GUI. The CDSM logs only severity level critical or higher messages from registered nodes. Also, the CDSM logs certain other status messages that are considered important to the Centralized Management System (CMS). The messages displayed in the system message log for device, SE, are not related to the messages logged in the system log file on the sysfs partition on the CDSM as /local1/syslog.txt.

The syslog.txt file on the CDSM contains information about events that have occurred on the CDSM and not on the registered nodes. The messages that are written to the syslog.txt file depend on specific parameters of the system log file that you have set by using the **logging** global configuration command. For example, a critical error message logged on a registered node does not appear in the syslog.txt file on the CDSM because the problem never occurred on the CDSM but only on the registered node. However, this error message is displayed in the system message log for device, SE

show logging

Examples

The following example displays the syslog host configuration on an SE:

```
ServiceEngine#show logging
Syslog to host is disabled
Priority for host logging is set to:  warning

Syslog to console is disabled
Priority for console logging is set to:  warning

Syslog to disk is enabled
Priority for disk logging is set to:  notice
Filename for disk logging is set to:  /local1/syslog.txt

Syslog facility is set to *
```

Syslog disk file recycle size is set to 500000

Related Commands

**clear
logging**

show movie-streamer

To display the Movie Streamer configuration, use the **show movie-streamer** EXEC command.

show movie-streamer [**bandwidth** | **cache** | **proxy**]

Syntax Description	bandwidth	(Optional) Displays Movie Streamer bandwidth configuration.
	cache	(Optional) Displays Movie Streamer cache configuration.
	proxy	(Optional) Displays Movie Streamer proxy configuration.

Defaults No default behavior or values.

Command Modes EXEC

Examples The following example shows the Movie Streamer configuration:

```
ServiceEngine#show movie-streamer
Movie Streamer version cde200-5.0.3
Movie Streamer is not enabled
----- Movie Streamer General Configurations -----
Movie Streamer max sessions configured: 8000
Movie Streamer transport source ip address is not configured
Movie Streamer accelerate for VOD is enabled
Movie Streamer client idle timeout is 300 seconds
Movie Streamer origin-server idle interval is 10 seconds
Movie Streamer client rtp timeout is 180 seconds
Movie Streamer outgoing bitrate per streamer has no limit
Movie Streamer incoming bitrate per streamer has no limit
----- Movie Streamer Bandwidth Configurations ----
Movie Streamer Outgoing bandwidth enforced is 2000000 kbps
Movie Streamer Incoming bandwidth enforced is 2000000 kbps
----- Movie Streamer Cache Configurations -----
Movie Streamer cache is enabled
Movie Streamer cache age-multiplier: 30%
Movie Streamer cache max-ttl: 1 (days)
Movie Streamer cache revalidate for each request is enabled
----- Movie Streamer Proxy Configurations -----
Movie Streamer proxy has not been configured.
----- Movie Streamer Broadcast List -----
```

Related Commands

- movie-streamer**
- show statistics movie-streamer**

show ntp

To display the Network Time Protocol (NTP) parameters, use the **show ntp** EXEC command.

show ntp status

Syntax Description	status Displays the NTP status.
Defaults	No default behavior or values.
Command Modes	EXEC
Examples	Table 2-36 describes the fields shown in the show ntp status display.

Table 2-36 *show ntp status Field Descriptions*

Field	Description
NTP	Status of whether NTP is enabled or disabled.
server list	NTP server IP and subnet addresses.
remote	Name (first 15 characters) of remote NTP server.
*	In the remote column, identifies the system peer to which the clock is synchronized.
+	In the remote column, identifies a valid or eligible peer for NTP synchronization.
space	In the remote column, indicates that the peer was rejected. (The peer could not be reached or excessive delay occurred in reaching the NTP server.)
x	In the remote column, indicates a false tick and is ignored by the NTP server.
-	In the remote column, indicates a reading outside the clock tolerance limits and is ignored by the NTP server.
refid	Clock reference ID to which the remote NTP server is synchronized.
st	Clock server stratum or layer.
t	Type of peer (local, unicast, multicast, or broadcast).
when	Status of when the last packet was received from the server in seconds.
poll	Time check or correlation polling interval in seconds.
reach	8-bit reachability register. If the server was reachable during the last polling interval, a 1 is recorded; otherwise, a 0 is recorded. Octal values 377 and above indicate that every polling attempt reached the server.
delay	Estimated delay (in milliseconds) between the requester and the server.
offset	Clock offset relative to the server.
jitter	Clock jitter.

Related Commands

clock
ntp

show processes

To display CPU or memory processes, use the **show processes** EXEC command.

show processes [**cpu** | **debug** *pid* | **memory** | **system** [**delay** 1-60 | **count** 1-100]]

Syntax Description

cpu	(Optional) Displays the CPU utilization.
debug	(Optional) Displays the system call and signal traces for a specified process identifier (PID) to display system progress.
<i>pid</i>	Process identifier.
memory	(Optional) Displays memory allocation processes.
system	(Optional) Displays system load information in terms of updates.
delay	(Optional) Specifies the delay between updates, in seconds (1–60).
1-60	Displays delays between updates, in seconds.
count	(Optional) Specifies the number of updates that are displayed (1–100).
1-100	Displays the number of updates displayed.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Use the commands shown in this section to track and analyze system CPU utilization.

The **show processes debug** command displays the extensive internal system call information and a detailed account of each system call (and arguments) made by each process and the signals that it has received.

Use the **show processes system** command to display system updates. The **delay** option specifies the delay between updates, in seconds. The **count** option specifies the number of updates that are displayed. This command displays these items:

- A list of all processes in wide format.
- Two tables listing the processes that utilize CPU resources. The first table displays the list of processes in descending order of utilization of CPU resources based on a snapshot taken after the processes system (ps) output is displayed. The second table displays the same processes based on a snapshot taken 5 seconds after the first snapshot.
- Virtual memory used by the corresponding processes in a series of five snapshots, each separated by 1 second.



Note

CPU utilization and system performance may be affected when you use the **show process** command. We recommend that you avoid using the **show process** command with keywords **system** and especially **debug**, unless it is absolutely necessary.

Examples

Table 2-37 describes the fields shown in the **show processes** displays.

Table 2-37 *show processes Field Descriptions*

Field	Description
CPU Usage	CPU utilization as a percentage for user, system overhead, and idle.
PID	Process identifier.
STATE	Current state of corresponding processes. R = Running S = Sleeping in an interruptible wait D = Sleeping in an uninterruptible wait or swapping Z = Zombie T = Traced or stopped on a signal
PRI	Priority of processes.
User T	User time utilization in seconds.
Sys T	System time utilization in seconds.
COMMAND	Process command.
Total	Total available memory in bytes.
Used	Memory currently used in bytes.
Free	Free memory available in bytes.
Shared	Shared memory currently used in bytes.
Buffers	Buffer memory currently used in bytes.
Cached	Cache memory currently used in bytes.
TTY	TTY to which the process is attached. For example, TTY may indicate which processes belong to network Telnet sessions.
%MEM	Percentage of memory used by corresponding processes.
VM Size	Virtual memory size (in bytes) allocated to the corresponding process.
RSS (pages)	Resident set size, which indicates the number of pages that the process has in real memory minus three (–3) for administrative purposes. These pages count toward text, data, and stack space but do not count demand-loaded or swapped-out pages.
Name	Filename of the executable in parentheses.

show programs

To display a list of programs on the SE, use the **show programs** EXEC command.

```
show programs [ movie-streamer [cli | live | rebroadcast] | program-id id | program-name
name]
```

Syntax Description

movie-streamer	(Optional) Displays the list of programs served by the Movie Streamer.
cli	(Optional) Displays the list of CLI programs served by the Movie Streamer.
live	(Optional) Displays the list of live programs served by the Movie Streamer.
rebroadcast	(Optional) Displays the list of rebroadcast programs served by the Movie Streamer.
program-id	(Optional) Displays detailed program information for the specified program ID.
<i>id</i>	Unique number identifying the program.
program-name	(Optional) Displays detailed program information for the specified program name.
<i>name</i>	Name of the program.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Typically, users create programs using the CDSM by defining programs in the manifest file or by using the Program API. The **show programs** command output displays the program type, the channel with which the program is associated, the current status of the program, and the next time that the program will start and end.

A program in the Internet Streamer CDS software is defined as a scheduled event in which the content is presented to the end user. Attributes of the program include the start and end time of the program, whether the content is pre-positioned or live, the set of SEs assigned to the program, and the streaming server to be used for content delivery.

Program types determine the hardware or software component involved in delivering content to the user. Different program types that are shown in the output of the **show programs** command are as follows:

- Movie streamer live
- Movie streamer rebroadcast

The CDSM GUI allows you to create a program, schedule it, and deliver it over your multicast-enabled CDS network. Programs can consist of prerecorded video or live events. In the case of live events, the Internet Streamer CDS software interoperates with third-party encoders and IP/TV Broadcast Servers to transmit the live stream across the CDS network.

When creating a program in the CDSM GUI, the administrator specifies the following information:

- Streaming server—How the program will be streamed or delivered to the end user.
 - Movie streamer—The event is played from a PC using the Apple QuickTime application or using the IP/TV Viewer application.
 - Exported—The program is exported over HTTP to a set-top box.
- Media source
 - Live stream transmitted from a third-party encoder or an IP/TV Broadcast Server
 - Pre-positioned content stored on SEs
- Destination
 - A set of SEs or device groups
 - A channel (live or export)
- Delivery method
 - Unicast or multicast live events
 - Multicast scheduled rebroadcasts
 - TV-out or export playlists
- Schedule
 - Start time and duration
 - Looping forever (enabled or disabled)
 - Multiple playback times
 - Repeating playback times
- Publishing URL—The URL used to view the program

Live Events

Live events are streamed from third-party encoders (such as the Windows Media encoder Version 9 and the QuickTime encoder) or from streaming servers (such as Windows Media Server). The live stream is acquired by the root SE and transmitted to edge SEs using unicast. From the edge SEs, the live stream is transmitted to end users using either multicast or multicast and unicast live splitting. The live program is available to viewers only during its scheduled times.

Before setting up a live event in the CDSM GUI, the administrator must complete the following tasks:

1. Set up the live event on the encoder or streaming server. This task is done externally to the CDSM GUI.
2. In the CDSM GUI, accept the streaming server's license agreement on the SEs designated to acquire and distribute the stream.
3. Create a live channel (or designate an existing channel as a live channel), assign SEs to the live channel, and designate a root SE to acquire the stream.

After you have completed the preceding tasks, you are ready to define the program and configure the program settings in the CDSM GUI. The CDSM allows you to define two types of live events based on the streaming server being used:

- WMT live
- Cisco Streaming Engine live

Configuration Requirements for Managed Live Events

If you have channels for live programs configured in your Internet Streamer CDS Release 2.4 network, make sure that there are no external proxy servers physically located between your Internet Streamer SEs and your root SE that require proxy authentication. Also, make sure that proxy authentication is not enabled on any receiver SEs that might be in the logical, hierarchical path between the root SE and the receiver SE that is going to serve the live stream to the requesting clients. If a live stream encounters any device that requires proxy authentication, the stream will be dropped before it reaches its destination.

If your network is set up with intermediary devices that require proxy authentication, you can work around the problem by configuring rules to bypass authentication on these devices.

For example, to enable the formation of the unicast splitting tree and, in turn, enable live broadcasting from all receiver SEs, you can specify the following rule on all of the parent SEs in the channel:

```
ServiceEngine(config)# rule pattern-list 1 downstream-SE-ipaddress
ServiceEngine(config)# rule no-auth pattern-list 1
```

Live Stream Interruptions

During a WMT live broadcast, any interruption of the live stream that lasts 5 minutes or longer causes the multicast broadcast to stop for the duration of the currently scheduled period. If the live stream is interrupted for less than five minutes, the broadcast resumes.

Live stream interruptions can be caused by unexpected encoder failures or by an operational restart. If you have early trials scheduled prior to the live event, we recommend that you configure multiple schedules, one for each trial. We also recommend that you start the encoder prior to the scheduled time.

If the live stream stops for more than 5 minutes and resumes later while the program is still scheduled, you can modify the schedule or any other attribute of the program (such as the description) to trigger a restart of the multicast broadcast. Restarting might take up to 5 minutes under these circumstances. This setting does not apply to Movie Streamer live programs.

Scheduled Rebroadcasts

In a scheduled rebroadcast, the pre-positioned content is scheduled to be streamed from edge SEs using multicast. To define a program for a rebroadcast event, the administrator must complete the following tasks:

1. Create a content acquisition channel and pre-position the content.
2. Assign media files to the program.
3. Specify the multicast address and port or define a program address pool.
4. Specify the days and times for the rebroadcast.



Note

For rebroadcast programs, the media can only be selected from one channel. The SEs and device groups assigned to the channel are selected automatically when you choose the media files for the program.

The CDSM allows you to define a program as a Movie Streamer rebroadcast.

Fast Encoder Failover

In Internet Streamer CDS, release 2.4, the **show programs** command was enhanced to support encoder failover. Issues with the previous release were as follows:

- In the forwarder list item, only the primary origin server's IP address showed. If the device failed over to the backup origin server, the forwarder list presented the primary origin server's IP address and did not reflect the real origin server that was connected by the root SE.

- In the source item, it presented every track's server IP address and port in the source, and there were no other explanations and tips. If the source included two tracks in the same server, the output was confusing.
- In the non-root SE, users could not obtain the information about the serving origin server.

With this release, the output of the command looks like the following:

```
ServiceEngine#show programs program-name live2
Current Time      : May 18 2009 @ 10:10:33 IST      (1242621633)
Program ID       : 1341
Program Name     : live2
Delivery Service ID : 1340
Delivery Service Name : live2
Type            : WMT Managed Scheduled Live

Forwarder List   : 3.1.2.11 <- 172.22.28.104

Schedules       :
Schedule #1:
  Start Time (loc) : May 18 2009 @ 10:11:00 IST (1242621660)
  End Time (loc)   : May 18 2009 @ 10:12:00 IST (1242621720)
  Duration         : 60 secs
  Repeat           : N/A
  Repeatdays      : N/A
  Time spec        : local

Source           :
  Server          : http://172.22.28.104:1881

Destination      :
  Unicast Access URL: rtsp://kinswmt.spcdn.net/live2
  Multicast URL     : http://kinswmt.spcdn.net/live2.nsc.asx
  Multicast Address : 224.2.2.58:94

Start Time (loc) : May 18 2009 @ 10:11:00 IST (1242621660)
Start Time       : May 18 2009 @ 04:41:00 GMT (1242601860)
End Time (loc)   : May 18 2009 @ 10:12:00 IST (1242621720)
End Time        : May 18 2009 @ 04:42:00 GMT (1242601920)

Current Status   : Scheduled
Time left        : N/A

ServiceEngine#show clock
Local time: Mon May 18 10:10:47 IST 2009
RT-612-2#sh programs program-name live2
Current Time     : May 18 2009 @ 10:11:05 IST      (1242621665)
Program ID       : 1341
Program Name     : live2
Delivery Service ID : 1340
Delivery Service Name : live2
Type            : WMT Managed Scheduled Live

Forwarder List   : 3.1.2.11 <- 172.22.28.104

Schedules       :
Schedule #1:
  Start Time (loc) : May 18 2009 @ 10:11:00 IST (1242621660)
  End Time (loc)   : May 18 2009 @ 10:12:00 IST (1242621720)
  Duration         : 60 secs
  Repeat           : N/A
  Repeatdays      : N/A
  Time spec        : local
```

■ show programs

```

Source          :
  Server        : http://172.22.28.104:1881

Destination     :
  Unicast Access URL: rtsp://kinswmt.spcdn.net/live2
  Multicast URL    : http://kinswmt.spcdn.net/live2.nsc.asx
  Multicast Address : 224.2.2.58:94

Start Time (loc) : May 18 2009 @ 10:11:00 IST      (1242621660)
Start Time       : May 18 2009 @ 04:41:00 GMT      (1242601860)
End Time (loc)   : May 18 2009 @ 10:12:00 IST      (1242621720)
End Time        : May 18 2009 @ 04:42:00 GMT      (1242601920)

Current Status   : Playing
Time left        : 55 secs

ServiceEngine#show clock
Local time: Mon May 18 10:11:10 IST 2009
RT-612-2#sh programs program-name live2
Current Time     : May 18 2009 @ 10:12:10 IST      (1242621730)
Program ID       : 1341
Program Name     : live2
Delivery Service ID : 1340
Delivery Service Name : live2
Type            : WMT Managed Scheduled Live

Forwarder List   : 3.1.2.11 <- 172.22.28.104

Schedules        :
Schedule #1:
  Start Time (loc) : May 18 2009 @ 10:11:00 IST      (1242621660)
  End Time (loc)   : May 18 2009 @ 10:12:00 IST      (1242621720)
  Duration         : 60 secs
  Repeat           : N/A
  Repeatdays      : N/A
  Time spec        : local

Source          :
  Server        : http://172.22.28.104:1881

Destination     :
  Unicast Access URL: rtsp://kinswmt.spcdn.net/live2
  Multicast URL    : http://kinswmt.spcdn.net/live2.nsc.asx
  Multicast Address : 224.2.2.58:94

Start Time (loc) : End of Program Reached
Start Time       : End of Program Reached
End Time (loc)   : End of Program Reached
End Time        : End of Program Reached

Current Status   : Stopped
Time left        : N/A

ServiceEngine#show clock
Local time: Mon May 18 10:12:14 IST 2009

```

Now the **show programs** command output contains the forwarder list with the backup source, and the root SE and non-root SE output is consistent. Also, if the user executes the **show statistics wmt streamstat** command from the root SE, the output shows which server is currently serving.

The source URL displays in the source section and the CLI and CDSM are consistent. Because the non-content acquirer cannot get the information on which source is serving, the output contains tips, such as “Please check which source is serving in content acquirer.”

The CDSM parses the backup SDP file and puts the results into the database. The item video_file_back_up saves the backup source server’s IP address and port in the play_media table.

Examples

Table 2-38 describes the fields shown in the **show programs program-name** and **program-id** display.

Table 2-38 *show programs* Field Descriptions

Field	Description
Current Time	Date and time of the output.
Program ID	Unique number identifying the program.
Program Name	Name of the program.
Delivery Service ID	Unique number identifying the delivery service.
Delivery Service Name	Unique name identifying the delivery service.
Type	Program type. Program types are as follows: • Movie streamer live • Movie streamer rebroadcast • Windows Media live • Windows Media rebroadcast
Forwarder List	List with primary and backup origin server’s IP address.
Schedules	Schedule list. Information is as follows: • Start Time (loc) • End Time (loc) • Duration • Repeat • Repeatdays • Time spec
Source (for Content Acquirer)	Primary and backup source URLs.
Source (for Non-content Acquirer)	Primary and backup source URLs and tips.
Destination	Unicast URLs.

show qos

To display Quality of Service (QoS) information, use the **show qos** EXEC command.

show qos

Syntax Description	This command has no arguments or keywords.

Defaults	No default behavior or values.

Command Modes	EXEC

Examples	This example shows the output that might be displayed if you do not enter any keywords:

```
ServiceRouter# show qos
Camiant policy service config file is not configured
Camiant policy service is running
```

Related Commands	qos show statistics qos

show radius-server

To display RADIUS information, use the **show radius-server** EXEC command.

show radius-server

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes EXEC

Examples [Table 2-39](#) describes the fields shown in the **show radius-server** display.

Table 2-39 *show radius-server Field Descriptions*

Field	Description
Login Authentication for Console/Telnet Session	Status of whether RADIUS server is enabled for login authentication.
Configuration Authentication for Console/Telnet Session	Status of whether RADIUS server is enabled for authorization or configuration authentication.
Authentication scheme fail-over reason	Status of whether SEs fail over to the secondary method of administrative login authentication whenever the primary administrative login authentication method fails.
RADIUS Configuration	RADIUS authentication settings.
RADIUS Authentication	Status of whether RADIUS authentication is enabled on the SE.
Key	Key used to encrypt and authenticate all communication between the RADIUS client (the SE) and the RADIUS server.
Timeout	Number of seconds that the SE waits for a response from the specified RADIUS authentication server before declaring a timeout.
Retransmit	Number of times that the SE is to retransmit its connection to the RADIUS if the RADIUS timeout interval is exceeded.
Radius Redirect	Status of whether the RADIUS server redirects the response if an authentication request fails.
Reply-Message	Message sent to the user if redirection occurs.
URL(s) to authentication failure instructions expired	HTML page location or URL where the redirect message should be sent.
Servers	RADIUS servers that the SE is to use for RADIUS authentication.

Table 2-39 *show radius-server* Field Descriptions (continued)

Field	Description
IP	Hostname or IP address of the RADIUS server.
Port	Port number on which the RADIUS server is listening.

Related Commands radius-server

show rea

To display the remote execution agent (REA) information use the **show rea** EXEC command.

show rea info

Syntax Description	info (Optional)Displays the agent information.
Defaults	No default behavior or values.
Command Modes	EXEC
Examples	The following example displays the REA information: <pre>ServiceEngine#show rea info rea agent is running</pre>
Related Commands	rea

show rcp

To display Remote Copy Program (RCP) information, use the **show rcp** EXEC command.

show rcp

Syntax Description	This command has no keywords or arguments.

Defaults	No default behavior or values.

Command Modes	EXEC

Examples	This example shows how to display RCP information:

```
ServiceEngine#show rcp
rcp service configurations:
rcp                enable
```

Related Commands	rcp

show rtsp

To display the Real-Time Streaming Protocol (RTSP) configurations, use the **show rtsp** EXEC command.

show rtsp [gateway]

Syntax Description

gateway	(Optional) Displays the RTSP gateway configuration.

Defaults

No default behavior or values.

Command Modes

EXEC

Examples

The following example display the output of the **show rtsp gateway** EXEC command.

```
ServiceEngine#show rtsp gateway
RTSP Gateway ip-address 10.107.193.30
RTSP Gateway incoming port 67
RTSP Gateway L4-switch not enabled
RTSP Gateway Transparent Interception:
    Not configured.
```

Related Commands

rtsp

show rule

To display rules configuration information, use the **show rule** EXEC command.

```

show rule action all [protocol {http | rtmp | rtsp}]

show rule action allow [protocol {http | rtmp | rtsp}]

show rule action block [protocol {http | rtmp | rtsp}]

show rule action generate-url-signature [protocol {http | rtmp | rtsp}]

show rule action no-cache [protocol {http | rtmp | rtsp}]

show rule action [protocol {http | rtmp | rtsp}]

show rule action redirect [protocol {http | rtmp | rtsp}]

show rule action refresh [protocol {http | rtmp | rtsp}]

show rule action rewrite [protocol {http | rtmp | rtsp}]

show rule action use-icap-service [protocol {http | rtmp | rtsp}]

show rule action validate-url-signature [protocol {http | rtmp | rtsp}]

show rule all

show rule pattern-list {1-512 pattern-type | all}

```

Syntax Description

all	Displays rules with all action types.
http	Displays HTTP-related requests for this action.
rtmp	Displays RTMP-related requests for this action.
rtsp	Displays RTSP-related requests for this action.
protocol	(Optional) Specifies the protocol to which actions apply.
allow	Allows the request.
block	Blocks the request.
generate-url-signature	Generates a signed URL.
no-cache	Does not cache the object.
redirect	Redirects the request to the rewritten URL.
refresh	Revalidates the object with the web server.
rewrite	Rewrites the URL and fetch.
use-icap-service	Sets ICAP service.
validate-url-signature	Validates a signed URL.
all	Displays all the configured actions and pattern lists.
pattern-list	Displays the rules with the specified patterns.
<i>1-512</i>	Specifies the pattern number (1–512).

<i>pattern-type</i>	Pattern type (see Table 2-40).
all	Displays rules with all pattern lists.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines You can use the **show rule pattern-list *pattern-type*** command to display rules using a specific pattern type. For a more complete explanation of specific rules, see the “[rule](#)” section on [page 2-183](#). [Table 2-40](#) shows the permitted pattern types and describes each pattern type.

Table 2-40 Pattern Types

Pattern Type	Description
all	Displays configured patterns for all pattern types.
domain	Regular expression to match the domain name.
dst-ip	Destination IP address of the request.
header-field	Request header field pattern.
src-ip	Source IP address of the request.
url-regex	Regular expression to be matched against the URL.
url-regsub	Regular expression to match URL and replacement pattern.

Examples The following example displays all rules with the configured action types and pattern lists:

```
ServiceEngine#show rule all
Rules Template Configuration
-----
Rule Processing Enabled
rule block domain bar.com
rule block domain \.foo.com
rule rewrite url-regsub http://www.ietf.org/rfc/.* http://wwwin-eng.cisco.com/RFC/$1
rule no-cache dst-ip 172.31.120.0 255.255.192.0
rule no-cache url-regex \.*cgi-bin*
```

Related Commands **clear rule**

show running-config

To display the current running configuration information on the terminal, use the **show running-config** EXEC command.

show running-config

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines Use this command with the **show startup-config** command to compare the information in running memory to the startup configuration used during bootup.



Note

This command replaces the **write terminal** command.

Examples The following example displays the current running configuration information:

```
ServiceEngine#show running-config
V2-CDE200-3#show running-config
! CDS version 2.3.9
!
device mode service-engine
!
!
hostname V2-CDE200-3
!
!
primary-interface PortChannel 1
!
!
interface PortChannel 1
 ip address 3.1.14.72 255.255.255.0
 exit
interface PortChannel 2
 ip address 4.0.8.13 255.255.255.0
 exit
!
interface GigabitEthernet 1/0
 channel-group 2
 exit
interface GigabitEthernet 2/0
 channel-group 2
 exit
interface GigabitEthernet 3/0
 channel-group 1
 exit
```



```
interface GigabitEthernet 4/0
  channel-group 1
  exit
interface GigabitEthernet 5/0
  channel-group 1
  exit
interface GigabitEthernet 6/0
  channel-group 1
  exit
!
!
ip default-gateway 3.1.14.1
!
!
offline-operation enable
!
!
rule action block pattern-list 3
rule action redirect http://www.baidu.com pattern-list 2
rule pattern-list 1 url-regex http://chunliu.com/b.wmv
rule pattern-list 2 header-field request-line b.wmv
rule pattern-list 3 header-field request-line c.wmv
!
icap service camiant
  server icap://trythis/servername
  exit
!
!
transaction-logs enable
transaction-logs archive interval 120
!
username admin password 1 bVmDmMMmZAPjY
username admin privilege 15
!
!
authentication login local enable primary
authentication configuration local enable primary
!
access-lists 300 deny groupname Disney
access-lists 300 permit groupname any
access-lists enable
!
!
telnet enable
!
!
cdsm ip 4.0.8.10
cms enable
!
!
service-router service-monitor threshold wmt 50
service-router service-monitor number-of-samples wmt 5
service-router service-monitor sample-period wmt 15
qos device-policy-service enable
!
!
cache content max-cached-entries 1000
! End of CDS configuration
V2-CDE200-3#
```

■ show running-config

Related Commands

configure
copy

show service-router

To display the service router configuration, use the **show service-router** EXEC command.

On the SE or on the CDSM:

```
show service-router {keepalive-interval | service-monitor}
```

On the SR:

```
show service-router {access-policy | content-based-routing | dns-ttl | forwarding
[content-origin content-origin] | lastresort [domain name] | load {all | sename sename} |
location-based-routing | proximity-based-routing | routes [content-origin content-origin] |
service-monitor | services {all | sename sename} | summary [content-origin content-origin]}
```

Syntax Description	
access-policy	Configures the service-router access-policy.
content-based-routing	Displays the content-based routing configuration.
dns-ttl	Displays the time to live (TTL) of domain name server (DNS) record.
forwarding	Displays the content origin forwarding tables.
content-origin	(Optional) Displays information for one content origin.
<i>content-origin</i>	Content origin fully qualified domain name (FQDN).
lastresort	Displays the domain and alternate domain configured.
domain	(Optional) Displays information for one domain.
<i>name</i>	Domain name.
load	Displays the load and threshold reached status.
all	Displays for all SEs.
sename	Displays for one SE.
<i>sename</i>	SE name.
location-based-routing	Displays the location-based routing configurations.
proximity-based-routing	Displays the proximity-based routing configurations.
routes	Displays the content origin routing tables.
service-monitor	Displays the service monitor configuration.
services	Displays the services status.
summary	Displays the content origin routing table summary statistics.
keepalive-interval	Displays the keepalive interval.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines

This command allows users to check the service router-related configuration. Through this command, users can view the configured features of an SR, such as location-based routing and content-based routing.

Examples

The following example displays the service router information on the SE:

```
ServiceEngine#show service-router service-monitor
Monitor types configured:
-----
CPU, MEM, KMEM, WMT, FMS, WEB, MS, DISK, NIC

Threshold values configured:
-----
CPU          : 80%
MEM          : 80%
KMEM         : 50%
WMT          : 50%
FMS          : 90%
MS           : 90%
WEB          : 90%
NIC          : 90%
DISK         : 80%
DISKFAILCNT  : 7

Sample periods configured:
-----
CPU   : 1 (secs)
MEM   : 1 (secs)
KMEM  : 1 (secs)
WMT   : 15 (secs)
FMS   : 1 (secs)
NIC   : 3 (secs)
DISK  : 1 (secs)

Sample counts configured to use in calculating average:
-----
CPU   : 2
MEM   : 2
KMEM  : 2
WMT   : 5
FMS   : 2
NIC   : 2
DISK  : 2

Device Status
-----

CPU
Current load      : 0%
Average load      : 0%
Threshold         : Not reached

DISK
Current load      : 0%
Average load      : 0%
Threshold         : Not reached
Status            : Operational

MEM
Average Used Memory : 4%
Threshold           : Not reached
```

```

KMEM
Average Kernel Memory : 1%
Threshold              : Not reached

NIC
Average BW In         : 0%
Average BW Out        : 0%
Threshold             : Not reached

Average Device load   : 0%

Services Status
-----

Critical Service(s)   : Running

WEB
Enabled               : Yes
Threshold             : Not reached
Stopped              : No

WMT
Enabled               : Yes
Current Stream Count  : 0
Threshold             : Not reached
Stopped              : No

MS
Enabled               : No

FMS
Enabled               : No

```

The following example displays the service router information on the CDSM:

```

CDSM#show service-router service-monitor
Monitor types configured:
-----
CPU, MEM, KMEM, DISK

Threshold values configured:
-----
CPU      : 80%
MEM      : 80%
KMEM     : 50%
DISK     : 80%
DISKFAILCNT : 1

Sample periods configured:
-----
CPU  : 1 (secs)
MEM  : 1 (secs)
KMEM : 1 (secs)
DISK : 1 (secs)

Sample counts configured to use in calculating average:
-----
CPU  : 2
MEM  : 2
KMEM : 2
DISK : 2

```

show service-router

```
Device Status
-----

CPU
Current load      : 0%
Average load      : 0%
Threshold         : Not reached

DISK
Current load      : 0%
Average load      : 0%
Threshold         : Not reached
Status            : Operational

MEM
Average Used Memory : 13%
Threshold           : Not reached

KMEM
Average Kernel Memory : 1%
Threshold              : Not reached

Average Device load : 0%
```

Related Commands **service-router**

show services

To display services-related information, use the **show services** EXEC command.

show services {**ports** [*port-num*] | **summary**}

Syntax Description	ports	Displays services by port number.
	<i>port-num</i>	(Optional) Up to eight port numbers (1–65535).
	summary	Displays the services summary.

Defaults No default behavior or values.

Command Modes EXEC

Examples The following example displays the services information by the port number:

```
CDSM# show services ports
Service information by port
-----
 550   Started on Mon Oct 14 12:13:20 2002
       Runs 1 service
           Cisco_Streaming_Engine
 553   Started on Mon Oct 14 12:13:20 2002
       Runs 1 service
           RTSP_Gateway
 554   Started on Mon Oct 14 12:13:20 2002
       Runs 1 service
           RTSP_Gateway
.
.
.
15256  Started on Mon Oct 14 12:13:20 2002
       Runs 1 service
           CMS
27999  Started on Mon Oct 14 12:13:20 2002
       Runs 1 service
           Real_Server
28000  Started on Mon Oct 14 12:13:20 2002
       Runs 1 service
           Real_Proxy
```

The following example displays a services information summary, showing the service and the associated port numbers:

```
CDSM# show services summary

Service      Ports
-----
      CMS      15256  2000  2001  2002  2003  2004  2005
      GUI      8001
      Wmt      1755  1756  1757  1799
      icp      3128
      emdb      5432
```

show services

```

          CertMgr          6001
          MgmtAgent        5252
          Real_Proxy       1090  8082  9002   555 28000  7879  6060  7071  30
31
          Cdsm_UI_http     8443
          Real_Server       7070  8081  9091 27999  7878  7802  1554  3030  40
40 5050
          RTSP_Gateway     554   553
          RPC_APACHE_PORT  6550
temp_RPC_APACHE_PORT     8008
Cisco_Streaming_Engine   550 SNMP

```


show snmp

To check the status of Simple Network Management Protocol (SNMP) communications, use the **show snmp** EXEC command.

show snmp {alarm-history | engineID | group | stats | user}

Syntax Description

alarm-history	Displays SNMP alarm history information.
engineID	Displays the local SNMP engine identifier.
group	Displays SNMP groups.
stats	Displays SNMP statistics.
user	Displays SNMP users.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

This command provides information on various SNMP variables and statistics on SNMP operations.

Examples

[Table 2-41](#) describes the fields shown in the **snmp alarm-history** display.

Table 2-41 *show snmp alarm-history Field Descriptions*

Field	Description
Index	Serial number of the listed alarms.
Type	Status of whether the alarm has been Raised or Cleared.
Sev	Levels of alarm severity (Critical, Major, or Minor).
Alarm ID	Traps sent by a CDS device contain numeric alarm IDs.
ModuleID	Traps sent by a CDS device contain numeric module IDs. See Table 2-42 to map module names to module IDs.
Category	Traps sent by an CDS device contain numeric category IDs. See Table 2-43 to map category names to category IDs.
Descr	Description of the Internet Streamer CDS software alarm and the application that generated the alarm.

[Table 2-42](#) describes the mapping of module names to module ids.

Table 2-42 Mapping of Module Names to Module IDs

Module Name	Module ID
acquirer	4000
AD_DATABASE	8000
cms	3000
MULTICAST_DATA_SENDER	7000
NHM	1
NHM/NHM	2500
nodemgr	2000
standby	4000
sysmon	1000
UNICAST_DATA_RECEIVER	5000
UNICAST_DATA_SENDER	6000

Table 2-43 describes the mapping of category names to category ids.

Table 2-43 Mapping of Category Names to Category IDs

Category Name	Category ID
Communications	1
Service Quality	2
Processing Error	3
Equipment	4
Environment	5
Content	6

Table 2-44 describes the fields shown in the **show snmp stats** display.

Table 2-44 show snmp stats Field Descriptions

Field	Description
SNMP packets input	Total number of SNMP packets input.
Bad SNMP version errors	Number of packets with an invalid SNMP version.
Unknown community name	Number of SNMP packets with an unknown community name.
Illegal operation for community name supplied	Number of packets requesting an operation not allowed for that community.
Encoding errors	Number of SNMP packets that were improperly encoded.
Number of requested variables	Number of variables requested by SNMP managers.
Number of altered variables	Number of variables altered by SNMP managers.
Get-request PDUs	Number of GET requests received.

Table 2-44 *show snmp stats Field Descriptions (continued)*

Field	Description
Get-next PDUs	Number of GET-NEXT requests received.
Set-request PDUs	Number of SET requests received.
SNMP packets output	Total number of SNMP packets sent by the router.
Too big errors	Number of SNMP packets that were larger than the maximum packet size.
Maximum packet size	Maximum size of SNMP packets.
No such name errors	Number of SNMP requests that specified a MIB object that does not exist.
Bad values errors	Number of SNMP SET requests that specified an invalid value for a MIB object.
General errors	Number of SNMP SET requests that failed because of some other error. (It was not a No such name error, Bad values error, or any of the other specific errors.)
Response PDUs	Number of responses sent in reply to requests.
Trap PDUs	Number of SNMP traps sent.

Table 2-45 describes the fields shown in the **show snmp engineID** display.

Table 2-45 *show snmp engineID Field Descriptions*

Field	Description
Local SNMP Engine ID	String that identifies the copy of SNMP on the local device.

Table 2-46 describes the fields shown in the **show snmp group** display.

Table 2-46 *show snmp group Field Descriptions*

Field	Description
groupname	Name of the SNMP group, or collection of users who have a common access policy.
security_model	Security model used by the group (v1, v2c, or v3).
readview	String identifying the read view of the group.
writeview	String identifying the write view of the group.
notifyview	String identifying the notify view of the group.

Table 2-47 describes the fields shown in the **show snmp user** display.

Table 2-47 *show snmp user Field Descriptions*

Field	Description
User name	String identifying the name of the SNMP user.

Table 2-47 *show snmp user Field Descriptions*

Field	Description
Engine ID	String identifying the name of the copy of SNMP on the device.
Group Name	Name of the SNMP group, or collection of users who have a common access policy.

Related Commands

snmp-server community
snmp-server contact
snmp-server enable traps
snmp-server group
snmp-server host
snmp-server location
snmp-server notify inform
snmp-server user
snmp-server view

show ssh

To display Secure Shell (SSH) status and configuration information, use the **show ssh** EXEC command.

show ssh

Syntax Description	This command has no arguments or keywords.
Defaults	No default behavior or values.
Command Modes	EXEC
Usage Guidelines	To display SSH status, enter the show ssh EXEC command.
Related Commands	sshd

show standby

To display standby interface information, use the **show standby** EXEC command.

show standby

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines To display standby interface information, enter the **show standby** EXEC command.

Examples [Table 2-48](#) describes the fields shown in the **show standby** display.

Table 2-48 *show standby Field Descriptions*

Field	Description
Standby Group	Number that identifies the standby group.
Description	Description of the device, as configured by using the description option of the interface global configuration command.
IP address	IP address of the standby group.
netmask	Netmask of the standby group.
Member interfaces	Member interfaces of the standby group. Shows which physical interfaces are part of the standby group. Shows the interface definition, such as GigabitEthernet 1/0.
priority	Priority status of each interface.
Active interface	Interfaces that are currently active in the standby group.
Maximum errors allowed on the active interface	Maximum number of errors allowed on the active interface.

Related Commands

- show interface**
- show running-config**
- show startup-config**

show startup-config

To display the startup configuration, use the **show startup-config** EXEC command.

show startup-config

Syntax Description	This command has no keywords or arguments.
Defaults	No default behavior or values.
Command Modes	EXEC
Usage Guidelines	Use this command to display the configuration used during an initial bootup, stored in nonvolatile random-access memory (NVRAM).
Examples	The following example displays the startup configuration details on the SE: <pre>ServiceEngine#show startup-config ! CDS version 2.3.9 ! device mode service-engine ! ! hostname V2-CDE200-3 ! ! ! primary-interface PortChannel 1 ! ! interface PortChannel 1 ip address 3.1.14.72 255.255.255.0 exit interface PortChannel 2 ip address 4.0.8.13 255.255.255.0 exit ! interface GigabitEthernet 1/0 channel-group 2 exit interface GigabitEthernet 2/0 channel-group 2 exit interface GigabitEthernet 3/0 channel-group 1 exit interface GigabitEthernet 4/0 channel-group 1 exit interface GigabitEthernet 5/0 channel-group 1</pre>

■ show startup-config

```

exit
interface GigabitEthernet 6/0
  channel-group 1
exit
!
!
ip default-gateway 3.1.14.1
!
!
offline-operation enable
!
!
!
rule action block pattern-list 3
rule action redirect http://www.baidu.com pattern-list 2
rule pattern-list 1 url-regex http://chunliu.com/b.wmv
rule pattern-list 2 header-field request-line b.wmv
rule pattern-list 3 header-field request-line c.wmv
!
icap service camiant
  server icap://trythis/servername
exit
!
!
!
transaction-logs enable
transaction-logs archive interval 120
!
username admin password 1 bVmDmMMmZAPjY
username admin privilege 15
!
!
authentication login local enable primary
authentication configuration local enable primary
!
access-lists 300 deny groupname Disney
access-lists 300 permit groupname any
access-lists enable
!
!
telnet enable
!
!
!
cdsm ip 4.0.8.10
cms enable
!
!
!
service-router service-monitor threshold wmt 50
service-router service-monitor number-of-samples wmt 5
service-router service-monitor sample-period wmt 15
qos device-policy-service enable
!
!
cache content max-cached-entries 1000
! End of CDS configuration

```

Related Commands

configure
copy
show running-config

show statistics access-lists 300

To display SE access control list statistics, use the **show statistics access-lists 300** EXEC command.

show statistics access-lists 300

Syntax Description This command has no keywords or arguments.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines The access control list statistics display the number of access requests, denials, and permissions recorded. Use the **show statistics access-lists 300** command to display the number of group name accesses recorded.

Examples [Table 2-49](#) describes the fields shown in the **show statistics access-lists 300** display.

Table 2-49 *show statistics access-lists 300 Field Descriptions*

Field	Description
Access Control Lists Statistics	
Groupname and username-based List	Lists the group name-based access control lists.
Number of requests	Number of requests.
Number of deny responses	Number of deny responses.
Number of permit responses	Number of permit responses.

Related Commands clear

show statistics acquirer

To display SE acquirer channel statistics, use the **show statistics acquirer** EXEC command.

```
show statistics acquirer [contents {delivery-service-id delivery-service-id |  

delivery-service-name delivery-service-name} | delivery-service-id delivery-service-id |  

delivery-service-name delivery-service-name | errors {delivery-service-id  

delivery-service-id | delivery-service-name delivery-service-name} | job-list  

{delivery-service-id delivery-service-id | delivery-service-name delivery-service-name}]
```

Syntax Description

contents	(Optional) Displays the acquired contents of the specified channel.
delivery-service-id	Displays acquirer statistics for the specified delivery service id.
<i>delivery-service-id</i>	Delivery service ID.
delivery-service-name	Displays acquirer statistics for the specified delivery service name.
<i>delivery-service-name</i>	Delivery service name.
errors	(Optional) Displays the acquisition error logs for the specified channel.
job-list	(Optional) Displays the job list statistics for the specified channel.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

The **show statistics acquirer** command displays acquirer statistics for all channels for which the SE is the root SE. The output of the command displays any manifest file parsing or fetch errors if any errors occur. It displays the total number of acquired objects, number of failed objects, and total disk space used by the acquired objects. When a channel ID or name is specified, acquirer statistics are displayed for that channel specified by ID or name.

The **show statistics acquirer contents** command displays all the acquired content, its size, and its last-modified time, specified by channel ID or name.

The **show statistics acquirer errors** command displays acquisition errors, if any, for the channel specified by ID or name. Manifest file parsing and fetch errors, as well as single item or crawler job errors, are displayed.

The **show statistics acquirer job-list** command displays the details of all the single items and crawler jobs for the channel specified by ID or name.

Examples

Table 2-50 describes the fields shown in the **show statistics acquirer** display.

Table 2-50 *show statistics acquirer Field Descriptions*

Field	Description
Statistics For Channel ID: <i>channel-id</i>	
Delivery-service-id	Delivery service identification number.
Delivery-service-name	Name of the delivery service.
Manifest	
Fetch Errors	Number of manifest file fetch errors.
Parsing Errors	Number of manifest file parsing errors.
Acquisition	
Total Number of Acquired Objects	Total number of acquired objects.
Total Size of Acquired Objects (Bytes)	Total size of acquired objects (in bytes).
Total Number of Failed Objects	Total number of failed objects.

Related Commands

acquirer (EXEC)
clear statistics
show acquirer

show statistics authentication

To display SE authentication statistics, use the **show statistics authentication** EXEC command.

show statistics authentication

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Authentication statistics display the number of access requests, denials, and allowances recorded. Use the **show statistics authentication** command to display the number of authentication accesses recorded.

Examples

The fields shown in the **show statistics authentication** display include the following

- Number of access requests
- Number of access deny responses
- Number of access allow responses

Related Commands

authentication
clear statistics
show authentication
show statistics authentication

show statistics cdnfs

To display SE CDS network file system (cdnfs) statistics, use the **show statistics cdnfs** EXEC command.

show statistics cdnfs

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes EXEC

Examples [Table 2-51](#) describes the **show statistics cdnfs** command fields displayed in the command output.

Table 2-51 *show statistics cdnfs Fields*

Field	Description
Size of physical file system	Physical disk size of the CDS network file system.
Space assigned for cdnfs purposes	Amount of physical disk space on the CDS network file system that has been assigned to hold pre-positioned objects. The space can be less than the size of the file system.
Number of cdnfs entries	Number of cdnfs objects in the CDS network file system. Note One pre-positioned file internally uses two cdnfs entries. The count of cdnfs entries will be twice the number of actual files displayed to users.
Space reserved for cdnfs entries	Amount of disk space reserved for existing pre-positioned objects. This space is reserved for cdnfs objects before the file is created and written to the file system.
Available space for new entries	Amount of physical disk space available in the CDS network file system for new pre-positioned objects.
Physical file system in use	Amount of physical disk space currently in use by the CDS network file system.
Physical file system space free	Amount of unused physical disk space in the CDS network file system.
Physical file system percentage in use	Percentage of physical disk space in use relative to the total disk space available.

Related Commands

- cdnfs
- clear
- show cdnfs
- show disks

■ show statistics cdnfs

show statistics distribution

To display the statistics of the content distribution components, use the **show statistics distribution** EXEC command.

```
show statistics distribution [all | errors {delivery-service-id delivery-service-id |  
delivery-service-name delivery-service-name} | metadata-receiver | metadata-sender |  
unicast-data-receiver [delivery-service-id delivery-service-id | delivery-service-name  
delivery-service-name | hot-forwarders [forwarder_id | forwarder_name] | idle-forwarders  
max_idle_forwarders] | unicast-data-sender]
```

Syntax Description

all	Displays the content distribution statistics for all distribution components.
errors	Displays the distribution error records for the specified channel.
delivery-service-id	Displays statistics about the specified delivery service ID.
<i>delivery-service-id</i>	Delivery service number.
delivery-service-name	Displays statistics about the specified delivery service name.
<i>delivery-service-name</i>	Delivery service name.
metadata-receiver	Displays the content distribution statistics of the metadata receiver.
metadata-sender	Displays the content distribution statistics of the metadata sender.
unicast-data-receiver	Displays the content distribution statistics of the unicast data receiver.
delivery-service-id	(Optional) Displays statistics about the specified delivery service ID.
<i>delivery-service-id</i>	(Optional) Delivery service number.
delivery-service-name	(Optional) Displays statistics about the specified delivery service name.
<i>delivery-service-name</i>	(Optional) Delivery service name.
hot-forwarders	(Optional) Displays the content distribution statistics of hot forwarders.
<i>forwarder_id</i>	(Optional) Identifier for the hot forwarder SE.
<i>forwarder_name</i>	(Optional) Name of the hot forwarder SE.
idle-forwarders	(Optional) Displays the content distribution statistics of idle forwarders.
<i>max_idle_forwarders</i>	(Optional) Maximum number of idle forwarder SEs to be displayed.
unicast-data-sender	Displays the content distribution statistics of the unicast data sender.

Defaults

The **idle-forwarders** *max_idle_forwarders* default is 3.

Command Modes

EXEC

Usage Guidelines

Cisco Internet Streamer Release 2.4 software supports multicast file transfer features that enhance the reliability and performance of multicast file distribution. Previously, the file transfer session depended on a window of time to resend the missing packets. The sender had to transmit the packets within this window of time for each retransmission request (NACK) from receiver SEs. If a multicast receiver joined the session too late and missed blocks of data that were outside the transmission window, the sender would not resend the missing blocks. The receiver could not receive the entire file, and the

transmission failed. The receiver had to wait until a subsequent carousel pass to recover the missed files. The receiver could only receive the entire file or nothing. A slow receiver often failed to receive a large file if the receiving rate lagged behind the sending rate.

The multicast file transfer enhancements resolve these issues by eliminating the window of time for file transmissions. This feature is called checkpoint. Checkpoint allows the sender to divide the transferring file into blocks and to retransmit any and all blocks until the transfer session ends. At any time during the transfer session, a receiver can request retransmission of any block that it has missed. Also, receiver SEs can receive the blocks of a transfer in any order. Data transmission can occur over a longer period, and receivers can recover missed data blocks to successfully complete the transfer in most situations. File transfers are much more resistant to loss of data.

This feature also solves the problem of a multicast receiver joining a transfer session late. Even if a receiver goes offline and restarts during a transfer, it can recover missing data without requesting retransmission of the blocks that it has already received.

Examples

Table 2-52 describes the fields shown in the **show statistics distribution unicast-data-receiver** display.

Table 2-52 *show statistics distribution unicast-data-receiver Field Descriptions*

Field	Description
Channel ID	Numerical identifier for the channel.
Channel name	Name for the channel.
Current unicast forwarder ID	Numerical identifier for the current unicast forwarder.
Current unicast forwarder name	Name for the current unicast forwarder.
Use hot forwarder	Status of the forwarder SE. Values are Yes or No. Yes means that the forwarder is active, and the job for this channel can be started immediately. No means that the forwarder is currently inactive and may become active some time later depending on the failure reason. For example, any new forwarder must wait at least one minute before starting active jobs.
Current running job	Shows statistics for jobs that are currently running.
relative-cdn-url	Relative URL for the current job.
channel-id	Numerical identifier for the channel for this job.
fwdr ip address	IP address of the current unicast forwarder for this job.
bytes written/total	Total number of bytes written for this job.
last write time	Number of seconds since the last write time for this job.
Cumulative bps	Number of cumulative bits per second.
Last successful job was done at	Time of completion of the last successful job.
#Consecutive failures	Number of consecutive failures.
#Jobs in pending queue(P_Q)	Number of jobs pending.

Table 2-52 *show statistics distribution unicast-data-receiver Field Descriptions (continued)*

Field	Description
#Jobs in suspended queue(S_Q)	Number of jobs suspended.
#Jobs in waiting queue(W_Q)	Number of jobs waiting.
#Bytes of jobs in P_Q and W_Q	Total number of bytes for jobs that are pending and waiting.
#Bytes of jobs in S_Q	Number of bytes for jobs that are suspended.
#Bytes of running jobs	Number of bytes for jobs that are currently running.

Related Commands

clear
show distribution

show statistics flash-media-streaming

To display the statistics for Flash Media Streaming, use the **show statistics flash-media-streaming EXEC** command.

show statistics flash-media-streaming [**connections** | **dvrcast** | **errors** | **livestats** | **performance** | **requests**]

Syntax Description		
connections	(Optional)	Displays Flash Media Streaming connections statistics.
dvrcast	(Optional)	Displays Flash Media Streaming dvrcast application statistics.
		
	Note	The dvrcast option will be available until the 2.4.3 release.
errors	(Optional)	Displays Flash Media Streaming errors statistics.
livestats	(Optional)	Displays Flash Media Streaming live application statistics.
performance	(Optional)	Displays Flash Media Streaming performance statistics.
requests	(Optional)	Displays Flash Media Streaming requests statistics.

Defaults No default behavior or values.

Command Modes EXEC

Examples The following example displays the statistics for Flash Media Streaming:

```
ServiceEngine#show statistics flash-media-streaming
Flash Media Streaming Statistics
Statistics have not been cleared since last Flash Media Streaming starts

Connections
-----
Current          :                0
Current VOD      :                0
Current LIVE     :                0
Current DVRCast  :                0
Max Concurrent   :                0
Total            :                0
Total VOD Req    :                0
Total LIVE Req   :                0
Total DVRCast Req :                0
Total Other Proxy Req:            0

Live Streaming
-----
UpStream BW      :                0 Kbps
DownStream BW    :                0 Kbps
UpStream Bytes   :                0
DownStream Bytes :                0
Num of Instance Load :            0

DVRCast Streaming
```

```

-----
UpStream BW      :          0 Kbps
DownStream BW    :          0 Kbps
UpStream Bytes   :          0
DownStream Bytes :          0
Num of Instance Load :        0

Flash Video Cache Statistics
-----
Hits             :          0
Misses           :          0
Released         :          0
Bytes in cache   :          0
Bytes in use     :          0

Performance
-----
Server Up Time   :          0 S
Mem Usage        :          0 %
Max Mem Usage    :          0 %

Cache
-----
Cache Hit        :          0
Cache Miss       :          0
Proxy Case       :          0
Cache Hit Percentage :      0.00 %

Preposition
-----
Preposition Hit   :          0

Bytes Served
-----
Total Server Bytes :          0
Local Disk Reads   :          0
HTTP Based Reads   :          0
Bytes From Local Disk:          0
Bytes Through HTTP :          0

Rules
-----
Action Allow      :          0
Action Block      :          0
Validate url Sign :          0
Errors            :          0
Auth Server Allow :          0
Auth Server Deny  :          0

Error
-----
Invalid Error     :          0
Server Error      :          0
Media Not Found   :          0
Media Unauthorize :          0
Invalid Request   :          0

```

Related Commands

flash-media-streaming
show flash-media-streaming

show statistics http

To display SE HTTP statistics, use the **show statistics http** EXEC command.

show statistics http {ims | object | pcmm | performance | requests | rule}

Syntax Description

ims	Displays HTTP if-modified-since statistics.
object	Displays HTTP object statistics.
pcmm	Displays PacketCable Multimedia (PCMM) statistics.
performance	Displays HTTP performance statistics.
requests	Displays HTTP request statistics.
rule	Displays rule statistics.

Defaults

No default behavior or values.

Command Modes

EXEC

Examples

[Table 2-53](#) describes the fields shown in the **show statistics http ims** displays.

Table 2-53 *show statistics http ims Field Descriptions*

Field	Description
Total Issued	
Range Issued	
Responses	
Fresh	
Revalid	
Partial Fresh	

[Table 2-54](#) describes the fields shown in the **show statistics http object** displays.

Table 2-54 *show statistics http object Field Descriptions*

Field	Description
Revalidate Requests	
Stale Content	
No-Cache Requests	
Min TTL Expired	
Max TTL Expired	
Object Expired	

Table 2-54 *show statistics http object Field Descriptions (continued)*

Field	Description
Max Age Header	
Large File Size	
Content Not Modified	
No Content Length	
Range Request	
No Store	
Private	
Auth Required	
Non Cacheable	
Head Request	
Vary Header	
Miscellaneous	

Table 2-55 describes the fields shown in the **show statistics http pcmm** displays.

Table 2-55 *show statistics http pcmm Field Descriptions*

Field	Description
No: of Icap Request	
No: of Signature Generation	
No: of Signature Validation	

Table 2-56 describes the fields shown in the **show statistics http performance** displays.

Table 2-56 *show statistics http performance Field Descriptions*

Field	Description
Total Accesses	
Total kBytes	
Request Per Second	
kBytes Per Second	
kBytes Per Request	

Table 2-57 describes the fields shown in the **show statistics http requests** displays.

Table 2-57 *show statistics http requests Field Descriptions*

Field	Description
Cache Hit	Number of requests that resulted in a cache hit for all SEs in the CDS network.
Cache Miss	Number of requests that resulted in a cache miss (the web object was not available in the cache) for all SEs in the CDS network.
Range Requests	Number of requests in the range.
Partial Hit–Live fill	Number of requests that resulted in a partial hit-live fill.
Partial Hit–Refill	Number of requests that resulted in a partial hit-refill.
Partial Caching–Bypassed	Number of bypassed partial caching requests.
Preposition Hits	Number of preposition hit requests.
Reply Meta	Number of reply meta requests.
Alternate Media	Number of alternate media requests.
Num Lookups	Number of lookup requests.
Lookup Errors	Number of lookup request errors.
Streaming Redirected Requests	Number of client requests for the content redirected by the SR to the closest SE in the CDS network containing that content.
WMT Liveness Requests	Number of WMT liveness requests.
Hierarchical Cache Liveness Requests	Number of hierarchical cache liveness requests.
Client Errors	Number of client error requests or authentication failures handled by the SE.
Server Errors	Number of origin server errors or authentication failures handled by the SE.
HTTP 0.9 Requests	Number of requests made using the HTTP 0.9 version. HTTP/0.9 cannot manage caches because document transfers are not optimized. HTTP/0.9, which is the first version of HTTP, has only the GET method. Everything is performed with this method, including sending data to the server (the requested URI looks like the following: http://www.foo.bar/url?var1=foo; the string that follows the first question mark means that the variable called var1 is set to foo).

Table 2-57 *show statistics http requests Field Descriptions (continued)*

Field	Description
HTTP 1.0 Requests	Number of requests made using the HTTP 1.0 version. HTTP/1.0 provides a simple caching mechanism. An origin server may mark a response, using the Expires header, with a time until which the cache could return the response without violating semantic transparency. A cache may check the current validity of a response using a conditional request. It may include an If-Modified-Since header in a request for the resource, specifying the value in the cached response's Last-Modified header. The server may then either respond with a 304 (Not Modified) status code, implying that the cache entry is valid, or it may send a normal 200 (OK) response to replace the cache entry. HTTP/1.0 also included a mechanism, the Pragma: no-cache header, for the client to indicate that a request should not be satisfied from a cache.
HTTP 1.1 Requests	Number of requests made using the HTTP 1.1 version. HTTP/1.1 includes a number of new conditional request-headers, in addition to If-Modified-Since. The most basic is If-None-Match, which allows a client to present one or more entity tags from its cache entries for a resource. If none of these matches the resource's current entity tag value, the server returns a normal response; otherwise, it may return a 304 (Not Modified) response with an ETag header that indicates which cache entry is currently valid. This mechanism allows the server to cycle through a set of possible responses, while the If-Modified-Since mechanism only generates a cache hit if the most recent response is valid. HTTP/1.1 also adds new conditional headers called If-Unmodified-Since and If-Match, which create other forms of preconditions on requests.
Http Invalid Requests	Number of invalid HTTP requests.
Blocked	Number of blocked requests.
Allowed	Number of allowed requests.

Related Commands

clear
show ftp

show statistics icap

To display Internet Content Adaptation Protocol (ICAP)-related statistics for the SE, use the **show statistics icap** EXEC command.

show statistics icap

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes EXEC

Examples [Table 2-58](#) describes the fields shown in the **show statistics icap** display.

Table 2-58 *show statistics icap Field Descriptions*

Field	Description
ICAP-client statistics (http proxy)	Statistics of the client of the ICAP process running on the Service Engine. The client of the ICAP process refers to the caching application that contacts the ICAP process which in turn communicates with the ICAP server. The server of the ICAP process refers to the ICAP server.
Total requests for V1 via RPC	Total number of client requests processed at the vectoring point V1.
Time per ICAP request (last 1k reqs)	Time taken to process each ICAP request. This field displays the time taken per request for the last 1000 requests.
ICAP daemon connection error	Number of errors that occurred when the caching application on the Service Engine attempted to connect to the ICAP daemon on the Service Engine.
Bad packets from ICAP daemon	Number of responses received by the Service Engine from the ICAP daemon that were not correct.
Error parsing HTTP req hdr from ICAP	Number of HTTP response headers received from the ICAP daemon that were incorrect. The ICAP daemon is the outgoing proxy server of the Service Engine.
ICAP daemon internal error	Number of internal errors that occurred on an ICAP daemon.
Total requests via outgoing proxy	Total number of requests sent from the caching application to the ICAP process through the outgoing proxy configured on the Service Engine.
ICAP daemon overloaded	Number of times that the ICAP process running on the Service Engine was overloaded.
Other errors	Number of all other errors that occurred when an ICAP request is processed.

Table 2-58 *show statistics icap Field Descriptions (continued)*

Field	Description
ICAP Daemon statistics	Statistics recorded on the ICAP daemon running on the Service Engine.
Total requests served	Total number of requests that were served by the ICAP daemon running on the Service Engine.
Total bytes to ICAP-Client	Total number of bytes sent to the ICAP client running on the Service Engine.
Average latency in milliseconds	Average delay in serving ICAP requests to ICAP clients in milliseconds.
ICAP Service statistics	Statistics for each ICAP service configured on the Service Engine.
Service	Name of the configured ICAP service.
Service Errors	Number of error messages returned by the ICAP service in response to client requests. These errors are also entered in the transaction log to show the status of the action performed by the ICAP service.
Service Bypasses	Number of requests that bypassed this ICAP service. The value of this field is incremented when you have configured this service to be bypassed when an error occurs with this service.
Server	Hostname or IP address of the ICAP server. Displays the statistics associated with the ICAP server. More than one ICAP service may be associated with an ICAP service.
Total Reqmods (0), Total Respmods (0)	Total number of requests processed at the reqmod-precache , reqmod-postcache , or respmod-precache vector points.
Modifications (Reqmod - 0), (Respmod - 0)	Total number of requests for which the request header or request body was modified after processing at the reqmod-precache , reqmod-postcache , or respmod-precache vector points.
No Modifications (Reqmod - 0), (Respmod - 0)	Total number of requests for which the request header or request body was not modified after processing at the reqmod-precache , reqmod-postcache , or respmod-precache vector points.
Error Responses (Reqmod - 0), (Respmod - 0)	Total number of requests for which error responses were returned to the client after processing at the reqmod-precache , reqmod-postcache , or respmod-precache vector points.
Server Errors	Number of errors that occurred at the ICAP server.
Server Bypasses	Number of times the ICAP server was bypassed during request processing.

Table 2-58 *show statistics icap Field Descriptions (continued)*

Field	Description
Options Req Success	Number of keepalive requests made by the Service Engine to the ICAP server that succeeded. The ICAP OPTIONS method is used by the ICAP client to retrieve configuration information from the ICAP server. In this method, the ICAP client sends a request addressed to a specific ICAP resource and receives a response with options that are specific to the service named by the URL. All OPTIONS requests may also return options that are global to the server (apply to all services). The OPTIONS method consists of a request line, such as the following example: <pre>OPTIONS icap://icap.server.net/sample-service ICAP/1.0 User-Agent: ICAP-client-XYZ/1.001</pre> In the following example, an ICAP Client sends an OPTIONS Request to an ICAP Service named icap.server.net/sample-service to receive configuration information for the service provided. <pre>OPTIONS icap://icap.server.net/sample-service ICAP/1.0 Host: icap.server.net User-Agent: BazookaDotCom-ICAP-Client-Library/2.3</pre>
Options Req Failed	Number of keepalive requests made by the Service Engine to the ICAP server that failed.
Max Conn Available	Maximum number of connections that can be made to the ICAP server.
Used Connections	Number of connections currently established with the ICAP server.
Total Bytes sent	Total number of bytes sent to the ICAP server.
Total Bytes received	Total number of bytes received from the ICAP server.
Total BPS sent	Total number of bytes sent per second to the ICAP server.
Total BPS received	Total number of bytes received per second from the ICAP server.
Server State	Current state of the connections made to the ICAP server. This field displays Not Available, CONNECTED, or DISCONNECTED.

Related Commands icap

show statistics icmp

To display SE Internet Control Message Protocol (ICMP) statistics, use the **show statistics icmp** EXEC command.

show statistics icmp

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines ICMP messages are sent in several situations, such as when a datagram cannot reach its destination, when the gateway does not have the buffering capacity to forward a datagram, and when the gateway can direct the host to send traffic on a shorter route. The purpose of these control messages is to provide feedback about problems in the communication environment, not to make IP reliable. There is still no guarantee that a datagram will be delivered or a control message will be returned. Some datagrams may still be undelivered without any report of their loss.

The ICMP messages typically report errors in the processing of datagrams. To avoid the infinite regress of messages about messages, no ICMP messages are sent about ICMP messages. Also, ICMP messages are only sent about errors in handling fragment zero of fragmented datagrams.

ICMP messages are sent using the basic IP header. The first octet of the data portion of the datagram is on a ICMP type field; the value of this field determines the format of the remaining data.

Many of the type fields contain more specific information about the error condition identified by a code value. ICMP messages have two types of codes:

- Query
- Error

Queries contain no additional information because they ask for information and will show a value of 0 in the code field. ICMP uses the queries as shown in [Table 2-59](#).

Table 2-59 *Queries*

Query	Type Field Value
Echo Reply	0
Echo Request	8
Router Advertisement	9
Router Solicitation	10
Time-stamp Request	13
Time-stamp Reply	14
Information Request (obsolete)	15

```
show statistics icmp
```

Table 2-59 *Queries (continued)*

Query	Type Field Value
Information Reply (obsolete)	16
Address Mask Request	17
Address Mask Reply	18

Error messages give specific information and have varying values that further describe conditions. Error messages always include a copy of the offending IP header and up to 8 bytes of the data that caused the host or gateway to send the error message. The source host uses this information to identify and fix the problem reported by the ICMP error message. ICMP uses the error messages as shown in [Table 2-60](#).

Table 2-60 *Errors*

Error	Type Field Value
Destination Unreachable	3
Source Quench	4
Redirect	5
Time Exceeded	11
Parameter Problems	12

Examples

[Table 2-61](#) describes the fields shown in the **show statistics icmp** display.

Table 2-61 *show statistics icmp Field Descriptions*

Field	Description
ICMP messages received	Total number of ICMP messages received by the SE.
ICMP messages receive failed	Total number of ICMP messages that were not received by the SE.
Destination unreachable	Number of destination-unreachable ICMP packets received by the SE. A destination-unreachable message (Type 1) is generated in response to a packet that cannot be delivered to its destination address for reasons other than congestion. The reason for the nondelivery of a packet is described by the code field value. Destination-unreachable packets use the code field values to further describe the function of the ICMP message being sent.

Table 2-61 *show statistics icmp Field Descriptions (continued)*

Field	Description
Timeout in transit	Number of ICMP time-exceeded packets received by the SE. The time-exceeded message occurs when a router receives a datagram with a TTL of 0 or 1. IP uses the TTL field to prevent infinite routing loops. A router cannot forward a datagram that has a TTL of 0 or 1. Instead, it trashes the datagram and sends a time-exceeded message. Two different time-exceeded error codes can occur, as follows: • 0 = Time-To-Live Equals 0 During Transit • 1 = Time-To-Live Equals 0 During Reassembly A router cannot forward a datagram with a TTL of 0 or 1 both during transit or reassembly. The TTL timer is measured in seconds and originally was used before the existence of routers to guarantee that a datagram did not live on the Internet forever. Each gateway processing a datagram reduces this value by at least one if it takes longer to process and forward the datagram. When this value expires, the gateway trashes the datagram and sends a message back to the sender notifying the host of the situation.
Wrong parameters	Number of ICMP packets with parameter problems received by the SE. An IP datagram that has been received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 12 denote a parameter problem on a datagram. ICMP parameter-problem datagrams are issued when a router has had to drop a malformed datagram. This condition is a normal and necessary type of network traffic; however, large numbers of this datagram type on the network can indicate network difficulties or hostile actions. A host or gateway can send this message when no other ICMP message covering the problem can be used to alert the sending host.
Source quenches	Number of ICMP source-quench packets received by the SE. A receiving host generates a source-quench message when it cannot process datagrams at the speed requested due to a lack of memory or internal resources. This message serves as a simple flow control mechanism that a receiving host can use to alert a sender to slow down its data transmission. When the source host receives this message, it must pass this information on to the upper-layer process, such as TCP, which then must control the flow of the application's data stream. A router generates this message when, in the process of forwarding datagrams, it has run low on buffers and cannot queue the datagram for delivery.

Table 2-61 *show statistics icmp Field Descriptions (continued)*

Field	Description
Redirects	Number of ICMP redirect packets received by the SE. A router sends a redirect error to the sender of an IP datagram when the sender should have sent the datagram to a different router or directly to an end host (if the end host is local). The message assists the sending host to direct a misdirected datagram to a gateway or host. This alert does not guarantee proper delivery; the sending host has to correct the problem if possible. Only gateways generate redirect messages to inform source hosts of misguided datagrams. A gateway receiving a misdirected frame does not trash the offending datagram if it can forward it.
Echo requests	Number of echo ICMP packets received by the SE. An echo request is an IP datagram that has been received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 8. The ICMP echo request is issued by the source to determine if the destination is alive. When the destination receives the request, it replies with an ICMP echo reply. This request and reply pair is most commonly implemented using the ping utility. Many network management tools use this utility or some derivative of it, and this condition is common as a part of network traffic. Note You should be suspicious when a large number of these packets are found on the network.
Echo replies	Number of echo-reply ICMP packets received by the SE. An echo reply is the message that is generated in response to an echo request message. An echo reply is an IP datagram that has been received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 0. This condition is common as a part of network traffic. Note You should be suspicious when a large number of these packets are found on the network.
Timestamp requests	Number of ICMP time-stamp request packets received by the SE. An ICMP time-stamp request is an IP datagram that has been received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 13. The ICMP time-stamp request and reply pair can be used to synchronize system clocks on the network. The requesting system issues the time-stamp request bound for a destination, and the destination system responds with a time-stamp reply message. This condition is normal as a part of network traffic but is uncommon on most networks. Note You should be suspicious when a large number of these packets are found on the network.

Table 2-61 *show statistics icmp Field Descriptions (continued)*

Field	Description
Timestamp replies	Number of ICMP time-stamp reply packets received by the SE. Time-stamp request and reply messages work in tandem. You have the option of using time stamps. When used, a time-stamp request permits a system to query another for the current time. It expects a recommended value returned to be the number of milliseconds since midnight, UTC. This message provides millisecond resolution. The two systems compare the three time stamps and use a round-trip time to adjust the sender's or receiver's time if necessary. Most systems set the transmit and receive time as the same value.
Address mask requests	Number of ICMP address mask request packets received by the SE. An ICMP address mask request is an IP datagram that has been received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 17. ICMP address mask requests could be used to perform reconnaissance sweeps of networks. The ICMP address mask request and reply pair can be used to determine the subnet mask used on the network. When the requesting system issues the address mask request bound for a destination, the destination system responds with an address mask reply message. This condition can be a part of normal network traffic but is uncommon on most networks. Note You should be suspicious when a large number of these packets are found on the network.
Address mask replies	Number of ICMP address mask reply packets received by the SE. An address mask ICMP reply is an IP datagram that has been received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 18. No known exploits incorporate this option. The ICMP address mask request and reply pair can be used to determine the subnet mask used on the network. When the requesting system issues the address mask request bound for a destination, the destination system responds with an address mask reply message. This condition can be a part of normal network traffic but is uncommon on most networks. Note You should be suspicious when a large number of these packets are found on the network.
ICMP messages sent	Total number of ICMP messages sent by the SE.
ICMP messages send failed	Total number of ICMP messages that failed to be sent by the SE.
Destination unreachable	Number of destination-unreachable ICMP packets sent by the SE.
Timeout in transit	Number of ICMP time-exceeded packets sent by the SE.
Wrong parameters	Number of ICMP packets with parameter problems sent by the SE.
Source quenches	Number of ICMP source-quench packets sent by the SE.
Redirects	Number of ICMP redirect packets sent by the SE.
Echo requests	Number of echo ICMP packets sent by the SE.

 show statistics icmp**Table 2-61** *show statistics icmp Field Descriptions (continued)*

Field	Description
Echo replies	Number of echo-reply ICMP packets sent by the SE.
Timestamp requests	Number of ICMP time-stamp request packets sent by the SE.
Timestamp replies	Number of ICMP time-stamp reply packets sent by the SE.
Address mask requests	Number of ICMP address mask requests sent by the SE.
Address mask replies	Number of ICMP address mask replies sent by the SE.

Related Commands

clear

show statistics ip

To display SE IP statistics, use the **show statistics ip** EXEC command.

show statistics ip

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes EXEC

Examples [Table 2-62](#) describes the fields shown in the **show statistics ip** display.

Table 2-62 *show statistics ip Field Descriptions*

Field	Description
Total packets in	Total number of input datagrams received from interfaces, including those received in error.
with invalid header	Number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, Time To Live exceeded, errors discovered in processing their IP options, and so on.
with invalid address	Number of input datagrams discarded because the IP address in the IP header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported classes (for example, Class E). For entities that are not IP routers and do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
forwarded	Number of input datagrams for which this entity was not the final IP destination, but the SE attempted to find a route to forward them to that final destination. In entities that do not act as IP routers, this counter will include only those packets that were source-routed through this entity, and the source-route option processing was successful.
unknown protocol	Number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
discarded	Number of input IP datagrams that were discarded even though the datagrams encountered no problems to prevent their continued processing. This counter does not include any datagrams discarded while awaiting reassembly.
delivered	Total number of input datagrams successfully delivered to IP user protocols (including ICMP).

Table 2-62 *show statistics ip Field Descriptions (continued)*

Field	Description
Total packets out	Total number of IP datagrams that local IP user protocols (including ICMP) supplied to IP in requests for transmission. This counter does not include any datagrams counted in the forwarded field.
dropped	Number of output IP datagrams that were discarded even though the datagrams encountered no problems that would prevent their transmission to their destination. This counter would include datagrams counted in the forwarded field if any such packets met this (discretionary) discard criterion.
dropped (no route)	Number of IP datagrams that were discarded because the SE found no route to transmit them to their destination. This counter includes any packets counted in the forwarded field that meet this no-route criterion including any datagrams that a host cannot route because all of its default routers are down.
Fragments dropped after timeout	Number of received fragments at this entity that are dropped after being held for the maximum number of seconds while awaiting reassembly at this entity.
Reassemblies required	Number of IP fragments received that needed to be reassembled at this entity.
Packets reassembled	Number of IP datagrams successfully reassembled.
Packets reassemble failed	Number of failures detected by the IP reassembly algorithm (because of reasons such as timed out and errors.) This counter is not necessarily a count of discarded IP fragments because some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.
Fragments received	Number of IP datagrams that have been successfully fragmented at this entity.
Fragments failed	Number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be fragmented for reasons such as the Don't Fragment flag was set.
Fragments created	Number of IP datagram fragments that have been generated as a result of fragmentation at this entity.

Related Commands

clear statistics ip
ip
show ip routes

show statistics movie-streamer

To display statistics for the Movie Streamer, use the **show statistics movie-streamer EXEC** command.

show statistics movie-streamer {all | bw-usage | error | performance | requests | rule}

Syntax Description	all	Displays all statistics.
	bw-usage	Displays bandwidth usage statistics.
	error	Displays error statistics.
	performance	Displays server performance.
	requests	Displays request statistics.
	rule	Displays rule statistics.

Defaults No default behavior or values.

Command Modes EXEC

Examples The following example shows all the Movie Streamer statistics:

```
ServiceEngine#show statistics movie-streamer all
```

```
Movie Streamer Request Statistics
Total
```

```
-----
```

```
Current RTSP Sessions: 3400
Total RTSP Sessions: 283299
Current RTP Connections: 2739
Total RTP Connections: 282885
```

```
CDN Related Statistics
```

```
-----
```

```
Preposition Hits: 0
Cache Hits: 0
Cache Miss: 0
Live Requests: 283299
```

```
Cache Revalidation Statistics
```

```
-----
```

```
Fresh Content Requests: 0
Revalidated Requests: 0
```

```
Movie Streamer Bandwidth Usage Statistics
```

```
Total
```

```
-----
```

```
Current Incoming Bandwidth: 0 bps
Current Outgoing Bandwidth: 3921755 bps
Current Total Bandwidth: 3921755 bps
```

```
Average Incoming Bandwidth: 475217 bps
Average Outgoing Bandwidth: 13038460 bps
Average Total Bandwidth: 13513677 bps
```

show statistics movie-streamer

```

By Type of Connection
-----
Unicast Incoming Bandwidth: 0 bps
Multicast Incoming Bandwidth: 0 bps
Unicast Outgoing Bandwidth: 3816953 bps
Multicast Outgoing Bandwidth: 0 bps

By Type of Content
-----
Live Incoming Bandwidth: 0 bps
VOD Incoming Bandwidth: 0 bps
Live Outgoing Bandwidth: 3816953 bps
VOD Outgoing Bandwidth: 0 bps

Overall Traffic
-----
Incoming Bytes: 709316834819 Bytes
Outgoing Bytes: 62627648126402 Bytes
Total Bytes: 63336964961221 Bytes

Incoming Packets: 652577871
Outgoing Packets: 191008363529
Total Packets: 191660941400

Movie Streamer Error Statistics
Total
Server Error
-----
Internal Error: 0
Not Implemented: 0
Server Unavailable: 0
Gateway Timeout: 0
Others: 0

Client Error
-----
Bad Request: 0
File Not Found: 6
Session Not Found: 0
Method Not Allowed: 0
Not Enough Bandwidth: 0
Client Forbidden: 0
Others: 0

Movie Streamer Performance Statistics
Total
-----
CPU Usage: 0.166702 %
Uptime: 254328 sec
Statistics was last cleared on Monday, 18-May-2009 20:04:42 UTC.

```

The following example shows the Movie Streamer rule statistics:

```

ServiceEngine#show statistics movie-streamer rule
RTSP Rule Template Statistics
=====
URL Rewrite: 0
URL Block: 0
Allow: 0
Redirect: 0

```

Related Commands

movie-streamer
show movie-streamer

show statistics netstat

To display SE Internet socket connection statistics, use the **show statistics netstat** EXEC command.

show statistics netstat

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes EXEC

Examples [Table 2-63](#) describes the fields shown in the **show statistics netstat** display.

Table 2-63 *show statistics netstat Field Descriptions*

Field	Description
Proto	Layer 4 protocol used on the Internet connection, such as TCP, UDP, and so forth.
Recv-Q	Amount of data buffered by the Layer 4 protocol stack in the receive direction on a connection.
Send-Q	Amount of data buffered by the Layer 4 protocol stack in the send direction on a connection.
Local Address	IP address and Layer 4 port used at the device end point of a connection.
Foreign Address	IP address and Layer 4 port used at the remote end point of a connection.
State	Layer 4 state of a connection. TCP states include the following: ESTABLISHED, TIME-WAIT, LAST-ACK, CLOSED, CLOSED-WAIT, SYN-SENT, SYN-RCVD, SYN-SENT, SYN-ACK-SENT, and LISTEN.

show statistics qos

To display statistics for the QoS policy service, use the **show statistics qos** EXEC command.

show statistics qos policy-service

Syntax Description	policy-service	Displays statistics of Camiant cdn-am policy service

Defaults	No default behavior or values.

Command Modes	EXEC

Examples The following example displays the statistics for the QoS policy service:

```
ServiceEngine#show statistics qos policy-service
Camiant CDN-AM Policy Service Statistics
-----

Application : WMT
  Protocol  : RTSP
    PLAY   : 0
    PAUSE  : 0
    STOP   : 0

  Protocol  : HTTP
    PLAY   : 0
    PAUSE  : 0
    STOP   : 0

Application : WEB-ENGINE
  Protocol  : HTTP
    PLAY   : 0
    PAUSE  : 0
    STOP   : 0

Errors : 0
```

Related Commands	qos show qos

show statistics radius

To display SE RADIUS authentication statistics, use the **show statistics radius** EXEC command.

show statistics radius

Syntax Description	This command has no arguments or keywords.

Defaults	No default behavior or values.

Command Modes	EXEC

Examples	The fields in the show statistics radius display are as follows: • Number of access requests • Number of access deny responses • Number of access allow responses • Number of authorization requests • Number of authorization failure responses • Number of authorization success responses

Related Commands	clear radius-server show radius-server

show statistics replication

To display delivery service replication status and related statistical data, use the following **show statistics replication** EXEC command.

On the CDSM:

```
show statistics replication {content-items {selected-delivery-service delivery-service-name} |  
  delivery-service [selected-delivery-service delivery-service-name] | item url | service engines  
  {selected-delivery-service delivery-service-name}}
```

On the SE:

```
show statistics replication {content-items content-name | selected-delivery-service  
  delivery-service-name}
```

Syntax Description		
content-items		Displays the replication status of the specified content items.
<i>content-name</i>		Content item name or pattern including an asterisk (*) and question mark (?). Use an asterisk to select all content items.
selected-delivery-service		Selects a delivery service.
<i>delivery-service-name</i>		Delivery service name.
delivery-service		Displays replication status of the delivery service.
item		Displays the detailed replication status of a content item across all SEs in a delivery service.
<i>url</i>		URL of the content item.
service-engines		Displays the replication status of the specified SEs.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines The **show statistics replication** command displays the delivery service replication status on the CDSM and the SE and shows the progressive file count status during acquisition and replication.

Examples [Table 2-64](#) describes the fields shown in the **show statistics replication** displays.

Table 2-64 show statistics replication Field Descriptions

Field	Description
Delivery service	Delivery service name.
State	Overall state of the delivery service. Values are Complete or Failed.
User Selected Root SE	Name of the root SE that has been selected for delivery service.

Table 2-64 *show statistics replication Field Descriptions (continued)*

Field	Description
Current Root SE	Name of the currently acting root SE for the delivery service.
Receiver SEs Completed	Total number of SEs that have completed content replication for the delivery service.
Receiver SEs In Progress	Total number of SEs for which content replication is in progress for the delivery service.
Receiver SEs Failed	Total number of SEs that have some error condition and are treated as failed.
Receiver SEs Not Responding	Total number of SEs not responding to the replication status queries from the CDSM.
Device	Name and ID of the device.
Website	Name of the website used for the delivery service.
Type	Role of the device, such as Root or Receiver.
State	State of the SE replication. For receiver SEs, states are Failed, Replicating, or Completed. For the root SE, states are Acquiring Content, Rechecking Content, or Completed.
Status	Replication status. Values are Red for failure and Green for success.
Completed	Number of content items completed.
To Do	Number of content items pending for the delivery service.
Failed	Number of failed content items.
Total	Total number of content items.
Last Report Time	Time that this status was obtained.
Disk Quota Used	Total disk quota used for the delivery service.
Manifest Last Modified	Time at which the manifest file was last modified.
Manifest Last Check	Time at which the manifest file was last checked for freshness.
Manifest State	State of the manifest. Values are Complete or Error with details of the error displayed.

show statistics service-router

To display service router statistics, use the **show statistics service-router** EXEC command.

```
show statistics service-router {all | content-origin name | dns | history | keepalive | se name |  
summary}
```

Syntax Description		
	all	Displays all statistics.
	content-origin	Displays content origin specific statistics.
	<i>name</i>	Content origin name to show.
	dns	Displays DNS statistics.
	history	Displays statistics history.
	keepalive	Displays keepalive statistics.
	se	Displays Service Engine specific statistics.
	<i>name</i>	Service Engine name to show.
	summary	Displays summary statistics.

Defaults	No default behavior or values.

Command Modes	EXEC

Related Commands	service-router show service-router

show statistics services

To display SE services statistics, use the **show statistics services** EXEC command.

show statistics services

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes EXEC

Examples [Table 2-65](#) describes the fields shown in the **show statistics services** display.

Table 2-65 *show statistics services Field Descriptions*

Field	Description
Port Statistics	Service-related statistics for each port on the Wide Area Application Services (WAAS) device.
Port	Port number.
Total Connections	Number of total connections.

Related Commands **show services**

show statistics snmp

To display SE Simple Network Management Protocol (SNMP) statistics, use the **show statistics snmp** EXEC command.

show statistics snmp

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes EXEC

Examples [Table 2-66](#) describes the fields shown in the **show statistics snmp** display.

Table 2-66 *show statistics snmp Field Descriptions*

Field	Description
SNMP packets input	Total number of SNMP packets input.
Bad SNMP version errors	Number of packets with an invalid SNMP version.
Unknown community name	Number of SNMP packets with an unknown community name.
Illegal operation for community name supplied	Number of packets requesting an operation not allowed for that community.
Encoding errors	Number of SNMP packets that were improperly encoded.
Number of requested variables	Number of variables requested by SNMP managers.
Number of altered variables	Number of variables altered by SNMP managers.
Get-request PDUs	Number of GET requests received.
Get-next PDUs	Number of GET-NEXT requests received.
Set-request PDUs	Number of SET requests received.
SNMP packets output	Total number of SNMP packets sent by the router.
Too big errors	Number of SNMP packets that were larger than the maximum packet size.
Maximum packet size	Maximum size of SNMP packets.
No such name errors	Number of SNMP requests that specified a MIB object that does not exist.
Bad values errors	Number of SNMP SET requests that specified an invalid value for a MIB object.

■ show statistics snmp

Table 2-66 *show statistics snmp Field Descriptions (continued)*

Field	Description
General errors	Number of SNMP SET requests that failed because of some other error. (It was not a No such name error, Bad values error, or any of the other specific errors.)
Response PDUs	Number of responses sent in reply to requests.
Trap PDUs	Number of SNMP traps sent.

Related Commands

show snmp
 snmp-server access-list
 snmp-server community
 snmp-server contact
 snmp-server enable
 snmp-server group
 snmp-server host
 snmp-server location
 snmp-server notify
 snmp-server user

show statistics tacacs

To display Service Engine TACACS+ authentication and authorization statistics, use the **show statistics tacacs** EXEC command.

show statistics tacacs

Syntax Description	This command has no arguments or keywords.

Defaults	No default behavior or values

Command Modes	EXEC

Examples	The fields shown in the show statistics tacacs display for the service engine are as follows:

- Number of access requests
- Number of access deny responses
- Number of access allow responses
- Number of authorization requests
- Number of authorization failure responses
- Number of authorization success responses
- Number of accounting requests
- Number of accounting failure responses
- Number of accounting success responses

Related Commands	clear show tacacs tacacs

show statistics tcp

To display SE Transmission Control Protocol (TCP) statistics, use the **show statistics tcp** EXEC command.

show statistics tcp

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes EXEC

Examples [Table 2-67](#) describes the fields shown in the **show statistics tcp** display.

Table 2-67 *show statistics tcp Field Descriptions*

Field	Description
Server connection openings	Number of connections opened from the SE to the server.
Client connection openings	Number of connections opened from the client to the SE.
Failed connection attempts	Number of incoming SYN connections rejected due to rate limiting or resource shortage.
Connections established	Number of incoming connections that have been set up.
Connections resets received	Number of resets (RSTs) received by the SE.
Connection resets sent	Number of resets (RSTs) sent by the SE.
Segments received	Number of TCP segments received from the client and the server. The value of this field is almost equal to the sum of the values of the Server segments received and the Client segments received fields.
Segments sent	Number of TCP segments sent by the client and the server. The value of this field is almost equal to the sum of the values of the Server segments sent and the Client segments sent fields.
Bad segments received	Number of incoming segments dropped due to checksum or being outside the TCP window.
Segments retransmitted	Number of TCP segments retransmitted by the client and the server. The value of this field is almost equal to the sum of the values of the Server segments retransmitted and the Client segments retransmitted fields.

Table 2-67 *show statistics tcp Field Descriptions (continued)*

Field	Description
Retransmit timer expirations	Number of times that the TCP retransmit timer expires. The TCP sender uses a timer to measure the time that has elapsed between sending a data segment and receiving the corresponding ACK from the receiving side of the TCP transmission. When this retransmit timer expires, the sender (according to the RFC standards for TCP congestion control) must reduce its sending rate.
Server segments received	Number of TCP segments received by the SE from the server.
Server segments sent	Number of TCP segments sent by the SE to the server.
Server segments retransmitted	Number of TCP segments retransmitted by the SE from the server.
Client segments received	Number of TCP segments received by the SE from the client.
Client segments sent	Number of TCP segments sent by the SE to the server.
Client segments retransmitted	Number of TCP segments retransmitted by the SE to the client.
Sync cookies sent	Number of synchronized (SYN) cookies sent by the SE. TCP requires unacknowledged data to be retransmitted. The server is supposed to retransmit the SYN.ACK packet before giving up and dropping the connection. When SYN.ACK arrives at the client but the ACK gets lost, there is a disparity about the establishment state between the client and server. Typically, this problem can be solved by the server's retransmission. But in the case of a SYN cookie, there is no state kept on the server and retransmission is impossible.
Sync cookies received	Number of synchronized (SYN) cookies received by the SE. The entire process of establishing the connection is performed by the ACK packet sent by the client, making the connection process independent of the preceding SYN and SYN.ACK packets. This type of connection establishment opens the possibility of ACK flooding, in the hope that the client will have the correct value to establish a connection. This method also allows you to bypass firewalls that normally only filter packets with SYN bit set.
Sync cookies failed	Number of synchronized (SYN) cookies rejected by the SE. The SYN cookies feature attempts to protect a socket from a SYN flood attack. This feature is a violation of TCP and conflicts with other areas of TCP such as TCP extensions. It can cause problems for clients and relays. We do not recommend that you use this feature as a tuning mechanism for heavily loaded servers to help with overloaded or misconfigured conditions.
Embryonic connection resets	Number of TCP connections that have been reset before the SE accepted the connection.
Prune message called	Number of calls that the SE makes to the function that tries to reduce the number of received but not acknowledged packets.

Table 2-67 *show statistics tcp Field Descriptions (continued)*

Field	Description
Packets pruned from receive queue	Number of packets that the TCP drops from the receive queue (usually due to low memory).
Out-of-order-queue pruned	Number of times that the packet was dropped from the out-of-order queue.
Out-of-window Icmp messages	Number of ICMP packets that were outside the TCP window and dropped.
Lock dropped Icmp messages	Number of ICMP packets that hit a locked (busy) socket and were dropped.
Arp filter	Number of Address Resolution Protocol (ARPs) not sent because they were meant for the SE.
Time-wait sockets	Number of current sockets in the TIME-WAIT state. The TIME-WAIT state removes old duplicates for fast or long connections. The clock-driven ISN selection is unable to prevent the overlap of the old and new sequence spaces. The TIME-WAIT delay allows enough time for all old duplicate segments to die in the Internet before the connection is reopened.
Time-wait sockets recycled	Number of TIME-WAIT sockets that were recycled (the address or port was reused before the waiting period was over). In TCP, the TIME-WAIT state is used as protection against old duplicate segments
Time-wait sockets killed	Number of TIME-WAIT sockets that were terminated to reclaim memory.
PAWS passive	Number of passive connections that were made with Protection Against Wrapped Sequence (PAWS) numbers enabled. PAWS operates within a single TCP connection using a state that is saved in the connection control block.
PAWS active	Number of active connections that were made with PAWS enabled. PAWS uses the same TCP time stamps as the round-trip time measurement mechanism and assumes that every received TCP segment (including the data and ACK segments) contains a time-stamp SEG.TSval that has values that are monotone and nondecreasing in time. A segment can be discarded as an old duplicate if it is received with a time-stamp SEG.TSval less than some time stamp recently received on this connection.
PAWS established	Number of current connections that were made with PAWS enabled.
Delayed acks sent	Number of delayed ACK counters sent by the SE.
Delayed acks blocked by socket lock	Number of delayed ACK counters that were blocked because the socket was in use.
Delayed acks lost	Number of delayed ACK counters lost during transmission.

Table 2-67 *show statistics tcp* Field Descriptions (continued)

Field	Description
Listen queue overflows	Number of times that the three-way TCP handshake was completed, but enough space was not available in the listen queue.
Connections dropped by listen queue	Number of TCP connections dropped due to a resource shortage.
TCP packets queued to prequeue	Number of TCP packets queued to the prequeue.
TCP packets directly copied from backlog	Number of TCP packets delivered to the client from the backlog queue. Packets are queued in the backlog when the TCP receive routine runs and notices that the socket was locked.
TCP packets directly copied from prequeue	Number of TCP packets delivered to the client from the prequeue.
TCP prequeue dropped packets	Number of TCP packets dropped from the prequeue. The prequeue is where the TCP receives routine runs. It notes that the current running process as the TCP target process and queues it directly for copy after the TCP software interrupt is completed.
TCP header predicted packets	Number of incoming packets that successfully matched the TCP header prediction.
Packets header predicted and queued to user	Number of TCP packets copied directly to the user space.
TCP pure ack packets	Number of acknowledgment (ACK) packets that contain no data.
TCP header predicted acks	Number of incoming ACKs that successfully matched the TCP header prediction.
TCP Reno recoveries	Number of times that the TCP fast recovery algorithm recovered a packet loss. TCP Reno induces packet losses to estimate the available bandwidth in the network. When there are no packet losses, TCP Reno continues to increase its window size by one during each round trip. When it experiences a packet loss, it reduces its window size to one half of the current window size. This feature is called additive increase and multiplicative decrease. TCP Reno, however, does not fairly allocate bandwidth because TCP is not a synchronized rate-based control scheme, which is necessary for the convergence.
TCP SACK recoveries	Number of times that the SE recovered from a selective acknowledgment (SACK) packet loss. If the data receiver has received a SACK-Permitted option on the SYN for this connection, the data receiver may choose to generate SACK options. If the data receiver generates SACK options under any circumstance, it should generate them under all permitted circumstances. If the data receiver has not received a SACK-Permitted option for a given connection, it must not send SACK options on that connection.

Table 2-67 *show statistics tcp Field Descriptions (continued)*

Field	Description
TCP SACK renegeing	Number of times that the SE refused to accept packets that have not been acknowledged to the data sender, even if the data has already been reported in a SACK option. Such discarding of SACK packets is discouraged but may be used if the receiver runs out of buffer space. The data receiver may choose not to keep data that it has reported in a SACK option. Because the data receiver may later discard data reported in a SACK option, the sender must not discard data before it is acknowledged by the Acknowledgment Number field in the TCP header.
TCP FACK reorders	Number of forward acknowledgment (FACK) packets that were out of sequence order. The FACK algorithm makes it possible to treat congestion control during recovery in the same manner as during other parts of the TCP state space. The FACK algorithm is based on first principles of congestion control and is designed to be used with the proposed TCP SACK option. By decoupling congestion control from other algorithms, such as data recovery, it attains more precise control over the data flow in the network. FACK takes advantage of the SACK option; it takes into account which segments have been SACKed. It also uses the receipt of a SACK that leaves at least 3*MSS bytes unacknowledged as a trigger for Fast Retransmit.
TCP SACK reorders	Number of selective acknowledgment (SACK) packets that were out of sequence order.
TCP Reno reorders	Number of TCP Renos that were out of sequence order.
TCP TimeStamp reorders	Number of segments received with out-of-order time stamps.
TCP full undos	Number of times that the congestion window (cwnd) was fully recovered.
TCP partial undos	Number of times that the congestion window (cwnd) was partially recovered.
TCP DSACK undos	Number of times that the duplicate selective acknowledgment (DSACK) packets were recovered.
TCP loss undos	Number of times that the congestion window (cwnd) recovered from a packet loss.
TCP losses	Number of times that data was lost and the size of the congestion window (cwnd) decreased.
TCP lost retransmit	Number of times that a retransmitted packet was lost.

Table 2-67 *show statistics tcp Field Descriptions (continued)*

Field	Description
TCP Reno failures	Number of times that the congestion window (cwnd) failed because the TCP fast recovery algorithm failed to recover from a packet loss. The congestion avoidance mechanism, which is adopted by TCP Reno, causes the window size to vary. This situation causes a change in the round-trip delay of the packets, larger delay jitter, and an inefficient use of the available bandwidth due to many retransmissions of the same packets after the packet drops occur. The rate at which each connection updates its window size depends on the round-trip delay of the connection. The connections with shorter delays can update their window sizes faster than other connections with longer delays.
TCP SACK failures	Number of times that the congestion window (cwnd) shrunk because the SE failed to recover from a selective acknowledgment (SACK) packet loss. The selective acknowledgment extension uses two TCP options. The first is an enabling option, SACK-permitted, which may be sent in a SYN segment to indicate that the SACK option can be used once the connection is established. The other is the SACK option, which may be sent over an established connection once permission has been given by the SACK-permitted option.
TCP loss failures	Number of times that the TCP timeout occurred and data recovery failed.
TCP fast retransmissions	Number of TCP fast retransmission counters. TCP may generate an immediate acknowledgment (a duplicate ACK) when an out-of-order segment is received. The duplicate ACK lets the other end know that a segment was received out of order and tells it what sequence number is expected. Because TCP does not know whether a duplicate ACK is caused by a lost segment or just a reordering of segments, it waits for a small number of duplicate ACKs to be received. If there is just a reordering of the segments, there will be only one or two duplicate ACKs before the reordered segment is processed, which will then generate a new ACK. If three or more duplicate ACKs are received in a row, it is a strong indication that a segment has been lost. TCP then retransmits what appears to be the missing segment without waiting for a retransmission timer to expire.

Table 2-67 *show statistics tcp Field Descriptions (continued)*

Field	Description
TCP forward retransmissions	Number of TCP forward retransmission counters. This field applies only to SACK-negotiated connections; this field is the counter for FACK segments. The value of this field is for segments that were retransmitted even though there is no indication that they were actually lost. Retransmission is stopped when either one of the following occurs: • The maximum time to wait for a remote response is reached. This timeout occurs when the total time of all retransmission intervals exceeds the maximum time to wait for a remote response. • The number of retransmissions configured in maximum retransmissions per packet is reached.
TCP slowstart retransmissions	Number of TCP slow-start retransmission counters. The slow-start algorithm begins by sending packets at a rate that is determined by the congestion window. The algorithm continues to increase the sending rate until it reaches the limit set by the slow-start threshold (ssthresh) variable. (Initially, the value of the ssthresh variable is adjusted to the receiver's maximum window size [RMSS]. However, when congestion occurs, the ssthresh variable is set to half the current value of the cwnd variable, marking the point of the onset of network congestion for future reference.)
TCP Timeouts	Number of times that a TCP timeout occurred.
TCP Reno recovery fail	Number of times that the TCP fast recovery algorithm failed to recover from a packet loss. In TCP Reno, the maximum number of recoverable packet losses in a congestion window without timeout is limited to one or two packets. No more than six losses can be recovered with a maximum window size of 128 packets. This failure of recovery is because TCP Reno cuts the congestion window by half for each recovered loss.
TCP Sack recovery fail	Number of times that the SE failed to recover from a SACK packet loss. When receiving an ACK containing a SACK option, the data sender should record the selective acknowledgment for future reference. The data sender is assumed to have a retransmission queue that contains the segments that have been transmitted but not yet acknowledged in sequence number order. If the data sender performs repacketization before retransmission, the block boundaries in a SACK option that it receives may not fall within the boundaries of segments in the retransmission queue.
TCP scheduler failed	Number of times that the TCP scheduler failed.
TCP receiver collapsed	Number of times that the data in an out-of-order queue collapsed.

Table 2-67 *show statistics tcp Field Descriptions (continued)*

Field	Description
TCP DSACK old packets sent	Number of duplicate selective acknowledgments (D-SACKs) sent by the SE. The use of D-SACK does not require a separate negotiation between a TCP sender and receiver that have already negotiated SACK. The absence of a separate negotiation for D-SACK means that the TCP receiver could send D-SACK blocks when the TCP sender does not understand this extension to SACK. In this case, the TCP sender discards any D-SACK blocks and processes the other SACK blocks in the SACK option field as it normally would.
TCP DSACK out-of-order packets sent	Number of out-of-order D-SACK packets sent by the SE. A D-SACK block is used only to report a duplicate contiguous sequence of data received by the receiver in the most recent packet. Each duplicate contiguous sequence of data received is reported in at most one D-SACK block. (The receiver sends two identical D-SACK blocks in subsequent packets only if the receiver receives two duplicate segments.) If the D-SACK block reports a duplicate contiguous sequence from a (possibly larger) block of data in the receiver's data queue above the cumulative acknowledgement, then the second SACK block in that SACK option should specify that (possibly larger) block of data.
TCP DSACK packets received	Number of D-SACK packets received by the SE. TCP senders receiving D-SACK blocks should be aware that a segment reported as a duplicate segment could possibly have been from a prior cycle through the sequence number space. This awareness of the TCP senders is independent of the use of PAWS by the TCP data receiver.
TCP DSACK out-of-order packets received	Number of out-of-order D-SACK packets received by the SE. Following a lost data packet, the receiver receives an out-of-order data segment, which triggers the SACK option as specified in RFC 2018. Because of several lost ACK packets, the sender then retransmits a data packet. The receiver receives the duplicate packet and reports it in the first D-SACK block.
TCP connections abort on sync	Number of times that a valid SYN segment was sent in the TCP window and the connection was reset.
TCP connections abort on data	Number of times that the connection closed after reading the data.
TCP connections abort on close	Number of times that the connection aborted with pending data.
TCP connections abort on memory	Number of times that memory was not available for graceful closing of the connection resulting in the connection being aborted immediately.
TCP connections abort on timeout	Number of times that the connection timed out.
TCP connections abort on linger	Number of times that the linger timeout expired resulting in the data being discarded and closing of the connection.

 show statistics tcp**Table 2-67** *show statistics tcp Field Descriptions (continued)*

Field	Description
TCP connections abort failed	Number of times that the TCP connection ran out of memory, transmits failed, or peer TCP Reset (RST) could not be sent.
TCP memory pressures	Number of times that the TCP subsystem encounters memory constraints.

Related Commands

clear
show tcp
tcp

show statistics transaction-logs

To display SE transaction log export statistics, use the **show statistics transaction-logs** EXEC command.

show statistics transaction-logs

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines To display the transaction log export statistics, you must first configure the FTP server.

Examples [Table 2-68](#) describes the fields shown in the **show statistics transaction-logs** display.

Table 2-68 *show statistics transaction-logs* Field Descriptions

Field	Description
Initial Attempts	Initial attempts made to contact the external server at the configured export intervals.
Initial Successes	Number of times that an initial attempt made to contact the external server succeeded.
Initial Open Failures	Number of times that the SE failed to open a connection to the FTP export server.
Initial Put Failures	Number of times that the SE failed to transfer a file to the FTP export server.
Retry Attempts	Number of retries made to contact the external server at the configured export intervals.
Retry Successes	Number of times that a retry made to contact the external server succeeded.
Retry Open Failures	Number of times that the SE failed to open a connection to the FTP export server on a retry.
Retry Put Failures	Number of times that the SE failed to transfer a file to the FTP export server on a retry.

 show statistics transaction-logs**Table 2-68** *show statistics transaction-logs Field Descriptions (continued)*

Field	Description
Authentication Failures	Number of times that the SE failed to authenticate with the FTP export server. This situation might occur if the SE is misconfigured with the wrong password for the FTP server or the password on the FTP server has been changed since the SE was configured.
Invalid Server Directory Failures	Number of times the SE failed to direct traffic to the correct server directory.

Related Commands

clear
show transaction-logging
transaction-log force

show statistics udp

To display SE User Datagram Protocol (UDP) statistics, use the **show statistics udp** EXEC command.

show statistics udp

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes EXEC

Examples [Table 2-69](#) describes the fields shown in the **show statistics udp** display.

Table 2-69 *show statistics udp Field Descriptions*

Field	Description
Packets received	Total number of UDP packets received.
Packets to unknown port received	Number of packets to unknown ports received.
Packet receive error	Number of packet receive errors.
Packet sent	Number of UDP packets sent.

show statistics wmt

To display the SE Windows Media Technologies (WMT) statistics, use the **show statistics wmt** EXEC command.

show statistics wmt { **all** | **bytes** [**incoming** | **outgoing**] | **cache** | **errors** | **multicast** | **requests** | **rule** | **savings** | **streamstat** [**incoming** | **live** | **outgoing** | **stream-id** 1-999999] | **usage** }

Syntax Description		
all		Displays all WMT statistics.
bytes		Displays unicast byte statistics.
incoming		(Optional) Displays unicast incoming byte statistics.
outgoing		(Optional) Displays unicast outgoing byte statistics.
cache		Displays cache validation statistics.
errors		Displays error statistics.
multicast		Displays multicast statistics.
requests		Displays unicast request statistics.
rule		Displays the Rule Template statistics.
savings		Displays savings statistics.
streamstat		Displays Windows Media streaming connections.
incoming		(Optional) Displays statistics of all incoming WMT streams from the SE.
live		(Optional) Displays aggregated live stream statistics.
outgoing		(Optional) Displays statistics of all outgoing WMT streams from the SE.
stream-id		(Optional) Displays statistics of the WMT streams that have the specified stream ID.
1-999999		WMT stream ID to display.
usage		Displays current usage statistics.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines The output of the **show statistics wmt** EXEC command includes information about WMT RTSP requests. For example, the output from the **show statistics wmt** EXEC command was changed as follows:

- RTSP-related information was added to the **show statistics wmt all** command output.
- Information about RTSP and RTSPU was added in the transport protocol portion of the **show statistics wmt bytes** command output.

- RTSPT and RTSPU errors were added to the **show statistics wmt errors** command output.
- The **show statistics wmt requests** command output includes the RTSPT and RTSPU protocols and Fast Start and Fast Cache data.

The **live** option was added to the **show statistics wmt streamstat EXEC** command to enable you to display aggregated live statistics. Also, the **incoming**, **outgoing**, and **stream-id** options were added to the **show statistics wmt streamstat EXEC** command to display statistics of all incoming WMT streams, outgoing WMT streams, and streams with the specified ID.

Configuring the HTTP Allow/Block Rule

For the MMS over HTTP request rule, even though the request is served by WMT, it doesn't increment the statistics. The user needs the statistics for all WMT requests. Now the user can execute the **show statistics http rule** command as the rules daemon check is done from the HTTP side, and the request is redirected to WMT.

Examples

[Table 2-70](#) describes the fields shown in the **show statistics wmt all** display.

Table 2-70 *show statistics wmt all Field Descriptions*

Field	Description
Unicast Requests Statistics	
Total unicast requests received	Total number of unicast requests received. Display shows the number of requests in each category and calculates the percentage of the total for each category.
Streaming Requests served	Number of streaming requests received.
Mcast nsc file Request	Number of multicast NSC file requests received.
Authenticate Requests	Number of authenticated requests received.
Requests error	Number of request errors received.
By Type of Content	
Live content	Number of live content requests received.
On-Demand Content	Number of on-demand content requests received.
By Transport Protocol	
HTTP	Number of HTTP requests received.
RTSPT	Number of RTSPT requests received.
RTSPU	Number of RTSPU requests received.
Unicast Savings Statistics	
Total bytes saved	Total number of bytes saved.
By Source of Content	
Local	Number of local bytes saved.
Remote HTTP	Number of remote HTTP bytes saved.

Table 2-70 *show statistics wmt all Field Descriptions (continued)*

Field	Description
Remote RTSP	Number of remote RTSP bytes saved.
Multicast	Number of multicast bytes saved.
CDN-Related WMT Requests	
CDN Content Hits	Number of CDN content request hits.
CDN Content Misses	Number of CDN content request misses.
CDN Content Live	Number of CDN live content requests.
CDN Content Errors	Number of CDN content request errors.
Fast Streaming-related WMT Requests	
Normal Speed	Number of normal-speed Fast Streaming-related WMT requests.
Fast Start Only	Number of Fast Start WMT requests.
Fast Cache Only	Number of Fast Cache WMT requests.
Fast Start and Fast Cache	Number of Fast Start and Fast Cache WMT requests.
Authenticated Requests	
By Type of Authentication	
Negotiate	Number of negotiated authentication authenticated requests.
Digest	Number of digest authentication authenticated requests.
Basic	Number of basic authentication authenticated requests.
Unicast Bytes Statistics	
Total unicast incoming bytes	Total number of bytes incoming as unicast streams.
By Type of Content	
Live content	Number of bytes incoming as unicast streams for live content.
On-Demand Content	Number of bytes incoming as unicast streams for on-demand content.
By Transport Protocol	
HTTP	Number of bytes incoming as unicast streams using the HTTP transport protocol.
RTSPT	Number of bytes incoming as unicast streams using the RTSPT transport protocol.
Total unicast outgoing bytes	Total number of bytes outgoing as unicast streams.
Unicast Savings Statistics	
Total bytes saved	Total number of bytes saved.

Table 2-70 *show statistics wmt all Field Descriptions (continued)*

Field	Description
By pre-positioned content	Number of bytes saved for pre-positioned content.
By live-splitting	Number of bytes saved for live-splitting content.
By cache-hit	Number of bytes saved for cached content.
Live Splitting	
Incoming bytes	Number of bytes incoming as live-split streams.
Outgoing bytes	Number of bytes outgoing as live-split streams.
Bytes saved	Number of bytes saved.
Caching	
Bytes cache incoming	Number of bytes incoming for the cache.
Bytes cache outgoing	Number of bytes outgoing from the cache.
Bytes cache total	Total number of bytes cached.
Bytes cache-bypassed	Number of bytes that bypassed the cache.
Cacheable requests	Number of cacheable requests.
Req cache-miss	Number of cacheable requests that were cache misses.
Req cache-hit	Number of cacheable requests that were cache hits.
Req cache-partial-hit	Number of cacheable requests that were partial cache hits.
Req cache-total	Total number of requests that were cached.
Objects not cached	Number of objects that were not cached.
Cache bypassed	Number of objects that were not cached because they bypassed the cache.
Exceed max-size	Number of objects that were not cached because they exceeded the maximum cacheable size limit.
Usage Summary	
Concurrent Unicast Client Sessions	Total number of concurrent unicast client sessions.
Current	Number of concurrent unicast client sessions currently running.
Max	Maximum number of concurrent unicast client sessions recorded.
Concurrent Remote Server Sessions	Total number of concurrent remote server sessions.
Concurrent Active Multicast Sessions	Total number of concurrent active multicast sessions.
Concurrent Unicast Bandwidth (Kbps)	Total amount of bandwidth being used (in kilobits per second) for concurrent unicast sessions.

Table 2-70 *show statistics wmt all Field Descriptions (continued)*

Field	Description
Concurrent Bandwidth to Remote Servers (Kbps)	Total amount of bandwidth being used (in kilobits per second) for concurrent remote server sessions.
Concurrent Multicast Out Bandwidth (Kbps)	Total amount of bandwidth being used (in kilobits per second) for concurrent multicast out sessions.
Error Statistics	
Total request errors	Total number of request errors.
Errors generated by this box	Number of request errors generated by this device.
Errors generated by remote servers	Number of request errors generated by remote servers.
Other Statistics	
Authentication Retries from Clients	Number of authentication retries from clients.
WMT Rule Template Statistics	
URL Rewrite	Number of URL rewrites.
URL Redirect	Number of URL redirects.
URL Block	Number of blocked URLs.
No-Cache	Number of no-cache matches.
Allow	Number of allow matches.
Multicast Statistics	
Total Multicast Outgoing Bytes	Total number of bytes outgoing as multicast-out streams.
Total Multicast Logging Requests	Total number of multicast logging requests.
Aggregate Multicast Out Bandwidth (Kbps)	Aggregated amount of bandwidth being used (in kilobits per second) for multicast out sessions.
Current	Number of concurrent multicast out sessions currently running.
Max	Maximum number of multicast out sessions recorded.
Number of Concurrent Active Multicast Sessions	Number of concurrent active multicast sessions.

Related Commands

clear
show wmt
wmt

show tacacs

To display TACACS+ authentication protocol configuration information, use the **show tacacs** EXEC command.

show tacacs

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes EXEC

Examples The **show tacacs** command displays the TACACS+ configuration for the Service Engine. [Table 2-71](#) describes the fields shown in the **show tacacs** display.

Table 2-71 show tacacs Field Descriptions

Field	Description
Login Authentication for Console/Telnet Session	Status of whether TACACS+ server is enabled for login authentication.
Configuration Authentication for Console/Telnet Session	Status of whether TACACS+ server is enabled for authorization or configuration authentication.
Authentication scheme fail-over reason	Status of whether Service Engines fail over to the secondary method of administrative login authentication whenever the primary administrative login authentication method is used.
TACACS+ Configuration	TACACS+ server parameters.
TACACS+ Authentication	Status of whether TACACS+ authentication is enabled on the Service Engine.
Key	Secret key that the Service Engine uses to communicate with the TACACS+ server. The maximum number of characters in the TACACS+ key should not exceed 99 printable ASCII characters (except tabs).
Timeout	Number of seconds that the Service Engine waits for a response from the specified TACACS+ authentication server before declaring a timeout.
Retransmit	Number of times that the Service Engine is to retransmit its connection to the TACACS+ server if the TACACS+ timeout interval is exceeded.
Password type	Mechanism for password authentication. By default, the Password Authentication Protocol (PAP) is the mechanism for password authentication.

Table 2-71 *show tacacs Field Descriptions (continued)*

Field	Description
Server	Hostname or IP address of the TACACS+ server.
Status	Status of whether server is the primary or secondary host.

Related Commands

clear
show statistics tacacs
tacacs

show tech-support

To view information necessary for the Cisco Technical Assistance Center (TAC) to assist you, use the **show tech-support EXEC** command.

show tech-support list-files *directory name*

show tech-support [**page**]

show tech-support service authentication [**acquisition-distribution** | **cms** | **flash-media-streaming** | **http** | **icap** | **kernel** | **movie-streamer** | **rules** | **wmt**]

show tech-support service cms [**acquisition-distribution** | **authentication** | **flash-media-streaming** | **http** | **icap** | **kernel** | **movie-streamer** | **rules** | **wmt**]

show tech-support service flash-media-streaming [**acquisition-distribution** | **authentication** | **cms** | **http** | **icap** | **kernel** | **movie-streamer** | **rules** | **wmt**]

show tech-support service http [**acquisition-distribution** | **authentication** | **cms** | **flash-media-streaming** | **icap** | **kernel** | **movie-streamer** | **rules** | **wmt**]

show tech-support service icap [**acquisition-distribution** | **authentication** | **cms** | **flash-media-streaming** | **http** | **kernel** | **movie-streamer** | **rules** | **wmt**]

show tech-support service kernel [**acquisition-distribution** | **authentication** | **cms** | **flash-media-streaming** | **http** | **icap** | **movie-streamer** | **rules** | **wmt**]

show tech-support service movie-streamer [**acquisition-distribution** | **authentication** | **cms** | **flash-media-streaming** | **http** | **icap** | **kernel** | **rules** | **wmt**]

show tech-support service rules [**acquisition-distribution** | **authentication** | **cms** | **flash-media-streaming** | **http** | **icap** | **kernel** | **movie-streamer** | **wmt**]

show tech-support service wmt [**acquisition-distribution** | **authentication** | **cms** | **flash-media-streaming** | **http** | **icap** | **kernel** | **movie-streamer** | **rules**]

Syntax Description

list-files	(Optional) Displays the list of files under a directory.
<i>directory name</i>	Directory name (use absolute path, such as /local1/logs).
page	(Optional) Specifies the pages through the output.
service	(Optional) Displays technical support information specific to a service.
authentication	Displays technical support information related to HTTP authentication.
acquisition-distribution	Displays technical support information related to acquisition and distribution.
cms	Displays technical support information related to CMS.
flash-media-streaming	Displays technical support information related to Flash media streaming.
http	Displays technical support information related to HTTP.
icap	Displays technical support information related to ICAP.
kernel	Displays technical support information related to the kernel.
movie-streamer	Displays technical support information related to the Movie Streamer.

rules	Displays technical support information related to rules.
wmt	Displays technical support information related to WMT.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Use this command to view system information necessary for TAC to assist you with your SE. We recommend that you log the output to a disk file. Use the streaming option to view information specific to the streaming feature.

The following types of information are available when using the streaming option with the **show tech-support** command.

General Information

You can access the following general information when you enter the **show tech-support** command:

- Version and hardware ([show version](#))
- Running configuration ([show running-config](#))
- Processes ([show processes](#))
- Process memory ([show processes memory](#))
- System memory
- File system information
- Interface information
- Media file system statistics
- Application and kernel core dump information
- Netstat

Information Common to WMT and RTSP

Information that is common to both WMT and RTSP is as follows:

- CPU or memory processes ([show programs](#))
- WMT streaming connections ([show statistics wmt streamstat](#))
- Bandwidth allocation ([show bandwidth](#))
- Bit rate allocation ([show bitrate](#))
- Acquirer information ([show acquirer](#))
- Rules ([show rule all](#))
- Distribution channel details

Information Specific to WMT

Information that is specific to WMT is as follows:

- WMT bandwidth and proxy mode configuration ([show wmt](#))

- WMT statistics ([show statistics wmt](#))

Information Specific to RTSP

Information that is specific to RTSP is as follows:

- RTSP configuration ([show rtsp](#))

Examples

The following example shows the types of information available about the CDS software. Because the **show tech-support** command output is comprehensive and can be extensive, only excerpts are shown in the following example.

```
ServiceEngine#show tech-support
```

CPU Usage:

```
cpu: 0.39% User, 0.42% System, 0.33% User(nice), 98.86% Idle
cpu0: 0.39% User, 0.42% System, 0.33% User(nice), 98.86% Idle
```

```
-----
PID  STATE  PRI  User  T   SYS  T   COMMAND
-----
1    S      0    4386  1706 (init)
2    S      0      0      0 (keventd)
3    S     19      0      0 (ksoftirqd_CPU0)
4    S      0      0      0 (kswapd)
5    S      0      0      0 (bdflood)
6    S      0      0      0 (kupdated)
7    S      0      0      0 (scsi_ah_0)
45   S      0    4733  4114 (nodemgr)
46   S      0      0      0 (syslogd)
47   R      0     83     65 (dataserver)
920  S      0      0      0 (login)
1207 S      0      0      0 (parser_server)
1208 S      0      0      0 (eval_timer_mana)
1211 S      0     46      1 (parser_server)
1443 S      0      0      0 (overload)
1444 S      0      0      0 (standby)
1445 S      0     13     29 (cache)
1446 S      0      0      0 (proxy_poll)
1447 S      0      0      0 (snmpcd)
1448 S      0      0      0 (http_authmod)
1458 S      0      0      0 (http_authmod)
1465 S      0      0      0 (http_authmod)
1466 S      0      0      0 (http_authmod)
1467 S      0      0      0 (http_authmod)
1537 S      0      0      0 (cache)
1538 S      0      0      0 (unified_log)
1540 S      0      0      1 (webserver)
1541 S      0      2      2 (mcm)
1542 S      0      0      0 (cache)
1543 S      0      0      0 (cache)
1550 S      0      0      0 (cache)
1551 S      0      0      0 (cache)
1556 S      0      0      0 (cache)
1567 S      0      0      0 (mcm)
1568 S      0      0      0 (mcm)
1629 S      0   18982  4140 (crond)
1936 S      0   1669     61 (bootnet)
1937 S     10      0      0 (tracknet)
1938 S     10  33545  5556 (checkup)
1983 S      0      0      0 (srcpd)
2023 S      0      1      0 (admin-shell)
2024 S      0      0      0 (parser_server)
```

show tech-support

```

2150    S    0      0      0 (rsrpd)
2152    S    0      0      0 (rtspd)
2153    S    0  1635  1067 (httpsd)
2164    S    0      0      0 (librarian)
2167    S    0  1667  2105 (libaux)
2170    S    0      0      0 (mapper)
2178    S    0    32    37 (cache)
2179    S    0      0      0 (router)
2180    S    0      0      0 (fill)
2183    S    0      0      0 (remotereq)
2185    S   -20     0      0 (videosvr)
2188    S    0     9     4 (contentsvr)
2189    S    0      0      0 (routeraux)
2190    S    0      0      1 (dfcontrolsrvr)
2226    S    0      0      0 (smbd)
2228    S    0      0      0 (nmbd)
2973    Z    0      0      0 (cache)
8446    S    0      0      0 (httpsd)
8447    S    0      0      0 (gcache)
18173   S    0      0      0 (in.telnetd)
18174   S    0      0      0 (login)
18175   S    0     2     2 (admin-shell)
18176   S    0      0      0 (parser_server)
19426   S    0      0      0 (httpsd)
19427   S    0      0      0 (httpsd)
19456   Z    0      0      0 (cache)
19503   Z    0    30     3 (crond)
19515   S    0      0      0 (more)
19516   S    0     6    18 (exec_show_tech-)
19553   R    0      0      0 (exec_show_proce)

```

----- process memory -----

Total	Used	Free	Shared	Buffers	Cached
1050943488	564785152	486158336	0	5222400	475176960

PID	State	TTY	%MEM	VM Size	RSS (pages)	Name
1	S	0	0.0	1146880	119	(init)
2	S	0	0.0	0	0	(keventd)
3	S	0	0.0	0	0	(ksoftirqd_CPU0)
4	S	0	0.0	0	0	(kswapd)
5	S	0	0.0	0	0	(bdflush)
6	S	0	0.0	0	0	(kupdated)
7	S	0	0.0	0	0	(scsi_eh_0)
45	S	0	0.0	1208320	143	(nodemgr)
46	S	0	0.0	1630208	194	(syslogd)
47	R	0	0.0	1974272	238	(dataserver)
920	S	1088	0.0	1728512	236	(login)
1207	S	0	0.3	4980736	847	(parser_server)
1208	S	0	0.0	1933312	151	(eval_timer_mana)
1211	S	0	0.3	4980736	847	(parser_server)
1443	S	0	0.0	1548288	154	(overload)
1444	S	0	0.0	1724416	161	(standby)
1445	S	0	5.9	65646592	15266	(cache)
1446	S	0	0.0	1957888	173	(proxy_poll)
1447	S	0	0.1	2097152	290	(snmpcd)
1448	S	0	0.0	1757184	205	(http_authmod)
1458	S	0	0.0	1757184	205	(http_authmod)
1465	S	0	0.0	1757184	205	(http_authmod)
1466	S	0	0.0	1757184	205	(http_authmod)

```

1467      S      0 0.0    1757184      205 (http_authmod)
1537      S      0 5.9    65646592    15266 (cache)
1538      S      0 0.0    1789952      169 (unified_log)
1540      S      0 0.4    10817536    1164 (webserver)
1541      S      0 0.0    2150400      251 (mcm)
1542      S      0 5.9    65646592    15266 (cache)
1543      S      0 5.9    65646592    15266 (cache)
1550      S      0 5.9    65646592    15266 (cache)
1551      S      0 5.9    65646592    15266 (cache)
1556      S      0 5.9    65646592    15266 (cache)
1567      S      0 0.0    2150400      251 (mcm)
1568      S      0 0.0    2150400      251 (mcm)
1629      S      0 0.0    1187840      137 (crond)
1936      S      0 0.6    7532544    1605 (bootnet)
1937      S      0 0.2    3215360      545 (tracknet)
1938      S      0 0.2    3637248      654 (checkup)
1983      S      0 0.3    4374528      838 (srcpd)
2023      S    1088 0.0    2146304      182 (admin-shell)
2024      S      0 0.3    4980736      847 (parser_server)
2150      S      0 0.0    1679360      188 (rsvpd)
2152      S      0 0.3    6217728      881 (rtspd)
2153      S      0 0.1    2527232      329 (httpsd)
2164      S      0 0.3    6533120      990 (librarian)
2167      S      0 0.4    7110656    1144 (libaux)
2170      S      0 0.3    5955584      863 (mapper)
2178      S      0 0.3    6135808      927 (cache)
2179      S      0 0.3    6287360      948 (router)
2180      S      0 0.3    5955584      926 (fill)
2183      S      0 0.3    5832704      852 (remotereq)
2185      S      0 0.3    8269824      873 (videosvr)
2188      S      0 0.4    7651328    1196 (contentsvr)
2189      S      0 0.3    6103040      953 (routeraux)
2190      S      0 0.4    10272768    1075 (dfcontrolsrvr)
2226      S      0 0.1    3559424      504 (smbd)
2228      S      0 0.0    2084864      247 (nmbd)
2973      Z      0 0.0          0          0 (cache)
8446      S      0 0.1    2506752      327 (httpsd)
8447      S      0 0.0    1421312      116 (gcache)
18173     S      0 0.0    1220608      132 (in.telnetd)
18174     S    34816 0.0    1736704      238 (login)
18175     S    34816 0.0    2162688      184 (admin-shell)
18176     S      0 0.3    4980736      847 (parser_server)
19426     S      0 0.1    2551808      350 (httpsd)
19427     S      0 0.1    2576384      354 (httpsd)
19456     Z      0 0.0          0          0 (cache)
19503     Z      0 0.0          0          0 (crond)
19515     S    34816 0.0    1163264      109 (more)
19516     S    34816 0.0    1941504      168 (exec_show_tech-)
19554     R    34816 0.1    2277376      266 (exec_show_proce)

```

----- system memory -----

```

Total physical memory : 1026312 KB
Total free memory    : 474692 KB
Total memory shared   : 0 KB
Total buffer memory   : 5100 KB
Total cached memory   : 464040 KB

```

----- interfaces -----

```

Interface type: GigabitEthernet Slot: 0 Port: 0
Type:Ethernet
Ethernet address:00:05:32:02:DD:74
Internet address:172.16.5.234

```

show tech-support

```
Netmask:255.255.255.0
Maximum Transfer Unit Size:1500
Metric:1
Packets Received: 513241
Input Errors: 0
Input Packets Dropped: 0
Input Packets Overruns: 0
Input Packets Frames: 0
Packet Sent: 153970
Output Errors: 0
Output Packets Dropped: 0
Output Packets Overruns: 0
Output Packets Carrier: 0
Output Queue Length:100
Collisions: 0
Interrupts:9
MULTICASTMode:autoselect, 100baseTX
```


show telnet

To display the Telnet services configuration, use the **show telnet** EXEC command.

show telnet

Syntax Description	This command has no arguments or keywords.

Defaults	Enabled

Command Modes	EXEC

Examples	The following example displays the Telnet service details:

```
ServiceEngine#show telnet
telnet service is enabled
```

Related Commands	exec-timeout telnet enable

show transaction-logging

To display the transaction log configuration settings and a list of archived transaction log files, use the **show transaction-logging** EXEC command.

show transaction-logging

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines To display information about the current configuration of transaction logging on an SE, use the **show transaction-logging** EXEC command. Transaction log file information is displayed for HTTP and WMT caching proxy transactions and TFTP and ICAP transactions.

Examples The following example displays information about the current configuration of transaction logging on an SE:

```
ServiceEngine#show transaction-logging
Transaction log configuration:
-----
Logging is enabled.
Archive interval: 1800 seconds
Maximum size of archive file: 2000000 KB
Maximum number of archive files: 50 files
Log File format is apache.
Windows domain is not logged with the authenticated username

Exporting files to ftp servers is enabled.
File compression is disabled.
Export interval: 30 minutes

server                type  username      directory
10.77.153.110          ftp   root          /var/ftp/test

WMT MMS Caching Proxy/Server Transaction Log File Info
  Working Log file - size : 556
                   age: 483497
  Archive Log file - mms_export_3.1.18.8_20090522_074807      size: 556

WMT MMS Caching Proxy/Server Transaction Log File Info (WMS-90 format)
  Working Log file - size : 665
                   age: 483497
  Archive Log file - mms_export_wms_90_3.1.18.8_20090522_074807 size: 665

WMT MMS Caching Proxy/Server Transaction Log File Info (Ext. WMS-90 format)
  Working Log file - size : 702
```

```

                                age: 483497
Archive Log file - mms_export_e_wms_90_3.1.18.8_20090522_074807      size: 70
2

WMT MMS Caching Proxy/Server Transaction Log File Info (Ext. WMS-41 format)
Working Log file - size : 584
                                age: 483497
Archive Log file - mms_export_e_wms_41_3.1.18.8_20090522_074807      size: 58
4

A&D Transaction Log File Info
Working Log file - size : 138
                                age: 483497
Archive Log file - acqdist_3.1.18.8_20090522_074807      size: 138
Movie Streamer Transaction Log File Info
Working Log file - size : 488
                                age: 482196
Archive Log file - movie-streamer_3.1.18.8_20090522_062602      size: 648
Archive Log file - movie-streamer_3.1.18.8_20090522_064309      size: 805
Archive Log file - movie-streamer_3.1.18.8_20090522_065857      size: 645
Archive Log file - movie-streamer_3.1.18.8_20090522_070038      size: 648
Archive Log file - movie-streamer_3.1.18.8_20090522_074807      size: 645
Archive Log file - movie-streamer_3.1.18.8_20090522_080016      size: 648
Archive Log file - movie-streamer_3.1.18.8_20090523_030829      size: 645
ICAP Transaction Log File Info
Working Log file - size : 61
                                age: 483496
Archive Log file - icap_3.1.18.8_20090522_074807      size: 61

Web Engine Transaction Log File Info - Apache format
Working Log file - size : 86
                                age: 483497
Archive Log file - we_accesslog_apache_3.1.18.8_20090522_074807      size: 82

Web Engine Transaction Log File Info - CLF format
Working Log file - size : 3
                                age: 483497
Archive Log file - we_accesslog_clf_3.1.18.8_20090522_074807      size: 3

Web Engine Transaction Log File Info - Extended Squid format
Working Log file - size : 102
                                age: 483497
Archive Log file - we_accesslog_extsqu_3.1.18.8_20090522_074807      size: 10
2

Cached Content Log File Info
Working Log file - size : 41
                                age: 483496
Archive Log file - cache_content_3.1.18.8_20090522_074807      size: 41

Flash Media Streaming Access Transaction Log File Info
Working Log file - size : 36
                                age: 482196
Archive Log file - fms_access_3.1.18.8_20090522_062602      size: 650
Archive Log file - fms_access_3.1.18.8_20090522_064309      size: 509
Archive Log file - fms_access_3.1.18.8_20090522_065857      size: 650
Archive Log file - fms_access_3.1.18.8_20090522_074807      size: 509
Archive Log file - fms_access_3.1.18.8_20090522_080016      size: 509
Archive Log file - fms_access_3.1.18.8_20090523_030830      size: 650

Flash Media Streaming Authorization Transaction Log File Info
Working Log file - size : 43
                                age: 482196
Archive Log file - fms_auth_3.1.18.8_20090522_062602      size: 4826

```

show transaction-logging

```

Archive Log file - fms_auth_3.1.18.8_20090522_063036 size: 281
Archive Log file - fms_auth_3.1.18.8_20090522_064309 size: 596
Archive Log file - fms_auth_3.1.18.8_20090522_065857 size: 4789
Archive Log file - fms_auth_3.1.18.8_20090522_070038 size: 277
Archive Log file - fms_auth_3.1.18.8_20090522_074807 size: 596
Archive Log file - fms_auth_3.1.18.8_20090523_030830 size: 4790

```

Authserver Transaction Log File Info

```

Working Log file - size : 108
                  age: 483496
Archive Log file - authsvr_3.1.18.8_20090522_065857 size: 108

```

ServiceEngine#

The following example displays information about the current configuration of transaction logging on an SR:

ServiceRouter#show transaction-logging

Transaction log configuration:

Logging is enabled.

Archive interval: 120 seconds

Maximum size of archive file: 2000000 KB

Maximum number of archive files: 50 files

Exporting files to ftp servers is enabled.

File compression is disabled.

Export interval: 1 minute

server	type	username	directory
10.74.115.12	sftp	xinwwang	/workspace/xinwwang/test
10.74.124.156	sftp	root	/root/test
10.74.124.157	sftp	root	/root/test
171.71.50.162	sftp	root	/test

Service Router Log File Info

```

Working Log file - size : 96
                  age: 169813
Archive Log file - service_router_3.1.14.70_20090421_222006 size: 256
Archive Log file - service_router_3.1.14.70_20090422_020038 size: 223
Archive Log file - service_router_3.1.14.70_20090422_210022 size: 351
Archive Log file - service_router_3.1.14.70_20090423_020006 size: 1248
Archive Log file - service_router_3.1.14.70_20090423_210021 size: 456
Archive Log file - service_router_3.1.14.70_20090521_000218 size: 402
Archive Log file - service_router_3.1.14.70_20090521_014815 size: 243
Archive Log file - service_router_3.1.14.70_20090521_015020 size: 225
Archive Log file - service_router_3.1.14.70_20090521_015227 size: 243
Archive Log file - service_router_3.1.14.70_20090521_015417 size: 272
Archive Log file - service_router_3.1.14.70_20090521_015601 size: 390
Archive Log file - service_router_3.1.14.70_20090521_015816 size: 243
Archive Log file - service_router_3.1.14.70_20090521_020033 size: 243
Archive Log file - service_router_3.1.14.70_20090521_020249 size: 143
Archive Log file - service_router_3.1.14.70_20090521_032633 size: 168
Archive Log file - service_router_3.1.14.70_20090526_025027 size: 143
Archive Log file - service_router_3.1.14.70_20090526_030002 size: 176
Archive Log file - service_router_3.1.14.70_20090526_030226 size: 250
Archive Log file - service_router_3.1.14.70_20090526_052206 size: 250
Archive Log file - service_router_3.1.14.70_20090526_052413 size: 143
Archive Log file - service_router_3.1.14.70_20090526_200213 size: 168
Archive Log file - service_router_3.1.14.70_20090526_200413 size: 481
Archive Log file - service_router_3.1.14.70_20090526_200645 size: 173
Archive Log file - service_router_3.1.14.70_20090526_201010 size: 250

```

Related Commands

clear
clear
show statistics transaction-logs
transaction-log force

show url-signature

To display the URL signature information, use the **show url-signature** EXEC command.

show url-signature

Syntax Description	This command has no arguments or keywords.

Defaults	No default behavior or values.

Command Modes	EXEC

Examples	The following example displays the URL signature information:

```
ServiceEngine#show url-signature
key-id-owner key-id-number key
-----
```

show user

To display the user identification number and username information for a particular user, use the **show user** EXEC command.

show user {**uid** *number* | **username** *name*}

Syntax Description

uid	Displays the user's identification number.
<i>number</i>	Identification number (0–65535).
username	Displays the name of user.
<i>name</i>	Name of the user.

Defaults

No default behavior or values.

Command Modes

EXEC

Examples

[Table 2-72](#) describes the fields shown in the **show user** display.

Table 2-72 *show user Field Descriptions*

Field	Description
Uid	User ID number.
Username	Username.
Password	Login password. This field does not display the actual password.
Privilege	Privilege level of the user.
Configured in	Database in which the login authentication is configured.

Related Commands

clear
show users
username

show users

To display users, use the **show users** EXEC command.

show users administrative

Syntax Description	administrative	Lists users with administrative privileges.

Defaults	No default behavior or values.

Command Modes	EXEC

Examples	The following example displays the list of users with administrative privileges: ServiceEngine# show users administrative UID USERNAME 0 admin

Related Commands	clear show user username

show version

To display version information about the SE software, use the **show version** EXEC command.

show version

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes EXEC

Examples [Table 2-73](#) describes the fields shown in the **show version** display.

Table 2-73 *show version Field Descriptions*

Field	Description
Compiled hour:minute:second month day year by cnbuild	Compile information for the software build.
System was restarted on day of week month day hour:minute:second year	Date and time that the system was last restarted.
The system has been up for X hours, X minutes, X seconds	Length of time the system has been running since the last reboot.

show wmt

To display Windows Media Technologies (WMT) bandwidth and proxy mode configuration, use the **show wmt** EXEC command.

show wmt [**bandwidth** [**incoming** **bypass-list**] | **detail** | **diagnostics** {**header-info** {**stream-file** *word* | **nsc-file** *.nsc-filename*} | **network-trace** *word*} **http** **allow** **extension**]

Syntax Description	
bandwidth	(Optional) Displays WMT bandwidth settings.
incoming	(Optional) Displays WMT incoming bandwidth settings.
bypass-list	Displays the WMT incoming bandwidth bypass list.
detail	(Optional) Displays the detailed WMT configuration.
diagnostics	(Optional) Displays a set of WMT diagnostics tools.
header-info	Displays the file header information.
stream-file	Displays the headers of a Windows Media file.
<i>word</i>	An .asf, .wma, .wmv URL, or local file.
nsc-file	Displays the .nsc file headers.
<i>.nsc-filename</i>	Name of a local or remote WMT station.
network-trace	Displays WMT diagnostics information.
<i>word</i>	Name of a local tcpdump file.
http	(Optional) Displays HTTP configurations.
allow	Displays the HTTP filename extensions allowed to be served using WMT.
extension	Displays the list of HTTP filename extensions to be served using WMT.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines You can access the following three WMT diagnostic tools through the SE CLI:

- **asfhead**—Examine the headers of a Windows Media file (for example, an .asf, .wmv, or .wma file). To access the asfhead tool, enter the **show wmt diagnostics header-info stream-file word** EXEC command.
- **nschead**—Examine the .nsc file headers. To access the nschead tool, enter the **show wmt diagnostics header-info nsc-file .nsc-filename** EXEC command.
- **mmsdig**—Use this text-based tool to decode the Multimedia Messaging Service (MMS) protocol (a binary protocol) that is captured in tcpdump traces (or any standard network trace output). To access this tool, enter the **show wmt diagnostics network trace word** EXEC command.

The mmsdig tool does not currently support decoding for RTSP, RTP, and RTCP.

Examples

The following example shows sample output of the **show wmt diagnostics header-info stream-file EXEC** command. In this example, this command is used to display the headers of a .wmv file named 256.wmv.

```
ServiceEngine# show wmt diagnostics header-info stream-file 256.wmv
Start dumping ASF header objects...
```

```
Obj: ASF_Header_Object (size 30)
    Header Len: 5342
    Header Num Of Objs: 8
Obj: ASF_File_Properties_Object (size 104)
    file_size: 429275084
    creation_time: 128208475755620000
    packet_count: 53656
    play_duration: 36050290000
    send_duration: 35992950000
    preroll: 5000
    flags: 2
    min_pktsize: 8000
    max_pktsize: 8000
    min_bitrate: 1003200
Obj: ASF_Stream_Properties_Object (size 114)
    time_offset: 0
    stream_type: ASF_Audio_Media
    ecc_type: ASF_Audio_Spread
    type_data_len: 28
    ecc_data_len: 8
    flags: 0x0001 (stream #: 1)
    ASF type specific data: -----
    id_tag: 161                num_channels: 2
    sample_per_sec: 48000      bytes_per_sec: 15875
    block_align: 2032          bits_per_sample: 16
    codec_data(size: 10):
    0x00 0x88 0x00 0x00 0x0f 0x00 0xf0 0x07
    0x00 0x00
    ASF Ecc data: -----
    span: 1
    packet_len: 2032           chunk_len: 2032
    silence_data (1 bytes): 0x00
Obj: ASF_Stream_Properties_Object (size 133)
    time_offset: 0
    stream_type: ASF_Video_Media
    ecc_type: ASF_No_Error_Correction
    type_data_len: 55
    ecc_data_len: 0
    flags: 0x0002 (stream #: 2)
    ASF type specific data: -----
    image_width: 320           image_height: 240
    flags: 2                   data_size: 44
    width: 320                 height: 240
    bits_per_pixel: 24          compression_id: 861293911
    data_size: 44              image_size: 0
    h_pixels_per_meter: 0      v_pixels_per_meter: 0
    color_count: 0             important_color_count: 0
    codec_data (4 bytes): 0x4e 0xd9 0x1a 0x01
Obj: ASF_Extended_Content_Description_Object (size 208)
Obj: ASF_Content_Description_Object (size 42)
    title:
    author:
    copyright:
    description:
    rating:
Obj: ASF_Stream_Bitrate_Properties_Object (size 38)
```

```

        bitrate record count: 2
        # 0: flags = 0x0001, bitrate = 129550
        # 1: flags = 0x0002, bitrate = 873650
Obj: ASF_Codec_List_Object (size 252)
    codec_list_entry count: 2
    entry # 0:
        name = Windows Media Audio 9.1
        description = 127 kbps, 48 kHz, stereo Low Delay 1-pass CBR
        0x61 0x01
    entry # 1:
        name = Windows Media Video 9
        description =
        0x57 0x4d 0x56 0x33
Obj: ASF_Header_Extension_Object (size 4421)
Obj: ASF_Language_List_Object (size 39)
Obj: ASF_Extended_Stream_Properties_Object (size 88)
Obj: ASF_Extended_Stream_Properties_Object (size 110)
Obj: ASF_Compatibility_Object (size 26)
Obj: ASF_Metadata_Object (size 224)
Obj: ASF_Padding_Object (size 3850)
Obj: ASF_GUID_Invalid/Unknown_Object (size 38)
    0x20 0xde 0xaa 0xd9 0x17 0x7c 0x9c 0x4f
    0xbc 0x28 0x85 0x55 0xdd 0x98 0xe2 0xa2
Obj: ASF_Data_Object (size 50)
    data_size: 429248050
    packet_count: 53656

```

The following example shows an excerpt of sample output from the **show wmt diagnostics header-info nsc-file** EXEC command. In this example, this command is used to display the headers of the .nsc file named live1.nsc.

```

ServiceEngine# show wmt diagnostics header-info nsc-file live1.nsc
Press Ctrl-C to abort, if no information is shown within 30 secs.

```

```

=====Dumping NSC file - live1.nsc=====

```

```

[Address]
Name=(null)
NSC Format Version=3.0
Multicast Adapter=(null)
IP Address=224.2.2.3
IP Port=96
Time To Live=15
Default Ecc=10
Log URL=http://kinslive.spcdn.net/live1.nsclog
Unicast URL=rtsp://kinslive.spcdn.net/live1
Allow Splitting=1
Allow Caching=1
Cache Expiration Time=86400
[Formats]
Format1=[Binary data skipped], len = 5316, key = 1111

```

```

-----Now trying to dump ASF header(0)-----

```

```

Obj: ASF_Header_Object (size 30)
    Header Len: 5266
    Header Num Of Objs: 8
Obj: ASF_File_Properties_Object (size 104)
    file_size: 5268
    creation_time: 128880472543590000
    packet_count: 4294967295
    play_duration: 0
    send_duration: 0
    preroll: 5000

```

```

    flags: 9
    min_pktsize: 8000
    max_pktsize: 8000
    min_bitrate: 1003200
Obj: ASF_Stream_Properties_Object (size 114)
    time_offset: 0
    stream_type: ASF_Audio_Media
    ecc_type: ASF_Audio_Spread
    type_data_len: 28
    ecc_data_len: 8
    flags: 0x0001 (stream #: 1)
    ASF type specific data: -----
        id_tag: 161                num_channels: 2
        sample_per_sec: 48000      bytes_per_sec: 15875
        block_align: 2032         bits_per_sample: 16
    codec_data(size: 10):
        0x00 0x88 0x00 0x00 0x0f 0x00 0xf0 0x07
        0x00 0x00
    ASF Ecc data: -----
        span: 1
        packet_len: 2032          chunk_len: 2032
        silence_data (1 bytes): 0x00
Obj: ASF_Stream_Properties_Object (size 133)
    time_offset: 0
    stream_type: ASF_Video_Media
    ecc_type: ASF_No_Error_Correction
    type_data_len: 55
    ecc_data_len: 0
    flags: 0x0002 (stream #: 2)
    ASF type specific data: -----
        image_width: 320          image_height: 240
        flags: 2                  data_size: 44
        width: 320                height: 240
        bits_per_pixel: 24        compression_id: 861293911
        data_size: 44             image_size: 0
        h_pixels_per_meter: 0     v_pixels_per_meter: 0
        color_count: 0            important_color_count: 0
    codec_data (4 bytes): 0x4e 0xd9 0x1a 0x01
Obj: ASF_Stream_Bitrate_Properties_Object (size 38)
    bitrate record count: 2
    # 0: flags = 0x0001, bitrate = 129550
    # 1: flags = 0x0002, bitrate = 873650
Obj: ASF_Extended_Content_Description_Object (size 164)
Obj: ASF_Codec_List_Object (size 252)
    codec_list_entry count: 2
    entry # 0:
        name = Windows Media Audio 9.1
        description = 127 kbps, 48 kHz, stereo Low Delay 1-pass CBR
        0x61 0x01
    entry # 1:
        name = Windows Media Video 9
        description =
        0x57 0x4d 0x56 0x33
Obj: ASF_Error_Correction_Object (size 48)
    ecc type: ASF_Error_Correction_Default
    data_len: 4
    ecc span: 10
Obj: ASF_Header_Extension_Object (size 4383)
Obj: ASF_Language_List_Object (size 39)
Obj: ASF_Extended_Stream_Properties_Object (size 88)
Obj: ASF_Extended_Stream_Properties_Object (size 110)
Obj: ASF_Compatibility_Object (size 26)
Obj: ASF_Metadata_Object (size 224)
Obj: ASF_Padding_Object (size 3850)

```

```
Obj: ASF_Data_Object (size 50)
    data_size: 50
    packet_count: 0
```

Some of the fields are common between the command output from the **show wmt diagnostics header-info stream-file** and **show wmt diagnostics header-info nsc-file EXEC** commands.

The following example shows the WMT server configurations, the WMT HTTP configurations, and the WMT proxy configurations for the SE. The output of the **show wmt** and **show wmt detail** commands is identical.

```
ServiceEngine#show wmt
----- WMT Server Configurations -----
WMT is enabled
WMT disallowed client protocols: http
WMT bandwidth platform limit: 2000000 Kbits/sec
WMT outgoing bandwidth configured is 2000000 Kbits/sec
WMT incoming bandwidth configured is 2000000 Kbits/sec
WMT max sessions configured: 400
WMT max sessions platform limit: 14000
WMT max sessions enforced: 400 sessions
WMT max outgoing bit rate allowed per stream has no limit
WMT max incoming bit rate allowed per stream has no limit
WMT cache is enabled
WMT cache max-obj-size: 10000 MB
WMT cache revalidate for each request is enabled
WMT cache age-multiplier: 100%
WMT cache min-ttl: 75 minutes
WMT cache max-ttl: 7 days
WMT debug client ip not set
WMT debug server ip not set
WMT accelerate live-split is enabled
WMT accelerate proxy-cache is enabled
WMT accelerate VOD is enabled
WMT fast-start is enabled
WMT fast-start max. bandwidth per player is 65535 (Kbps)
WMT fast-cache is enabled
WMT fast-cache acceleration factor is 65535
WMT maximum data packet MTU (TCP) enforced is 1472 bytes
WMT maximum data packet MTU (UDP) is 16000 bytes
WMT client idle timeout is 300 seconds
WMT forward logs is enabled
WMT server inactivity-timeout is 65535
WMT Transaction Log format is Windows Media Services 9.0 logging and SE specific
information
RTSP Gateway incoming port 554

----- WMT HTTP Configurations -----
WMT http extensions allowed:
asf none nsc wma wmv nsclog

----- WMT Proxy Configurations -----
Outgoing Proxy-Mode:
-----
MMS-over-HTTP Proxy-Mode:
    is not configured.
RTSP Proxy-Mode:
    is configured: 2.2.23.19:86
ServiceEngine#
```

The following example displays the WMT bandwidth settings configured on an SE:

```
ServiceEngine# show wmt bandwidth
Outgoing bandwidth configured 2000000 kbps
```

```
Incoming bandwidth configured 2000000 kbps  
Incoming bandwidth configured 50000 kbps
```

Related Commands

```
clear  
show statistics wmt  
wmt
```

shutdown (interface configuration)

To shut down a specific hardware interface, use the **shutdown** interface configuration command. To restore an interface to operation, use the **no** form of this command.

shutdown

no shutdown

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes Interface configuration

Usage Guidelines See the [“interface” section on page 2-120](#) section for alternative mechanism.

Examples The following example shows how to shut down an interface configured on an SE:

```
ServiceEngine(config-if)#shutdown
```

Related Commands

- interface**
- show interface**
- show running-config**
- show startup-config**

shutdown (EXEC)

To shut down the SE, SR, or CDSM, use the **shutdown** EXEC command.

shutdown [poweroff]

Syntax Description	poweroff (Optional) Turns off the power after closing all applications and the operating system.
Defaults	No default behavior or values.
Command Modes	EXEC
Usage Guidelines	A controlled shutdown refers to the process of properly shutting down an SE without turning off the power on the device. With a controlled shutdown, all of the application activities and the operating system are properly stopped on an SE but the power is still on. Controlled shutdowns of an SE can help you minimize the downtime when the SE is being serviced. The shutdown EXEC command enables you to shut down and optionally power off an SE: - Shutdown means that all application activities (applications and operating system) are stopped, but the power is still on. This shutdown is similar to the Linux halt command. - Shutdown poweroff means that the SE is powered down by the Internet Streamer CDS software after being shut down. This operation is also referred to as a software poweroff. The implementation of the shutdown poweroff feature uses the Advanced Configuration and Power Interface (ACPI) power management interface.
 Caution	If you do not perform a controlled shutdown, the SE file system can be corrupted. It also takes longer to reboot the SE if the SE is not properly shut down.
 Note	You cannot power on SEs again through software after a software poweroff operation. You must press the power button once on these SEs to bring these SEs back online.

The **shutdown** EXEC command facilitates a proper shutdown for SEs, SRs, or CDSMs. Where the **shutdown** command is supported on all content networking hardware models, the **shutdown poweroff** command is supported only on those models that support ACPI.

The **shutdown** command closes all applications and stops all system activities but keeps the power on. The fans continue to run and the power LED is on, indicating that the device is still powered on. When you enter the **shutdown** command, you are prompted to save your configuration changes, if any. The device console displays a menu after the shutdown process is completed. You need to log in to the SE using a console to display the following menu:

```
ServiceEngine#shutdown
System configuration has been modified. Save? [yes]:yes
```

```

Device can not be powered on again through software after shutdown.
Proceed with shutdown?[confirm]yes
Shutting down all services, will timeout in 15 minutes.
shutdown in progress ..Halt requested by CLI@ttyS0.
.....
Shutdown success

Cisco Service Engine Console

Username: admin
Password:

===== SHUTDOWN SHELL =====
    System has been shut down.

    You can either
        Power down system by pressing and holding power button
    or
    1. Reload system through software
    2. Power down system through software
    Please select [1-2]:

```

The **shutdown poweroff** command closes all applications and the operating system, stops all system activities, and turns off the power. The fans stop running and the power LED starts flashing, indicating that the device has been powered off.

**Note**

If you use the **shutdown** or **shutdown poweroff** commands, the device does not perform a file system check when you power on and boot the device the next time.

Table 2-74 describes the shutdown and shutdown power-off operations for SEs.

Table 2-74 Shutting Down Content Engines Through CLI Commands

Activity	All Content Engine Models	Content Engines with Power Management Capability
User performs a shutdown operation on the SE	ServiceEngine# shutdown	ServiceEngine# shutdown poweroff
User intervention to bring SE back online	To bring an SE that has an on/off switch on the back online after a shutdown operation, flip the on/off switch twice. To bring an SE that has a power button (instead of an on/off switch on the back) back online after a shutdown operation, first press and hold the power button for several seconds to power off these models, and then press the power button once again.	After a shutdown poweroff, you must press the power button once to bring the SE back online.
File system check	Will not be performed after you turn the power on again and reboot the SE.	Will not be performed after you turn the power on again and reboot the SE.

You can enter the **shutdown** EXEC command from a console session or from a remote session (Telnet or SSH version 1 or SSH version 2) to perform a shutdown on an SE.

To perform a shutdown on an SE, enter the **shutdown** EXEC command as follows:

```
ServiceEngine# shutdown
```

When you are asked if you want to save the system configuration, enter **yes** as follows:

```
System configuration has been modified. Save? [yes]:yes
```

When you are asked if you want to proceed with the shutdown, press **Enter** to proceed with the shutdown operation as follows:

```
Device can not be powered on again through software after shutdown.
Proceed with shutdown? [confirm]
```

The following message appears, reporting that all services are being shut down on this SE:

```
Shutting down all services, will timeout in 15 minutes.
shutdown in progress ..System halted.
```

After the system is shut down (the system has halted), an Internet Streamer CDS software shutdown shell displays the current state of the system (for example, "System has been shut down") on the console. You are asked whether you want to perform a software power off (the Power down system by software option), or if you want to reload the system through the software.

```
===== SHUTDOWN SHELL =====
System has been shut down.
You can either
    Power down system by pressing and holding power button
or
1. Reload system through software
2. Power down system through software
```

To power down the SE, press and hold the power button on the SE, or use one of the following methods to perform a shutdown poweroff:

- From the console command line, enter **2** when prompted as follows:

```
===== SHUTDOWN SHELL =====
System has been shut down.
You can either
    Power down system by pressing and holding power button
or
1. Reload system through software
2. Power down system through software
```

- From the SE CLI, enter the **shutdown poweroff** EXEC command as follows:

```
ServiceEngine# shutdown poweroff
```

When you are asked if you want to save the system configuration, enter **yes** as follows:

```
System configuration has been modified. Save? [yes]:yes
```

When you are asked to confirm your decision, press **Enter**.

```
Device can not be powered on again through software after poweroff.
Proceed with poweroff? [confirm]
Shutting down all services, will timeout in 15 minutes.
poweroff in progress ..Power down.
```

Examples

The following example shows that the **shutdown** command is used to close all applications and stop all system activities:

```
ServiceEngine1# shutdown
System configuration has been modified. Save?[yes]:yes
Device can not be powered on again through software after shutdown.
Proceed with shutdown?[confirm]
Shutting down all services, will timeout in 15 minutes.
shutdown in progress ..System halted.
```

The following example shows that the **shutdown poweroff** command is used to close all applications, stop all system activities, and then turn off power to the SE:

```
ServiceEngine2# shutdown poweroff
System configuration has been modified. Save?[yes]:yes
Device can not be powered on again through software after poweroff.
Proceed with poweroff?[confirm]
Shutting down all services, will timeout in 15 minutes.
poweroff in progress ..Power down.
```

snmp-server community

To configure the community access string to permit access to the Simple Network Management Protocol (SNMP), use the **snmp-server community** command in global configuration mode. To remove the specified community string, use the **no** form of this command.

snmp-server community *community-string* [**group** *group name* | **rw**]

no snmp-server community *community-string* [**group** *group name* | **rw**]

Syntax Description

<i>community-string</i>	Community string that acts like a password and permits access to SNMP.
group	(Optional) Specifies the group to which this community name belongs.
<i>group name</i>	Name of the group.
rw	(Optional) Specifies read-write access with this community string.

Defaults

An SNMP community string permits read-only access to all MIB objects.
A community string is assigned to the Secure Domain Router (SDR) owner.

Command Modes

Global configuration

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. Use the **snmp-server community** command to configure the community access string to permit access to SNMP. To remove the specified community string, use the **no** form of this command.



Note

In a non-owner SDR, a community name provides access only to the object instances that belong to that SDR, regardless of the access privilege assigned to the community name. Access to the owner SDR and system-wide access privileges are available only from the owner SDR.

Examples

The following example shows how to add the community comaccess:

```
ServiceEngine(config)#snmp-server community comaccess rw
```

The following example shows how to remove the community comaccess:

```
ServiceEngine(config)#no snmp-server community comaccess
```

Related Commands

snmp-server view

snmp-server contact

To set the system server contact (sysContact) string, use the **snmp-server contact** global configuration command. To remove the system contact information, use the **no** form of this command.

snmp-server contact *line*

no snmp-server contact

Syntax Description	<i>line</i> Identification of the contact person for this managed node.
Defaults	No system contact string is set.
Command Modes	Global configuration
Usage Guidelines	The system contact string is the value stored in the MIB-II system group sysContact object.
Examples	The following example shows how to configure a system contact string: <pre>ServiceEngine(config)#snmp-server contact Dial System Operator at beeper # 27345</pre> The following example resets the system contact string: <pre>ServiceEngine(config)#no snmp-server contact</pre>
Related Commands	show snmp snmp-server community snmp-server enable traps snmp-server group snmp-server host snmp-server location snmp-server notify inform snmp-server user snmp-server view

snmp-server enable traps

To enable the SE to send SNMP traps, use the **snmp-server enable traps** global configuration command. To disable all SNMP traps or only SNMP authentication traps, use the **no** form of this command.

snmp-server enable traps [**alarm** [**clear-critical** | **clear-major** | **clear-minor** | **raise-critical** | **raise-major** | **raise-minor**] | **config** | **entity** | **event** | **service-engine** [**disk-fail** | **disk-read** | **disk-write** | **transaction-log**] | **snmp** [**authentication** | **cold-start**]]

no snmp-server enable traps [**alarm** [**clear-critical** | **clear-major** | **clear-minor** | **raise-critical** | **raise-major** | **raise-minor**] | **config** | **entity** | **event** | **service-engine** [**disk-fail** | **disk-read** | **disk-write** | **transaction-log**] | **snmp** [**authentication** | **cold-start**]]

Syntax Description	
alarm	(Optional) Enables SE alarm traps.
clear-critical	(Optional) Enables the clear-critical alarm trap.
clear-major	(Optional) Enables the clear-major alarm trap.
clear-minor	(Optional) Enables the clear-minor alarm trap.
raise-critical	(Optional) Enables the raise-critical alarm trap.
raise-major	(Optional) Enables the raise-major alarm trap.
raise-minor	(Optional) Enables the raise-minor alarm trap.
config	(Optional) Enables CiscoConfigManEvent traps.
entity	(Optional) Enables SNMP entity traps.
event	(Optional) Enables Event MIB traps.
service-engine	(Optional) Enables SNMP SE traps.
disk-fail	(Optional) Enables the disk failure error trap.
disk-read	(Optional) Enables the disk read error trap.
disk-write	(Optional) Enables the disk write error trap.
transaction-log	(Optional) Enables the transaction log write error trap.
snmp	(Optional) Enables SNMP-specific traps.
authentication	(Optional) Enables the authentication trap.
cold-start	(Optional) Enables the cold-start trap.

Defaults

This command is disabled by default. No traps are enabled.

Command Modes

Global configuration

Usage Guidelines

You can configure an SE to generate an SNMP trap for a specific alarm condition. You can configure the generation of SNMP alarm traps on SEs based on the following:

- The severity of the alarm (critical, major, or minor)
- The action (the alarm is raised or cleared)

Cisco Internet Streamer Release 2.4 software supports six generic alarm traps. These six generic alarm traps provide SNMP and Node Health Manager integration. Each trap can be enabled or disabled through the SE CLI.

SNMP notifications can be sent as traps or inform requests. The **snmp-server enable traps** command enables both traps and inform requests for the specified notification types.

To configure traps, you must enter the **snmp-server enable traps** command. If you do not enter the **snmp-server enable traps** command, no traps are sent.

If you do not enter an **snmp-server enable traps** command, no notifications controlled by this command are sent. In order to configure the SE to send these SNMP notifications, you must enter at least one **snmp-server enable traps** command. If you enter the command with no keywords, all notification types are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled. In order to enable multiple types of notifications, you must enter a separate **snmp-server enable traps** command for each notification type and notification option.

The **snmp-server enable traps** command is used with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP traps. To send traps, you must configure at least one host using the **snmp-server host** command.

For a host to receive a trap, you must enable both the **snmp-server enable traps** command and the **snmp-server host** command for that host.

In addition, you must enable SNMP with the **snmp-server community** command.

To disable the sending of the MIB-II SNMP authentication trap, you must enter the **no snmp-server enable traps snmp authentication** command.

Examples

The following example enables the SE to send all traps to the host 172.31.2.160 using the community string public:

```
ServiceEngine(config)#snmp-server enable traps
ServiceEngine(config)#snmp-server host 172.31.2.160 public
```

The following example disables all traps:

```
ServiceEngine(config)#no snmp-server enable traps
```

Related Commands

- show snmp
- snmp-server community
- snmp-server contact
- snmp-server group
- snmp-server host
- snmp-server location
- snmp-server notify inform
- snmp-server user
- snmp-server view

snmp-server group

To define a user security model group, use the **snmp-server group** global configuration command. To remove the specified group, use the **no** form of this command.

```
snmp-server group name {v1 [notify name] [read name] [write name] | v2c [notify name] [read name] [write name] | v3 {auth [notify name] [read name] [write name] | noauth [notify name] [read name] [write name] | priv [notify name] [read name] [write name]}}
```

```
no snmp-server group name {v1 [notify name] [read name] [write name] | v2c [notify name] [read name] [write name] | v3 {auth [notify name] [read name] [write name] | noauth [notify name] [read name] [write name] | priv [notify name] [read name] [write name]}}
```

Syntax Description

<i>name</i>	Name of the SNMP group. Supports up to a maximum of 64 characters.
v1	Specifies the group using the Version 1 Security Model.
notify	(Optional) Specifies a notify view for the group that enables you to specify a notify, inform, or trap.
<i>name</i>	Notify view name. Supports up to a maximum of 64 characters.
read	(Optional) Specifies a read view for the group that enables you only to view the contents of the agent.
<i>name</i>	Read view name. Supports up to a maximum of 64 characters.
write	(Optional) Specifies a write view for the group that enables you to enter data and configure the contents of the agent.
<i>name</i>	Write view name. Supports up to a maximum of 64 characters.
v2c	Specifies the group using the Version 2c Security Model.
v3	Specifies the group using the User Security Model (SNMPv3).
auth	Specifies the group using the AuthNoPriv Security Level.
noauth	Specifies the group using the noAuthNoPriv Security Level.
priv	Specifies the group using the AuthPriv Security Level.

Defaults

The default is that no user security model group is defined.

Command Modes

Global configuration

Usage Guidelines

The maximum number of SNMP groups that can be created is 10.

Select one of three SNMP security model groups: Version 1 (**v1**) Security Model, Version 2c (**v2c**) Security Model, or the User Security Model (**v3** or SNMPv3). Optionally, you then specify a notify, read, or write view for the group for the particular security model chosen. The **v3** option allows you to specify the group using one of three security levels: **auth** (AuthNoPriv Security Level), **noauth** (noAuthNoPriv Security Level), or **priv** (AuthPriv Security Level).

The Internet Streamer CDS Release 2.4 software supports the following versions of SNMP:

- Version 1 (SNMPv1)—This version is the initial implementation of SNMP. See RFC 1157 for a full description of its functionality.
- Version 2 (SNMPv2c)—This version is the second release of SNMP, described in RFC 1902. It provides additions to data types, counter size, and protocol operations.
- Version 3 (SNMPv3)—This version is the most recent SNMP version, defined in RFC 2271 through RFC 2275.

SNMP Security Models and Security Levels

SNMPv1 and SNMPv2c do not have any security (authentication or privacy) mechanisms to keep SNMP packet traffic on the wire confidential. As a result, packets on the wire can be detected and SNMP community strings can be compromised.

To solve the security shortcomings of SNMPv1 and SNMPv2c, SNMPv3 provides secure access to SEs by authenticating and encrypting packets over the network. The SNMP agent in the Internet Streamer CDS Release 2.4 software supports SNMPv3, SNMPv1, and SNMPv2c.

Using SNMPv3, users can securely collect management information from their SNMP agents. Also, confidential information, such as SNMP set packets that change an SE's configuration, can be encrypted to prevent their contents from being exposed on the wire. Also, the group-based administrative model allows different users to access the same SNMP agent with varying access privileges.

Examples

The following example configures the SNMP group name, security model, and notify view on the SE:

```
ServiceEngine(config)#snmp-server group acme v1 notify mymib
```

Related Commands

```
show snmp
snmp-server community
snmp-server contact
snmp-server enable traps
snmp-server host
snmp-server location
snmp-server notify inform
snmp-server user
snmp-server view
```

snmp-server host

To specify the recipient of a host SNMP trap operation, use the **snmp-server host** global configuration command. To remove the specified host, use the **no** form of this command.

```
snmp-server host {hostname | ip-address} communitystring [v2c [retry number] [timeout
seconds] | [v3 {auth [retry number] [timeout seconds] | noauth [retry number] [timeout
seconds] | priv [retry number] [timeout seconds}]}
```

```
no snmp-server host {hostname | ip-address} [v2c [retry number] [timeout seconds] | [v3 {auth
[retry number] [timeout seconds] | noauth [retry number] [timeout seconds] | priv [retry
number] [timeout seconds}] | communitystring]
```

Syntax Description		
<i>hostname</i>		Hostname of the SNMP trap host that will be sent in the SNMP trap messages from the SE.
<i>ip-address</i>		IP address of the SNMP trap host that will be sent in the SNMP trap messages from the SE.
<i>communitystring</i>		Password-like community string sent in the SNMP trap messages from the SE. You can enter a maximum of 64 characters.
v2c		(Optional) Specifies the Version 2c Security Model.
retry		(Optional) Sets the count for the number of retries for the inform request. (The default is 2 tries).
<i>number</i>		Number of retries for the inform request (1–10).
timeout		(Optional) Sets the timeout for the inform request. The default is 15 seconds.
<i>seconds</i>		Timeout value in seconds (1–1000).
v3		(Optional) Specifies the User Security Model (SNMPv3).
auth		Sends notification using the AuthNoPriv Security Level.
noauth		Sends notification using the noAuthNoPriv Security Level.
priv		Sends notification using the AuthPriv Security Level.

Defaults This command is disabled by default. No traps are sent. The version of the SNMP protocol used to send the traps is SNMP Version 1.

retry number: 2 retries

timeout seconds: 15 seconds

Command Modes Global configuration

Usage Guidelines SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If the sender never receives the response, the inform request can be sent again. Inform requests are more likely to reach their intended destination.

However, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in the memory until a response is received or the request times out. Also, traps are sent only once, while an inform may be retried several times. The retries increase traffic and contribute to a higher overhead on the network.

If you do not enter an **snmp-server host** command, no notifications are sent. To configure the SE to send SNMP notifications, you must enter at least one **snmp-server host** command. To enable multiple hosts, you must enter a separate **snmp-server host** command for each host. You can specify multiple notification types in the command for each host.

When multiple **snmp-server host** commands are given for the same host and kind of security model, each succeeding command overwrites the previous command. Only the last **snmp-server host** command will be in effect. For example, if you enter an **snmp-server host v2c** command for a host and then enter another **snmp-server host v3** command for the same host, the second command will replace the first.

The maximum number of SNMP hosts that can be created by entering the **snmp-server host** commands is eight.

When multiple **snmp-server host** commands are given for the same host, the community string in the last command is used.

The **snmp-server host** command is used with the **snmp-server enable traps** command. Use the **snmp-server enable traps** command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one **snmp-server enable traps** command and the **snmp-server host** command for that host must be enabled.

**Note**

You must enable SNMP with the **snmp-server community** command.

Examples

The following example sends the SNMP traps defined in RFC 1157 to the host specified by the IP address 172.16.2.160. The community string is comaccess.

```
ServiceEngine(config)#snmp-server enable traps
ServiceEngine(config)#snmp-server host 172.16.2.160 comaccess
```

The following example removes the host 172.16.2.160 from the SNMP trap recipient list:

```
ServiceEngine(config)#no snmp-server host 172.16.2.160
```

Related Commands

```
show snmp
snmp-server community
snmp-server contact
snmp-server enable traps
snmp-server group
snmp-server location
snmp-server notify inform
snmp-server user
snmp-server view
```

snmp-server location

To set the SNMP system location string, use the **snmp-server location** global configuration command. To remove the location string, use the **no** form of this command.

snmp-server location *line*

no snmp-server location

Syntax Description	<i>line</i> String that describes the physical location of this node.

Defaults	No system location string is set.

Command Modes	Global configuration

Usage Guidelines	The system location string is the value stored in the MIB-II system group system location object. You can see the system location string with the show snmp EXEC command.

Examples	The following example shows how to configure a system location string: ServiceEngine(config)# snmp-server location Building 3/Room 214

Related Commands	show snmp snmp-server community snmp-server contact snmp-server enable traps snmp-server group snmp-server host snmp-server notify inform snmp-server user snmp-server view

snmp-server notify inform

To configure the SNMP notify inform request, use the **snmp-server notify inform** global configuration command. To return the setting to the default value, use the **no** form of this command.

snmp-server notify inform

no snmp-server notify inform

Syntax Description

This command has no arguments or keywords.

Defaults

If you do not enter the **snmp-server notify inform** command, the default is an SNMP trap request.

Command Modes

Global configuration

Usage Guidelines

The **snmp-server host** command specifies which hosts will receive informs. The **snmp-server enable traps** command globally enables the production mechanism for the specified notifications (traps and informs).

In order for a host to receive an inform, you must enable the inform globally by entering the **snmp-server notify inform** command.

The SNMP inform requests feature allows SEs to send inform requests to SNMP managers. SEs can send notifications to SNMP managers when particular events occur. For example, an agent SE might send a message to a manager when the agent SE experiences an error condition.

SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send any acknowledgment when it receives a trap. The sender cannot determine if the trap was received. However, an SNMP manager that receives an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If the manager does not receive an inform request, it does not send a response. If the sender never receives a response, the inform request can be sent again. Informs are more likely to reach their intended destination.

Because they are more reliable, informs consume more resources in the SE and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in the memory until a response is received or the request times out. Also, traps are sent only once, while an inform may be retried several times. The retries increase traffic and contribute to a higher overhead on the network. Traps and inform requests provide a trade-off between reliability and resources.



Tip

If it is important that the SNMP manager receives every notification, then you should use inform requests in your network. If you are concerned about traffic on your network or about the memory in the SE and you do not need to receive every notification, then you should use traps in your network.

Examples

The following example configures the SNMP notify inform request on the SE:

```
ServiceEngine(config)#snmp-server notify inform
```

Related Commands

- show snmp**
- snmp-server community**
- snmp-server contact**
- snmp-server enable traps**
- snmp-server group**
- snmp-server host**
- snmp-server location**
- snmp-server user**
- snmp-server view**

snmp-server user

To define a user who can access the SNMP server, use the **snmp-server user** global configuration command. To remove access, use the **no** form of this command.

```
snmp-server user name group [auth {md5 password [priv password] | sha password [priv password]}] | remote octetstring [auth {md5 password [priv password] | sha password [priv password]}]]
```

```
no snmp-server user name group [auth {md5 password | sha password} [priv password] | remote octetstring [auth {md5 password | sha password} [priv password]]]
```

Syntax Description

<i>name</i>	Name of the SNMP user. Use letters, numbers, dashes, and underscores, but no blanks. This is the name of the user on the SNMP host who wants to communicate with the SNMP agent on the SE. You can enter a maximum of 64 characters.
<i>group</i>	Name of the group to which the SNMP user belongs. You can enter a maximum of 64 characters.
auth	(Optional) Configures user authentication parameters.
md5	Configures the Hashed-Based Message Authentication Code Message Digest 5 (HMAC MD5) authentication algorithm.
<i>password</i>	HMAC MD5 user authentication password.
priv	(Optional) Configures authentication parameters for the packet.
<i>password</i>	HMAC MD5 user private password. You can enter a maximum of 256 characters.
sha	Configures the HMAC Secure Hash Algorithm (SHA) authentication algorithm.
<i>password</i>	HMAC SHA authentication password. You can enter a maximum of 256 characters.
remote	(Optional) Specifies the engine identity of the remote SNMP entity to which the user belongs.
<i>octetstring</i>	Globally unique identifier for a remote SNMP entity (for example, the SNMP network management station) for at least one of the SNMP users.

Defaults

No default behavior or values.

Command Modes

Global configuration

Usage Guidelines

The maximum number of SNMP users that can be created is 10. Follow these guidelines when defining SNMP users for SEs:

- If SNMPv3 is going to be used for SNMP requests, you must define at least one SNMPv3 user account on the SE in order for the SE to be accessed through SNMP.
- A group defined with the SNMPv1 or SNMPv2c security model should not be associated with SNMP users; they should only be associated with the community strings.



To send an SNMPv3 inform message, you must configure at least one SNMPv3 user with a remote SNMP ID option on the SE. The SNMP ID is entered in octet string form. For example, if the IP address of a remote SNMP entity is 192.147.142.129, then the octet string would be 00:00:63:00:00:00:a1:c0:93:8e:81.

Examples

The following example shows that an SNMPv3 user account is created on the SE. The SNMPv3 user is named acme and belongs to the group named admin. Because this SNMP user account has been set up with no authentication password, the SNMP agent on the SE does not perform authentication on SNMP requests from this user.

```
ServiceEngine(config)# snmp-server user acme admin
```

Related Commands

show snmp
snmp-server community
snmp-server contact
snmp-server enable traps
snmp-server group
snmp-server host
snmp-server location
snmp-server notify inform
snmp-server view

snmp-server view

To define a SNMP Version 2 (SNMPv2) MIB view, use the **snmp-server view** global configuration command. To undefine the MIB view, use the **no** form of this command.

snmp-server view *viewname* *MIBfamily* {**excluded** | **included**}

no snmp-server view *viewname* *MIBfamily* {**excluded** | **included**}

Syntax Description

<i>viewname</i>	Name of this family of view subtrees. You can enter a maximum of 64 characters.
<i>MIBfamily</i>	An object identifier that identifies a subtree of the MIB. You can enter a maximum of 64 characters.
excluded	Excludes the MIB family from the view.
included	Includes the MIB family from the view.

Defaults

No default behavior or values.

Command Modes

Global configuration

Usage Guidelines

An SNMP view is a mapping between SNMP objects and the access rights available for those objects. An object can have different access rights in each view. Access rights indicate whether the object is accessible by either a community string or a user. The **snmp-server view** command is used with the **snmp-server group** to limit the read-write access of MIB trees based on the group. Because the group can be associated with the SNMP community string or users, using the **snmp-server view** command extends the limit to users and community strings. If the view is not configured, read-write access to the community string applies to the MIB tree and all users (SNMPv3).

The maximum number of views that can be created is 10. You can configure the SNMP view settings only if you have previously configured the SNMP server settings.

To remove a view record, use the **no snmp-server view** command.

You can enter the **snmp-server view** command multiple times for the same view record. Later lines take precedence when an object identifier is included in two or more lines.

Examples

The following example shows how to configure the view name, family name, and view type:

```
ServiceEngine(config)#snmp-server view contentview ciscoServiceEngineMIB included
```

The following example creates a view that includes all objects in the MIB-II system group and all objects in the Cisco enterprise MIB:

```
ServiceEngine(config)#snmp-server view phred system included
ServiceEngine(config)#snmp-server view phred cisco included
```

The following example creates a view that includes all objects in the MIB-II system group except for sysServices (System 7) in the MIB-II interfaces group:

```
ServiceEngine(config)#snmp-server view agon system included  
ServiceEngine(config)#snmp-server view agon system.7 excluded
```

Related Commands

- show snmp**
- snmp-server community**
- snmp-server contact**
- snmp-server enable traps**
- snmp-server group**
- snmp-server host**
- snmp-server location**
- snmp-server notify inform**
- snmp-server user**

sshd

To enable the Secure Shell (SSH) daemon, use the **sshd** global configuration command. To disable SSH, use the **no** form of this command.

sshd {**enable** | **timeout** *seconds* | **version** {**1** | **2**}}

no sshd {**enable** | **password-guesses** | **timeout** | **version** {**1** | **2**}}

Syntax Description

enable	Enables the SSH feature.
timeout	Configures the number of seconds for which an SSH session will be active during the negotiation (authentication) phase between the client and the server before it times out.
	Note If you have established an SSH connection to the SE but have not entered the username when prompted at the login prompt, the connection will be terminated by the SE even after successful login if the grace period expires.
<i>seconds</i>	SSH login grace time value in seconds (1–99999). (The default is 300.)
version	Configures the SSH version to be supported on the SE.
1	Specifies that SSH version 1 is supported on the SE.
2	Specifies that SSH version 2 is supported on the SE.

Defaults

timeout *seconds*: 300 seconds.

version: Both SSH version 1 and 2 are enabled.

Command Modes

Global configuration

Usage Guidelines

SSH enables login access to the SE through a secure and encrypted channel. SSH consists of a server and a client program. Like Telnet, you can use the client program to remotely log on to a machine that is running the SSH server, but unlike Telnet, messages transported between the client and the server are encrypted. The functionality of SSH includes user authentication, message encryption, and message authentication.

When you enable the SSH server, the Secure File Transfer Protocol (SFTP) server is also enabled. The SFTP is a file transfer program that provides a secure and authenticated method for transferring files between CDS devices and other workstations or clients.



Note

SFTP is the standard file transfer protocol introduced in SSH version 2. The SFTP client functionality is provided as part of the SSH component. If you use SSH version 1 on the SE, SFTP support is not available.

The **sshd version** global configuration command allows you to enable support for either SSH version 1 or SSH version 2. When you enable SSH using the **sshd enable** global configuration command, the Internet Streamer CDS software enables support for both SSH version 1 and SSH version 2 on the SE. If you want the SE to support only one version of SSH (for example SSH version 2), you must disable the other version (in this example, SSH version 1) by using the **no sshd version 1** command.

When support for both SSH version 1 and SSH version 2 are enabled in the SE, the **show running-config EXEC** command output does not display any sshd configuration. If you have disabled the support for one version of SSH, the **show running-config EXEC** command output contains the following line:

```
no sshd version version_number
```

**Note**

You cannot disable both SSH versions in an SE. Use the **no sshd enable** global configuration command to disable SSH on the SE.

Examples

The following example shows how to enable the SSH daemon and configure the number of allowable password guesses and timeout for the SE:

```
ServiceEngine(config)#sshd enable
ServiceEngine(config)#sshd password-guesses 4
ServiceEngine(config)#sshd timeout 20
```

The following example disables the support for SSH version 1 in the SE:

```
ServiceEngine(config)#no sshd version 1
```

Related Commands

show ssh

sysreport

To save the sysreport to a user-specified file, use the **sysreport** privilege EXEC command.

sysreport {**acquisition-distribution** [**date-range** *start-date end-date* | *filename*] | **authentication** [**date-range** *start-date end-date* | *filename*] | **cms** [**date-range** *start-date end-date* | *filename*] | **dns** | **flash-media-streaming** | **ftp** | **http** | **icap** | **movie-streamer** | **rules** | **wmt**}

Syntax Description

acquisition-distribution	Generates sysreport information related to acquisition/distribution.
date-range	Specifies the date range of system report.
<i>start-date</i>	Specifies start date of system report following the format yyyy/mm/dd assuming local time zone.
<i>end-date</i>	Specifies the end date of system report following the format yyyy/mm/dd assuming local time zone.
<i>filename</i>	Filename (xxx.tar.gz) for system report.
authentication	Generates sysreport information related to http authentication.
cms	Generates sysreport information related to Centralized Management System (CMS).
dns	Generates sysreport information related to Domain Name Server (DNS).
flash-media-streaming	Generates sysreport information related to Flash Media Streaming.
ftp	Generates sysreport information related to FTP.
http	Generates sysreport information related to HTTP.
icap	Generates sysreport information related to ICAP
movie-streamer	Generates sysreport information related to Movie Streamer.
rules	Generates sysreport information related to rules.
wmt	Generates sysreport information related to Windows Media Technologies (WMT).

Defaults

No default behavior or values.

Command Modes

Privilege EXEC

Examples

The following example saves the sysreport for WMT to a user-specified file:

```
ServiceEngine#sysreport wmt date-range 2009/05/07 2009/05/11 xxx.tar.gz
The sysreport has been saved onto file xxx.tar.gz in local1
```

tacacs

To configure TACACS+ server parameters, use the **tacacs** command in global configuration mode. To disable individual options, use the **no** form of this command.

tacacs {**enable** | **host** {*hostname* | *ip-address*} [**primary**] | **key** *keyword* | **password** *ascii* | **retransmit** *retries* | **timeout** *seconds*}

no tacacs {**enable** | **host** {*hostname* | *ip-address*} [**primary**] | **key** | **password** *ascii* | **retransmit** | **timeout**}

Syntax Description	
enable	Enables the TACACS+ authentication.
host	Sets a server address.
<i>hostname</i>	Hostname of the TACACS+ server.
<i>ip-address</i>	IP address of the TACACS+ server.
primary	(Optional) Sets the server as the primary server.
key	Sets the security word.
<i>keyword</i>	Keyword. An empty string is the default.
password <i>ascii</i>	Specifies ASCII as the TACACS+ password type.
retransmit	Sets the number of times that requests are retransmitted to a server.
<i>retries</i>	Number of retry attempts allowed (1–3). The default is 2 retry attempts.
timeout	Sets the number of seconds to wait before a request to a server is timed out.
<i>seconds</i>	Timeout in seconds (1–20). The default is 5 seconds.

Defaults

keyword: none (empty string).

timeout *seconds*: 5

retransmit *retries*: 2

password *ascii*: PAP.

Command Modes

Global configuration

Usage Guidelines

Using the **tacacs** command, configure the TACACS+ key, the number of retransmits, the server hostname or IP address, and the timeout.

You must execute the following two commands to enable user authentication with a TACACS+ server:

```
ServiceEngine(config)# authentication login tacacs enable
ServiceEngine(config)# authentication configuration tacacs enable
```

You must enable TACACS+ for HTTP request authentication as follows:

```
ServiceEngine(config)# tacacs enable
```

TACACS+ can be disabled but remain configured for user authentication with a TACACS+ server if you use the **no** option of the command as follows:

```
ServiceEngine(config)# no tacacs enable
```

HTTP request authentication is independent of user authentication options and must be disabled with the following separate commands:

```
ServiceEngine(config)# no authentication login tacacs enable
ServiceEngine(config)# no authentication configuration tacacs enable
```

The Users GUI page or the **username** global configuration command provide a way to add, delete, or modify usernames, passwords, and access privileges in the local database. The TACACS+ remote database can also be used to maintain login and configuration privileges for administrative users. The **tacacs host** command or the TACACS+ Service Engine GUI page allows you to configure the network parameters required to access the remote database.

One primary and two backup TACACS+ servers can be configured; authentication is attempted on the primary server first and then on the others in the order in which they were configured. The primary server is the first server configured unless another server is explicitly specified as primary with the **tacacs host hostname primary** command.

Use the **tacacs key** command to specify the TACACS+ key that is used to encrypt the packets transmitted to the server. This key must be the same as the one specified on the server daemon. The maximum number of characters in the key should not exceed 99 printable ASCII characters (except tabs). An empty key string is the default. All leading spaces are ignored; spaces within and at the end of the key string are not ignored. Double quotes are not required even if there are spaces in the key, unless the quotes themselves are part of the key.

The **tacacs timeout** is the number of seconds that the Service Engine waits before declaring a timeout on a request to a particular TACACS+ server. The range is from 1 to 20 seconds with 5 seconds as the default. The number of times that the Service Engine repeats a retry-timeout cycle before trying the next TACACS+ server is specified by the **tacacs retransmit** command. The default is two retry attempts.

Three unsuccessful login attempts are permitted. TACACS+ logins may appear to take more time than local logins depending on the number of TACACS+ servers and the configured timeout and retry values.

Use the **tacacs password ascii** command to specify the TACACS+ password type as ASCII. The default password type is Password Authentication Protocol (PAP). In earlier releases, the password type was not configurable. When users needed to log in to a Service Engine, a TACACS+ client sent the password information in PAP format to a TACACS+ server. However, TACACS+ servers that were configured for router management required the passwords to be in ASCII clear text format instead of PAP format to authenticate users logging in to the Service Engine. The password type to authenticate user information to ASCII was configurable from the CLI.



Note

When the **no tacacs password ascii** command is used to disable the ASCII password type, the password type is once again reset to PAP.

The TACACS+ client can send different requests to the server for user authentication. The client can send a TACACS+ request with the PAP password type. In this scenario, the authentication packet includes both the username and the user's password. The server must have an appropriately configured user's account.

Alternatively, the client can send a TACACS+ request with the ASCII password type as another option. In this scenario, the authentication packet includes the username only and waits for the server response. Once the server confirms that the user's account exists, the client sends another Continue request with the user's password. The authentication server must have an appropriately configured user's account to support either type of password.

Examples

The following example configures the key used in encrypting packets:

```
ServiceEngine(config)#tacacs key human789
```

The following example configures the host named spearhead as the primary TACACS+ server:

```
ServiceEngine(config)#tacacs host spearhead primary
```

The following example sets the timeout interval for the TACACS+ server:

```
ServiceEngine(config)#tacacs timeout 10
```

The following example sets the number of times that authentication requests are retried (retransmitted) after a timeout:

```
ServiceEngine(config)#tacacs retransmit 5
```

The following example shows the password type to be PAP by default:

```
ServiceEngine#show tacacs
Login Authentication for Console/Telnet Session: enabled (secondary)
Configuration Authentication for Console/Telnet Session: enabled (secondary)

TACACS+ Configuration:
-----
TACACS+ Authentication is off
Key          = *****
Timeout      = 5
Retransmit   = 2
Password type: pap

Server                               Status
-----
10.107.192.148                        primary
10.107.192.168
10.77.140.77
ServiceEngine#
```

However, you can configure the password type to be ASCII using the **tacacs password ascii** command. You can then verify the changes using the **show tacacs** command as follows:

```
ServiceEngine(config)#tacacs password ascii
ServiceEngine(config)#exit
ServiceEngine#show tacacs
Login Authentication for Console/Telnet Session: enabled (secondary)
Configuration Authentication for Console/Telnet Session: enabled (secondary)

TACACS+ Configuration:
-----
TACACS+ Authentication is off
Key          = *****
Timeout      = 5
Retransmit   = 2
Password type: ascii
```

Server	Status
-----	-----
10.107.192.148	primary
10.107.192.168	
10.77.140.77	

Related Commands

- authentication
- show authentication
- show statistics authentication
- show statistics tacacs
- show tacacs

tcpdump

To dump the network traffic, use the **tcpdump** EXEC command.

tcpdump [*LINE*]

Syntax Description	<i>LINE</i> (Optional) Specifies the dump options.
Defaults	No default behavior or values.
Command Modes	EXEC

Usage Guidelines Use the **tcpdump** command to gather a sniffer trace on the SE, SR, or CDSM for troubleshooting when asked to gather the data by the Cisco TAC. This utility is very similar to the Linux or Unix **tcpdump** command.

The **tcpdump** command allows an administrator (must be an admin user) to capture packets from the Ethernet. On the SE 500 series, the interface names are eth0 and eth1. On all CDS platforms, we recommend that you specify a path/filename in the local1 directory.

You can do a straight packet header dump to the screen by entering the **tcpdump** command. Press **Ctrl-C** to stop the dump.

The **tcpdump** command has the following options:

- **-w <filename>**—writes the raw packet capture output to a file.
- **-s <count>**—captures the first <count> bytes of each packet.
- **-i <interface>**—allows you to specify a specific interface to use for capturing the packets.
- **-c <count>**—limits the capture to <count> packets.

The following example captures the first 1500 bytes of the next 10,000 packets from interface Ethernet 0 and puts the output in a file named dump.pcap in the local1 directory on the SE:

```
ServiceEngine#tcpdump -w /local1/dump.pcap -i eth0 -s 1500 -c 10000
```

When you specify the **-s** option, it sets the packet snap length. The default value captures only 64 bytes, and this default setting saves only packet headers into the capture file. For troubleshooting of redirected packets or higher level traffic (HTTP, authentication, and so on), you must copy the complete packets.

After the TCP dump has been collected, you need to move the file from the SE to a PC so that the file can be viewed by a sniffer decoder.

```
ftp <ip address of the SE>
```

```
!--- Log in using the admin username and password.
```

```
cd local1
bin
hash
```

```
get <name of the file>
```

```
!--- Using the above example, it would be dump.pcap.
```

```
bye
```

We recommend that you use Ethereal as the software application for reading the TCP dump. With Ethereal, you can decode packets that are encapsulated into a GRE tunnel. See the Ethereal website for further information.



Note

In most cases, redirected packets captured by the tcpdump facility with the CDS CLI differ from the data received on the interface. The destination IP address and TCP port number are modified to reflect the device IP address and the port number 8999.

Examples

The following example shows how to dump the TCP network traffic:

```
ServiceEngine#tcpdump
```

```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 68 bytes
12:45:42.617677 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P
3342832089:3342832201(112) ack 1248615673 win 15232
12:45:42.618950 IP 172.19.226.63 > ServiceEngine.cisco.com: icmp 36: 172.19.226.63 udp
port 2048 unreachable
12:45:42.619327 IP ServiceEngine.cisco.com.10015 > dns-sj2.cisco.com.domain:
49828+[]domain]
12:45:42.621158 IP dns-sj2.cisco.com.domain > ServiceEngine.cisco.com.10015: 49828
NXDomain*[]domain]
12:45:42.621942 IP ServiceEngine.cisco.com.10015 > dns-sj2.cisco.com.domain:
49829+[]domain]
12:45:42.623799 IP dns-sj2.cisco.com.domain > ServiceEngine.cisco.com.10015: 49829
NXDomain*[]domain]
12:45:42.624240 IP ServiceEngine.cisco.com.10015 > dns-sj2.cisco.com.domain:
49830+[]domain]
12:45:42.626164 IP dns-sj2.cisco.com.domain > ServiceEngine.cisco.com.10015:
49830*[]domain]
12:45:42.702891 802.1d config TOP_CHANGE 8000.00:03:9f:f1:10:63.8042 root
8000.00:01:43:9a:c8:63 pathcost 26 age 3 max 20 hello 2 fdelay 15
12:45:42.831404 IP 10.77.140.97.4314 > ServiceEngine.cisco.com.ssh: . ack 112 win 64351
12:45:42.831490 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: . 112:1444(1332) ack 1
win 15232
12:45:42.831504 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 1444:1568(124) ack 1
win 15232
12:45:42.831741 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 1568:1696(128) ack 1
win 15232
12:45:43.046176 IP 10.77.140.97.4314 > ServiceEngine.cisco.com.ssh: . ack 1568 win 65535
12:45:43.046248 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 1696:2128(432) ack 1
win 15232
12:45:43.046469 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 2128:2256(128) ack 1
win 15232
12:45:43.046616 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 2256:2400(144) ack 1
win 15232
12:45:43.107700 802.1d config TOP_CHANGE 8000.00:03:9f:f1:10:63.8042 root
8000.00:01:43:9a:c8:63 pathcost 26 age 3 max 20 hello 2 fdelay 15
12:45:43.199710 IP 10.77.140.97.4314 > ServiceEngine.cisco.com.ssh: . ack 1696 win 65407
12:45:43.199784 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 2400:2864(464) ack 1
win 15232
12:45:43.199998 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 2864:2992(128) ack 1
win 15232
```

```
12:45:43.259968 IP 10.77.140.97.4314 > ServiceEngine.cisco.com.ssh: . ack 2400 win 64703
12:45:43.260064 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 2992:3280(288) ack 1
win 15232
12:45:43.260335 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 3280:3408(128) ack 1
win 15232
12:45:43.260482 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 3408:3552(144) ack 1
win 15232
12:45:43.260621 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 3552:3696(144) ack 1
win 15232
12:45:43.413320 IP 10.77.140.97.4314 > ServiceEngine.cisco.com.ssh: . ack 2992 win 65535
12:45:43.413389 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 3696:3984(288) ack 1
win 15232
12:45:43.413597 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 3984:4112(128) ack 1
win 15232
12:45:43.413741 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 4112:4256(144) ack 1
win 15232
12:45:43.473601 IP 10.77.140.97.4314 > ServiceEngine.cisco.com.ssh: . ack 3552 win 64975
12:45:43.473659 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 4256:4544(288) ack 1
win 15232
12:45:43.473853 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 4544:4672(128) ack 1
win 15232
12:45:43.473994 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 4672:4816(144) ack 1
win 15232
12:45:43.474132 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 4816:4960(144) ack 1
win 15232
12:45:43.484117 IP 10.77.140.97.4314 > ServiceEngine.cisco.com.ssh: P 1:81(80) ack 3696
win 64831
12:45:43.484167 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 4960:5248(288) ack
81 win 15232
12:45:43.484424 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 5248:5392(144) ack
81 win 15232
12:45:43.627125 IP 10.77.140.97.4314 > ServiceEngine.cisco.com.ssh: . ack 4112 win 64415
12:45:43.627204 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 5392:5680(288) ack
81 win 15232
12:45:43.627439 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 5680:5808(128) ack
81 win 15232
12:45:43.627586 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 5808:5952(144) ack
81 win 15232
12:45:43.688261 IP 10.77.140.97.4314 > ServiceEngine.cisco.com.ssh: . ack 4544 win 65535
12:45:43.688316 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 5952:6240(288) ack
81 win 15232
12:45:43.688495 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 6240:6368(128) ack
81 win 15232
12:45:43.688638 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 6368:6512(144) ack
81 win 15232
12:45:43.689012 IP 10.77.140.97.4314 > ServiceEngine.cisco.com.ssh: . ack 4960 win 65119
12:45:43.689046 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 6512:6800(288) ack
81 win 15232
12:45:43.689170 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 6800:6928(128) ack
81 win 15232
12:45:43.689309 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 6928:7072(144) ack
81 win 15232
12:45:43.689447 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 7072:7216(144) ack
81 win 15232
12:45:43.698391 IP 10.77.140.97.4314 > ServiceEngine.cisco.com.ssh: . ack 5392 win 64687
12:45:43.698437 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 7216:7504(288) ack
81 win 15232
12:45:43.698599 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 7504:7632(128) ack
81 win 15232
12:45:43.698740 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 7632:7776(144) ack
81 win 15232
12:45:43.840558 IP 10.77.140.97.4314 > ServiceEngine.cisco.com.ssh: . ack 5808 win 64271
12:45:43.840622 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 7776:8064(288) ack
81 win 15232
```

```

12:45:43.840819 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 8064:8192(128) ack
81 win 15232
12:45:43.840962 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 8192:8336(144) ack
81 win 15232
12:45:43.901868 IP 10.77.140.97.4314 > ServiceEngine.cisco.com.ssh: . ack 6368 win 65535
12:45:43.901938 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 8336:8624(288) ack
81 win 15232
12:45:43.901887 IP 10.77.140.97.4314 > ServiceEngine.cisco.com.ssh: . ack 6928 win 64975
12:45:43.901910 IP 10.77.140.97.4314 > ServiceEngine.cisco.com.ssh: . ack 7216 win 64687
12:45:43.902137 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 8624:8752(128) ack
81 win 15232
12:45:43.902281 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 8752:8896(144) ack
81 win 15232
12:45:43.902414 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 8896:9024(128) ack
81 win 15232
12:45:43.902547 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 9024:9152(128) ack
81 win 15232
12:45:43.902687 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 9152:9296(144) ack
81 win 15232
12:45:43.902826 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 9296:9440(144) ack
81 win 15232
12:45:43.902965 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 9440:9584(144) ack
81 win 15232
12:45:43.903104 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 9584:9728(144) ack
81 win 15232
12:45:43.922413 IP 10.77.140.97.4314 > ServiceEngine.cisco.com.ssh: . ack 7632 win 64271
12:45:43.922459 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 9728:10304(576) ack
81 win 15232
12:45:43.922622 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 10304:10432(128) ack
81 win 15232
12:45:43.922764 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 10432:10576(144) ack
81 win 15232
12:45:44.053872 IP 10.77.140.97.4314 > ServiceEngine.cisco.com.ssh: . ack 8192 win 65535
12:45:44.053972 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 10576:10864(288) ack
81 win 15232
12:45:44.054308 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 10864:11104(240) ack
81 win 15232
12:45:44.054453 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 11104:11248(144) ack
81 win 15232
12:45:44.054596 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 11248:11392(144) ack
81 win 15232
12:45:44.111702 802.1d config TOP_CHANGE 8000.00:03:9f:f1:10:63.8042 root
8000.00:01:43:9a:c8:63 pathcost 26 age 3 max 20 hello 2 fdelay 15
12:45:44.114626 IP 10.77.140.97.4314 > ServiceEngine.cisco.com.ssh: . ack 8752 win 64975
12:45:44.114712 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 11392:11712(320) ack
81 win 15232
12:45:44.115219 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 11712:11952(240) ack
81 win 15232
12:45:44.115381 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 11952:12096(144) ack
81 win 15232
12:45:44.115426 IP 10.77.140.97.4314 > ServiceEngine.cisco.com.ssh: . ack 9152 win 64575
12:45:44.115617 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 12096:12336(240) ack
81 win 15232
12:45:44.115760 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 12336:12480(144) ack
81 win 15232
12:45:44.115904 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 12480:12624(144) ack
81 win 15232
12:45:44.116045 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 12624:12768(144) ack
81 win 15232
12:45:44.116094 IP 10.77.140.97.4314 > ServiceEngine.cisco.com.ssh: . ack 9440 win 64287
12:45:44.116114 IP 10.77.140.97.4314 > ServiceEngine.cisco.com.ssh: . ack 9728 win 65535
12:45:44.116332 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 12768:13088(320) ack
81 win 15232

```

```
12:45:44.116473 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 13088:13232(144) ack
81 win 15232
12:45:44.116614 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 13232:13376(144) ack
81 win 15232
12:45:44.116755 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 13376:13520(144) ack
81 win 15232
12:45:44.116895 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 13520:13664(144) ack
81 win 15232
12:45:44.135947 IP 10.77.140.97.4314 > ServiceEngine.cisco.com.ssh: . ack 10432 win 64831
12:45:44.135996 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 13664:13808(144) ack
81 win 15232
12:45:44.136223 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 13808:14048(240) ack
81 win 15232
12:45:44.136366 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P 14048:14192(144) ack
81 win 15232
12:45:44.144104 IP 10.77.140.97.4314 > ServiceEngine.cisco.com.ssh: P 81:161(80) ack 10576
win 64687

102 packets captured
105 packets received by filter
0 packets dropped by kernel
```

The following example shows how to dump the TCP network traffic and redirect it to a file named test:

```
ServiceEngine#tcpdump port 8080 -w test
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 68 bytes
216 packets captured
216 packets received by filter
0 packets dropped by kernel
```

telnet

To log in to a network device using the Telnet client, use the **telnet** EXEC command.

telnet {*hostname* | *ip-address*} [*portnum*]

Syntax Description

<i>hostname</i>	Hostname of the network device.
<i>ip-address</i>	IP address of the network device.
<i>portnum</i>	(Optional) Port number (1–65535). Default port number is 23.

Defaults

The default port number is 23.

Command Modes

EXEC

Usage Guidelines

Some UNIX shell functions, such as escape and the **suspend** command, are not available in the Telnet client. In addition, multiple Telnet sessions are also not supported.

The Telnet client allows you to specify a destination port. By entering the *telnet* command, you can test websites by attempting to open a Telnet session to the website from the SE CLI.

Examples

The following example shows how to open a Telnet session to a network device using the hostname:

```
ServiceEngine#telnet cisco-ce
```

The following example shows how to open a Telnet session to a network device using the IP address:

```
ServiceEngine#telnet 172.16.155.224
```

The following example shows how to open a Telnet session to a network device on port 8443 using the hostname:

```
ServiceEngine#telnet cisco-ce 8443
```

The following example shows how to open a Telnet session to a network device on port 80 using the hostname:

```
ServiceEngine#telnet www.yahoo.com 80
```


telnet enable

To enable Telnet, use the **telnet enable** global configuration command. To disable Telnet, use the **no** form of this command.

telnet enable

no telnet enable

Syntax Description	This command has no arguments or keywords.

Defaults	Enabled

Command Modes	Global configuration

Usage Guidelines	Use this terminal emulation protocol for a remote terminal connection. The telnet enable command allows users to log in to other devices using a Telnet session.

Examples	The following example shows how to enable Telnet on the SE:

```
ServiceEngine(config)#telnet enable
```

Related Commands	show telnet

terminal

To set the number of lines displayed in the console window, or to display the current console **debug** command output, use the **terminal** EXEC command.

terminal {**length** *length* | **monitor** [**disable**]}

Syntax Description

length	Sets the length of the display on the terminal.
<i>length</i>	Length of the display on the terminal (0–512). Setting the length to 0 means that there is no pausing.
monitor	Copies the debug output to the current terminal.
disable	(Optional) Disables monitoring at this specified terminal.

Defaults

The default length is 24 lines.

Command Modes

EXEC

Usage Guidelines

When 0 is entered as the *length* parameter, the output to the screen does not pause. For all nonzero values of *length*, the -More- prompt is displayed when the number of output lines matches the specified *length* number. The -More- prompt is considered a line of output. To view the next screen, press the **Spacebar**. To view one line at a time, press the **Enter** key.

The **terminal monitor** command allows a Telnet session to display the output of the **debug** commands that appear on the console. Monitoring continues until the Telnet session is terminated.

Examples

The following example sets the number of lines to display to 20:

```
ServiceEngine#terminal length 20
```

The following example configures the terminal for no pausing:

```
ServiceEngine#terminal length 0
```

Related Commands

All **show** commands

test-url

To test the accessibility of a URL using FTP, HTTP, or HTTPS, use the **test-url** EXEC command.

```
test-url {ftp url [use-ftp-proxy proxy-url] | http url [custom-header header [head-only]
[use-http-proxy proxy-url] | head-only [custom-header header] [use-http-proxy proxy-url] |
use-http-proxy proxy-url [custom-header header] [head-only]}}
```

Syntax Description		
ftp		Specifies the FTP URL to be tested.
<i>url</i>		FTP URL to be tested. Use one of the following formats to specify the FTP URL: <i>ftp://domainname/path</i> <i>ftp://user:password@domainname/path</i>
use-ftp-proxy		(Optional) Specifies the FTP proxy that is used to test the URL.
<i>proxy-url</i>		FTP proxy URL. Use one of the following formats to specify the proxy URL: <i>proxy IP Address:proxy Port</i> <i>proxy Username:proxy Password@proxy IP Address:proxy Port</i>
http		Specifies the HTTP URL to be tested.
<i>url</i>		HTTP URL to be tested. Use one of the following formats to specify the HTTP URL: <i>http://domainname/path</i> <i>http://user:password@domainname/path</i>
custom-header		(Optional) Specifies the custom header information to be sent to the server.
<i>header</i>		Custom header information to be sent to the server. Use the format <i>header:line</i> to specify the custom header.
head-only		(Optional) Specifies that only the HTTP header information must be retrieved.
use-http-proxy		(Optional) Specifies the HTTP proxy that is used to test the URL.
<i>proxy-url</i>		HTTP proxy URL. Use one of the following formats to specify the HTTP proxy URL: <pre>http://proxyIp:proxyPort http://proxyUser:proxypasswd@proxyIp:proxyPort</pre>
head-only		(Optional) Specifies that only the HTTPS header information must be retrieved.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines

In the Internet Streamer CDS Release 2.4 software and later releases, an HTTP CLI client is supported. This capability allows you to test connectivity and debug caching issues. The **test-url** EXEC command in the Internet Streamer CDS Release 2.4 software and later releases allows the users to test whether a URL is accessible over the FTP, HTTP, and HTTPS protocols. When you test the connectivity using the **test-url** command, the SE sends a request using the protocol that you have specified to the server and fetches the requested contents. The actual content is dumped into the path /dev/null, and the server response with the header information is displayed to the user.

You can use the **test-url ftp** command to test the following for the specified URL:

- Connectivity to the URL
- Connectivity to the URL through the FTP proxy (using the **use-ftp-proxy** option)
- Authentication
- FTP proxy authentication

You can use the **test-url http** command to test the following for the specified URL:

- Test the connectivity to the URL
- Test the connectivity to the URL through the HTTP proxy (using the **use-http-proxy** option)
- Authentication
- HTTP proxy authentication
- Header information only for the specified page (using the **head-only** option) or additional header information (using the **custom-header** option)

Examples

The following example tests the accessibility to the URL `http://192.168.171.22` using HTTP:

```
ServiceEngine#test-url http http://cel.server.com
--02:27:20-- http://cel.server.com/
=> `/dev/null'
Len - 22 , Restval - 0 , contlen - 0 , Res - 134728056Resolving cel.server.com..

done.
Connecting to cel.server.com[192.168.171.22]:80... connected.
HTTP request sent, awaiting response...
 1 HTTP/1.1 200 OK
 2 Date: Mon, 26 Jul 2004 08:41:34 GMT
 3 Server: Apache/1.2b8
 4 Last-Modified: Fri, 25 Apr 2003 12:23:04 GMT
 5 ETag: "laee29-663-3ea928a8"
 6 Content-Length: 1635
 7 Content-Type: text/html
 8 Via: 1.1 Content Delivery System Software 5.2
 9 Connection: Keep-Alive
(1635 to go)
0% [ ] 0 --.-K/s ETA --:--L
en - 0 ELen - 1635 Keepalive - 1
100%[=====>] 1,635 1.56M/s ETA 00:00

02:27:20 (1.56 MB/s) - `/dev/null' saved [1635/1635]
```

The following example tests the accessibility to the URL `http://192.168.171.22` through the HTTP proxy `10.107.192.148`:

```
ServiceEngine#test-url http http://192.168.171.22 use-http-proxy 10.107.192.148:8090
--15:22:51-- http://10.77.155.246/
=> `/dev/null'
```

```

Len - 1393 , Restval - 0 , contlen - 0 , Res - 134728344Connecting to
10.107.192.148:8090... connected.
Proxy request sent, awaiting response...
 1 HTTP/1.1 401 Authorization Required
 2 Date: Mon, 27 Sep 2004 15:29:18 GMT
 3 Server: Apache/1.3.27 (Unix) tomcat/1.0
 4 WWW-Authenticate: Basic realm="IP/TV Restricted Zone"
 5 Content-Type: text/html; charset=iso-8859-1
 6 Via: 1.1 Content Delivery System Software 5.2.1
 7 Connection: Close
Len - 0 , Restval - 0 , contlen - -1 , Res - -1Connecting to 10.107.192.148:8090...
connected.
Proxy request sent, awaiting response...
 1 HTTP/1.1 401 Authorization Required
 2 Date: Mon, 27 Sep 2004 15:29:19 GMT
 3 Server: Apache/1.3.27 (Unix) tomcat/1.0
 4 WWW-Authenticate: Basic realm="IP/TV Restricted Zone"
 5 Content-Type: text/html; charset=iso-8859-1
 6 Via: 1.1 Content Delivery System Software 5.2.1
 7 Connection: Keep-Alive
(1635 to go)
0% [                               ] 0          ---K/s      ETA ---L
en - 0      ELen - 1635      Keepalive - 1
100%[=====] 1,635          1.56M/s      ETA 00:00

02:27:20 (1.56 MB/s) - `/dev/null' saved [1635/1635]

```

The following example tests the accessibility to the URL `ftp://ssivakum:ssivakum@10.77.157.148` using FTP:

```

ServiceEngine#test-url ftp ftp://ssivakum:ssivakum@10.77.157.148/antinat-0.90.tar
Mar 30 14:33:44 nramaraj-ce admin-shell: %SE-PARSER-6-350232: CLI_LOG shell_parser_log:
test-url ftp ftp://ssivakum:ssivakum@10.77.157.148/antinat-0.90.tar
--14:33:44-- ftp://ssivakum:*password*@10.77.157.148/antinat-0.90.tar
      => `/dev/null'
Connecting to 10.77.157.148:21... connected.
Logging in as ssivakum ...
220 (vsFTPd 1.1.3)
--> USER ssivakum

331 Please specify the password.
--> PASS Turtle Power!
230 Login successful. Have fun.
--> SYST

215 UNIX Type: L8
--> PWD

257 "/home/ssivakum"
--> TYPE I

200 Switching to Binary mode.
==> CWD not needed.
--> PORT 10,1,1,52,82,16

200 PORT command successful. Consider using PASV.
--> RETR antinat-0.90.tar

150 Opening BINARY mode data connection for antinat-0.90.tar (1771520 bytes).
Length: 1,771,520 (unauthoritative)

0% [                               ] 0          ---K/s      ETA ---Len - 0      ELen - 1771520      Keepalive - 0

```

 test-url

```
100%[=====
>] 1,771,520    241.22K/s    ETA 00:00
```

```
226 File send OK.
```

```
14:33:53 (241.22 KB/s) - `/dev/null' saved [1771520]
```

```
ServiceEngine#
```

Related Commands **acquirer test-url**

traceroute

To trace the route to a remote host, use the **traceroute** EXEC command.

traceroute {hostname | ip-address}

Syntax Description	hostname	Name of the remote host.
	ip-address	IP address of the remote host.

Defaults No default behavior values

Command Modes EXEC

Usage Guidelines Traceroute is a widely available utility on most operating systems. Similar to ping, traceroute is a valuable tool for determining connectivity in a network. Ping allows the user to find out if there is a connection between the two end systems. Traceroute does this as well, but additionally lists the intermediate routers between the two systems. Users can see the routes that packets can take from one system to another. Use the **traceroute** command to find the route to a remote host when either the hostname or the IP address is known.

The **traceroute** command uses the TTL field in the IP header to cause routers and servers to generate specific return messages. Traceroute starts by sending a UDP datagram to the destination host with the TTL field set to 1. If a router finds a TTL value of 1 or 0, it drops the datagram and sends back an ICMP time-exceeded message to the sender. The traceroute facility determines the address of the first hop by examining the source address field of the ICMP time-exceeded message.

To identify the next hop, traceroute sends a UDP packet with a TTL value of 2. The first router decrements the TTL field by 1 and sends the datagram to the next router. The second router sees a TTL value of 1, discards the datagram, and returns the time-exceeded message to the source. This process continues until the TTL is incremented to a value large enough for the datagram to reach the destination host (or until the maximum TTL is reached).

To determine when a datagram has reached its destination, traceroute sets the UDP destination port in the datagram to a very large value that the destination host is unlikely to be using. When a host receives a datagram with an unrecognized port number, it sends an ICMP “port unreachable” error to the source. This message indicates to the traceroute facility that it has reached the destination.

Examples The following example shows how to trace the route to a remote host from the SE:

```
ServiceEngine#traceroute 10.77.157.43
traceroute to 10.77.157.43 (10.77.157.43), 30 hops max, 38 byte packets
 1  10.1.1.50 (10.1.1.50)  2.024 ms  2.086 ms  2.219 ms
 2  sblab2-rtr.cisco.com (192.168.10.1)  3.718 ms  172.19.231.249 (172.19.231.249)  0.653 ms  0.606 ms
 3  sjc22-00lab-gw1.cisco.com (172.24.115.65)  0.666 ms  0.624 ms  0.597 ms
 4  sjc20-lab-gw2.cisco.com (172.24.115.109)  0.709 ms  0.695 ms  0.616 ms
 5  sjc20-sbb5-gw2.cisco.com (128.107.180.97)  0.910 ms  0.702 ms  0.674 ms
 6  sjc20-rbb-gw5.cisco.com (128.107.180.9)  0.762 ms  0.702 ms  0.664 ms
 7  sjc12-rbb-gw4.cisco.com (128.107.180.2)  0.731 ms  0.731 ms  0.686 ms
```

```

 8  sjc5-gb3-f1-0.cisco.com (10.112.2.158)  1.229 ms  1.186 ms  0.753 ms
 9  capnet-hkidc-sjc5-oc3.cisco.com (10.112.2.238)  146.784 ms  147.016 ms  147.051 ms
10  hkidc-capnet-gw1-g3-1.cisco.com (10.112.1.250)  147.163 ms  147.319 ms  148.050 ms
11  hkidc-gb3-g0-1.cisco.com (10.112.1.233)  148.137 ms  148.332 ms  148.361 ms
12  capnet-singapore-hkidc-oc3.cisco.com (10.112.2.233)  178.137 ms  178.273 ms  178.005
ms
13  singapore-capnet2-fa4-0.cisco.com (10.112.2.217)  179.236 ms  179.606 ms  178.714 ms
14  singapore-gb1-fa2-0.cisco.com (10.112.2.226)  179.499 ms  179.914 ms  179.873 ms
15  capnet-chennai-singapore-ds3.cisco.com (10.112.2.246)  211.858 ms  212.167 ms  212.854
ms
16  hclodc1-rbb-gw2-g3-8.cisco.com (10.112.1.213)  213.639 ms  212.580 ms  211.211 ms
17  10.77.130.18 (10.77.130.18)  212.248 ms  212.478 ms  212.545 ms
18  codc-tbd.cisco.com (10.77.130.34)  212.315 ms  212.688 ms  213.063 ms
19  10.77.130.38 (10.77.130.38)  212.955 ms  214.353 ms  218.169 ms
20  10.77.157.9 (10.77.157.9)  217.217 ms  213.424 ms  222.023 ms
21  10.77.157.43 (10.77.157.43)  212.750 ms  217.260 ms  214.610 ms

```

The following example shows how the **tracert** command fails to trace the route to a remote host from the SE:

```

ServiceEngine#tracert 10.0.0.1
tracert to 10.0.0.1 (10.0.0.1), 30 hops max, 38 byte packets
 1  10.1.1.50 (10.1.1.50)  2.022 ms  1.970 ms  2.156 ms
 2  sblab2-rtr.cisco.com (192.168.10.1)  3.955 ms 172.19.231.249 (172.19.231.249)  0.654
ms  0.607 ms
 3  sjc22-00lab-gw1.cisco.com (172.24.115.65)  0.704 ms  0.625 ms  0.596 ms
 4  sjc20-lab-gw1.cisco.com (172.24.115.105)  0.736 ms  0.686 ms  0.615 ms
 5  sjc20-sbb5-gw1.cisco.com (128.107.180.85)  0.703 ms  0.696 ms  0.646 ms
 6  sjc20-rbb-gw5.cisco.com (128.107.180.22)  0.736 ms  0.782 ms  0.750 ms
 7  sjce-rbb-gw1.cisco.com (171.69.7.249)  1.291 ms  1.314 ms  1.218 ms
 8  sjce-corp-gw1.cisco.com (171.69.7.170)  1.477 ms  1.257 ms  1.221 ms
 9  * * *
10  * * *
.
.
.
29  * * *
30  * * *

```


Table 2-75 describes the fields in the **traceroute** command output.

Table 2-75 *traceroute Command Output Fields*

Field	Description
30 hops max, 38 byte packets	Maximum TTL value and the size of the ICMP datagrams being sent.
2.022 ms 1.970 ms 2.156 ms	Total time (in milliseconds) for each ICMP datagram to reach the router or host plus the time it took for the ICMP time-exceeded message to return to the host. An exclamation point following any of these values (for example, 20 ms !) indicates that the port-unreachable message returned by the destination had a TTL of 0 or 1. Typically, this situation occurs when the destination uses the TTL value from the arriving datagram as the TTL in its ICMP reply. The reply does not arrive at the source until the destination receives a traceroute datagram with a TTL equal to the number of hops between the source and destination.
*	An asterisk (*) indicates that the timeout period (default of 5 seconds) expired before an ICMP time-exceeded message was received for the datagram.

Related Commands

ping

traceroute6

To trace the route to a remote IPv6-enabled host, use the **traceroute6** EXEC command.

traceroute6 *ip-address*

Syntax Description

<i>ip-address</i>	Remote IPv6-enabled host or IP address.

Defaults

No default behavior values

Command Modes

EXEC

Examples

The following example shows how to trace the route to a remote IPv6-enabled host from the SE:

```
ServiceEngine#traceroute6 <IP address>
```

Related Commands

ipv6

transaction-log force

To force the archive or export of the transaction log, use the **transaction-log force** EXEC command.

transaction-log force {archive | export}

Syntax Description	archive	Forces the archive of the <i>working.log</i> file.
	export	Forces the archived files to be exported to the server.
Defaults	No default behavior or values.	
Command Modes	EXEC	
Usage Guidelines	The transaction-log force archive command causes the transaction log <i>working.log</i> file to be archived to the SE hard disk following the next transaction. This command has the same effect as the clear transaction-log command.	
	The transaction-log force export command causes the transaction log to be exported to an FTP server designated by the transaction-logs export ftp-server command.	
	The transaction-log force commands do not change the configured or default schedule for archive or export of transaction log files. If the archive interval is configured in seconds or the export interval is configured in minutes, the forced archive or export interval period is restarted after the forced operation.	
	If a scheduled archive or export job is in progress when a corresponding transaction-log force command is entered, the command has no effect. If a transaction-log force command is in progress when an archive or export job is scheduled to run, the forced operation is completed and the archive or export is rescheduled for the next configured interval.	

Examples

The following example shows how to archive the transaction log file to the SE hard disk:

```
ServiceEngine#transaction-log force archive
```

The following example shows that the SE is configured to export its transaction logs to two FTP servers:

```
ServiceEngine(config)# transaction-logs export ftp-server 10.1.1.1 mylogin mypasswd  
/ftpdirectory  
ServiceEngine(config)# transaction-logs export ftp-server myhostname mylogin mypasswd  
/ftpdirectory
```

The following example shows how to export the transaction log file from the SE hard disk to an FTP server designated by the **transaction-logs export ftp-server** command:

```
ServiceEngine#transaction-log force export
```

■ transaction-log force

Related Commands

clear
show statistics transaction-logs
show transaction-logging
transaction-logs

transaction-logs

To configure and enable transaction logs, use the **transaction-logs** command in global configuration mode. To disable transaction logs, use the **no** form of this command.

transaction-logs archive interval *seconds*

transaction-logs archive interval every-day {**at** *hour:minute* | **every** *hours*}

transaction-logs archive interval every-hour {**at** *minute* | **every** *minutes*}

transaction-logs archive interval every-week [**on** *weekdays* **at** *hour:minute*]

transaction-logs archive max-file-number *filenumber*

transaction-logs archive max-file-size *filesize*

transaction-logs enable

transaction-logs export compress

transaction-logs export enable

transaction-logs export ftp-server {*hostname* | *servipaddrs*} *login* *passw* *directory*

transaction-logs export interval *minutes*

transaction-logs export interval every-day {**at** *hour:minute* | **every** *hours*}

transaction-logs export interval every-hour {**at** *minute* | **every** *minutes*}

transaction-logs export interval every-week [**on** *weekdays* **at** *hour:minute*]

transaction-logs export sftp-server {*hostname* | *servipaddrs*} *login* *passw* *directory*

transaction-logs format {**apache** | **custom** *string* | **extended-squid**}

transaction-logs log-windows-domain

no transaction-logs {**archive** {**interval** | **max-file-number** | **max-file-size**} | **enable** | **export** {**compress** | **enable** | **ftp-server** {*hostname* | *servipaddrs*} | **interval** | **sftp-server** {*hostname* | *servipaddrs*}} | **format** | **log-windows-domain**}

Syntax Description

archive	Configures archive parameters.
interval	Determines how frequently the archive file is to be saved.
<i>seconds</i>	Frequency of archiving in seconds (120–604800).
every-day	Archives using intervals of 1 day or less.
at	Specifies the local time at which to archive each day.
<i>hour:minute</i>	Time of day at which to archive in local time (hh:mm).
every	Specifies the interval in hours. Interval aligns with midnight.

<i>hours</i>	Number of hours for daily file archive. 1—Hourly 12—Every 12 hours 2—Every 2 hours 24—Every 24 hours 3—Every 3 hours 4—Every 4 hours 6—Every 6 hours 8—Every 8 hours
every-hour	Specifies the archives using intervals of 1 hour or less.
at	Sets the time to archive at each hour.
<i>minute</i>	Minute alignment for the hourly archive (0–59).
every	Specifies the interval in minutes for hourly archive that aligns with the top of the hour.
<i>minutes</i>	Number of minutes for hourly archive. 10—Every 10 minutes 15—Every 15 minutes 2—Every 2 minutes 20—Every 20 minutes 30—Every 30 minutes 5—Every 5 minutes
every-week	Archives using intervals of 1 or more times a week.
on	(Optional) Sets the day of the week on which to archive.
<i>weekdays</i>	Weekdays on which to archive. One or more weekdays can be specified. Fri—Every Friday Mon—Every Monday Sat—Every Saturday Sun—Every Sunday Thu—Every Thursday Tue—Every Tuesday Wed—Every Wednesday
at	(Optional) Sets the local time at which to archive each day.
<i>hour:minute</i>	Time of day at which to archive in local time (hh:mm).
max-file-number	Sets the maximum number of the archived log file.
<i>filenumber</i>	Maximum number of the archived log file (1–10000).
max-file-size	Sets the maximum archive file size.
<i>filesize</i>	Maximum archive file size in kilobytes (1000–2000000).
enable	Enables the transaction log.
export	Configures file export parameters.
compress	Compresses the archived files in the gzip format before exporting.
enable	Enables the exporting of log files at the specified interval.
ftp-server	Sets the FTP server to receive exported archived files.
<i>hostname</i>	Hostname of the target FTP server.
<i>servipaddrs</i>	IP address of the target FTP server.
<i>login</i>	User login to target FTP server.

<i>passw</i>	User password to target FTP server.
<i>directory</i>	Target directory path for exported files on FTP server.
interval	Determines how frequently the file is to be exported.
<i>minutes</i>	Number of minutes in the interval at which to export a file (1–10080).
every-day	Specifies the exports using intervals of 1 day or less.
at	Specifies the local time at which to export each day.
<i>hour:minute</i>	Time of day at which to export in local time (hh:mm).
every	Specifies the interval in hours for the daily export.
<i>hours</i>	Number of hours for the daily export. 1—Hourly 12—Every 12 hours 2—Every 2 hours 24—Every 24 hours 3—Every 3 hours 4—Every 4 hours 6—Every 6 hours 8—Every 8 hours
every-hour	Specifies the exports using intervals of 1 hour or less.
at	Specifies the time at which to export each hour.
<i>minute</i>	Minute (0–59) alignment for the hourly export.
every	Specifies the interval in minutes that align with the top of the hour.
<i>minutes</i>	Number of minutes for the hourly export. 10—Every 10 minutes 15—Every 15 minutes 2—Every 2 minutes 20—Every 20 minutes 30—Every 30 minutes 5—Every 5 minutes
every-week	Specifies the exports using intervals of 1 or more times a week.
on	(Optional) Specifies the days of the week for the export.
<i>weekdays</i>	Weekdays on which to export. One or more weekdays can be specified. Fri—Every Friday Mon—Every Monday Sat—Every Saturday Sun—Every Sunday Thu—Every Thursday Tue—Every Tuesday Wed—Every Wednesday
at	(Optional) Specifies the time of day at which to perform the weekly export.
<i>hour:minute</i>	Time of day at which to export in the local time (hh:mm).
sftp-server	Sets the Secure File Transfer Protocol (SFTP) server to receive exported archived files.
<i>hostname</i>	Hostname of the target SFTP server.
<i>servipaddrs</i>	IP address of the target SFTP server.
<i>login</i>	User login to the target SFTP server (less than 40 characters).

<i>passw</i>	User password to the target SFTP server (less than 40 characters).
<i>directory</i>	Target directory path for exported files on the SFTP server.
format	Sets the format to use for the HTTP transaction log entries in the working.log file.
apache	Configures the HTTP transaction logs output to the Apache Common Log format (CLF).
custom	Configures the HTTP transaction logs output to the custom log format.
<i>string</i>	Quoted log format string containing the custom log format.
extended-squid	Configures the HTTP transaction logs output to the Extended Squid log format.
log-windows-domain	Logs the Windows domain with an authenticated username if available in HTTP transaction log entries.
enable	Enables the remote transaction logging.
entry-type	Specifies the type of transaction log entry.
all	Sets the SE to send all transaction log messages to the remote syslog server.
request-auth-failures	Sets the SE to log to the remote syslog server only those transactions that the SE failed to authenticate with the authentication server. Note Only those authentication failures that are associated with an end user who is attempting to contact the authentication server are logged. The transactions in pending state (that have contacted the authentication server, but waiting for a response from the authentication server) are not logged.
facility	Configures a unique facility to create a separate log on the remote syslog host for real-time transaction log entries.
<i>parameter</i>	Specifies one of the following facilities: auth Authorization system daemon System daemons kern Kernel local0 Local use local1 Local use local2 Local use local3 Local use local4 Local use local5 Local use local6 Local use local7 Local use mail Mail system news USENET news syslog Syslog itself user User process uucp UUCP system
host	Configures the remote syslog server.
<i>hostname</i>	Hostname of the remote syslog server.
<i>ip-address</i>	IP address of the remote syslog server.
port	Configures the port to use when sending transaction log messages to the syslog server.

<i>port-num</i>	Port number to use when sending transaction log messages to the syslog server (the default is 514).
rate-limit	Configures the rate at which the transaction logger is allowed to send messages to the remote syslog server.
<i>rate</i>	Rate (number of messages per second) at which the transaction logger is allowed to send messages to the remote syslog server.

Defaults

archive: disabled
enable: disabled
export compress: disabled
export: disabled
file-marker: disabled
archive interval: every day, every one hour
archive max-file-size: 2,000,000 KB
export interval: every day, every one hour
format: apache
logging port *port-num*: 514

Command Modes

Global configuration

Usage Guidelines

SEs that are running Cisco Internet Streamer Release 2.4 software can record all errors and access activities. Each content service module on the SE provides logs of the requests that were serviced. These logs are referred to as transaction logs.

Typical fields in the transaction log are the date and time when a request was made, the URL that was requested, whether it was a cache hit or a cache miss, the type of request, the number of bytes transferred, and the source IP address. Transaction logs are used for problem identification and solving, load monitoring, billing, statistical analysis, security problems, and cost analysis and provisioning.

The translog module on the SE handles transaction logging and supports the Apache Common Log Format (CLF), Extended Squid format, and the World Wide Web Consortium (W3C) customizable logging format.



Note

For RTSP, when you choose the **Repeat** option from the Play menu in the Windows Media player to play media files continuously in a loop, an extra entry is logged in the transaction logs for each playback of the file. This situation occurs mostly with the WMT RTSPU protocol due to the behavior of the player.

Enable transaction log recording with the **transaction-logs enable** command. The transactions that are logged include HTTP and FTP. In addition, Extensible Markup Language (XML) logging for MMS-over-HTTP and MMS-over-RTSP (RTSP over Windows Media Services 9) is also supported.

When enabled, daemons create a *working.log* file in */local1/logs/* on the sysfs volume for HTTP and FTP transactions and a separate *working.log* file in */local1/logs/export* for Windows Media transactions. The posted XML log file from the Windows Media Player to the SE (Windows Media server) can be parsed and saved to the normal WMT transaction logs that are stored on the SE.

The *working.log* file is a link to the actual log file with the timestamp embedded in its filename. When you configure the **transaction-logs archive interval** command, the first transaction that arrives after the interval elapses is logged to the *working.log* file as usual, and then actual log file is archived and a new log file is created. Only transactions subsequent to the archiving event are recorded in the new log file. The *working.log* file is then updated to point to the newly created log file. The transaction log archive file naming conventions are shown in [Table 2-82](#). The SE default archive interval is once an hour every day.

Use the **transaction-logs archive max-file-size** command to specify the maximum size of an archive file. The *working.log* file is archived when it attains the maximum file size if this size is reached before the configured archive interval time.

Use the **transaction-logs file-marker** option to mark the beginning and end of the HTTP, HTTPS, and FTP proxy logs. By examining the file markers of an exported archive file, you can determine whether the FTP process transferred the entire file. The file markers are in the form of dummy transaction entries that are written in the configured log format.

The following example shows the start and end dummy transactions in the default native Squid log format.

- 970599034.130 0 0.0.0.0 TCP_MISS/000 0 NONE TRANSLOG_FILE_START - NONE/- -
- 970599440.130 0 0.0.0.0 TCP_MISS/000 0 NONE TRANSLOG_FILE_END - NONE/- -

Use the **format** option to format the HTTP, HTTPS, and FTP proxy log files for custom format, native Squid or Extended Squid formats, or Apache Common Log Format (CLF).

The **transaction-logs format custom** command allows you to use a *log format string* to log additional fields that are not included in the predefined native Squid or Extended Squid formats or the Apache CLF format. The log format string is a string that contains the tokens listed in [Table 2-76](#) and mimics the Apache log format string. The log format string can contain literal characters that are copied into the log file. Two backslashes (\) can be used to represent a literal backslash, and a backslash followed by a single quotation mark (\') can be used to represent a literal single quotation mark. A literal double quotation mark cannot be represented as part of the log format string. The control characters \t and \n can be used to represent a tab and a new line character, respectively.

[Table 2-76](#) lists the acceptable format tokens for the log format string. The ellipsis (...) portion of the format tokens shown in this table represent an optional condition. This portion of the format token can be left blank, as in %a. If an optional condition is included in the format token and the condition is met, then what is shown in the Value column of [Table 2-76](#) is included in the transaction log output. If an optional condition is included in the format token but the condition is not met, the resulting transaction log output is replaced with a hyphen (-). The form of the condition is a list of HTTP status codes, which may or may not be preceded by an exclamation point (!). The exclamation point is used to negate all of the status codes that follow it, which means that the value associated with the format token is logged if none of the status codes listed after the exclamation point (!) match the HTTP status code of the request. If any of the status codes listed after the exclamation point (!) match the HTTP status code of the request, then a hyphen (-) is logged.

For example, %400,501{User-Agent}i logs the User-Agent header value on 400 errors and 501 errors (Bad Request, Not Implemented) only, and %!200,304,302{Referer}i logs the Referer header value on all requests that did not return a normal status.

The custom format currently supports the following request headers:

- User-Agent
- Referer
- Host
- Cookie

The output of each of the following Request, Referer, and User-Agent format tokens specified in the custom *log format string* is always enclosed in double quotation marks in the transaction log entry:

%r

%{Referer}i

%{User-Agent}i

The %{Cookie}i format token is generated without the surrounding double quotation marks, because the Cookie value can contain double quotes. The Cookie value can contain multiple attribute-value pairs that are separated by spaces. We recommend that when you use the Cookie format token in a custom format string, you should position it as the last field in the format string so that it can be easily parsed by the transaction log reporting tools. By using the format token string \"%{Cookie}i\" the Cookie header can be surrounded by single quotes (').

The following command can generate the well-known Apache Combined Log Format:

```
transaction-log format custom "[%{ %d}t/%{ %b}t/%{ %Y}t:%{ %H}t:%{ %M}t:%{ %S}t  
%{ %z}t] %r %s %b %{Referer}i %{User-Agent}i"
```

The following transaction log entry example in the Apache Combined Format is configured using the preceding custom format string:

```
[11/Jan/2003:02:12:44 -0800] "GET http://www.cisco.com/swa/i/site_tour_link.gif HTTP/1.1"  
200 3436 "http://www.cisco.com/" "Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0)"
```

Table 2-76 Custom Format “Log Format String” Values

Format Token	Value
%...a	IP address of the requesting client.
%...A	IP address of the SE.
%...B %...b	Bytes sent excluding HTTP headers.
%...c	Connection status when response is completed where X = Connection was aborted before the response was completed. + = Connection can be kept alive after the response is sent. – = Connection is closed after the response is sent.
%...f	Filename.
%...h	Remote host (IP address of the requesting client is logged).
%...H	Request protocol.
%...{Foobar}i	Contents of Foobar: header lines in the request that is sent to the server. The value of Foobar can be one of the following headers: User-Agent, Referer, Host, or Cookie.
%...l	Remote log name. Not implemented on the SE, so a hyphen (-) is logged.
%...m	Request method.

Table 2-76 Custom Format “Log Format String” Values (continued)

Format Token	Value
%...p	Canonical port of the server servicing the request. Not applicable on the SE, so a hyphen (-) is logged.
%...P	Process ID of the child that serviced the request.
%...q	Query string (that is preceded by a question mark (?) if a query string exists; otherwise, it is an empty string).
%...r	First line of the request.
%...s	Status. The translog code always returns the HTTP response code for the request.
%...t	Time in common log time format (or standard English format).
%...{format}t	Time in the form given by the format token specified in Table 2-77 .
%...T	Time consumed to serve the request in seconds (a floating point number with three decimal places).
%...u	Remote user.
%...U	URL path requested not including query strings.
%...v %...V	Value of the host request header field reported if the host appeared in the request. If the host did not appear in the host request header, the IP address of the server specified in the URL is reported.

[Table 2-77](#) specifies the format token for the date and time of the format token %...{format}t that is listed in [Table 2-78](#).

Table 2-77 Format Token for Date and Time

Format Token	Value
%a	Abbreviated weekday name.
%A	Full weekday name.
%b	Abbreviated month name.
%B	Full month name.
%c	Date and time representation.
%C	Century number (year/100) as a 2-digit integer.
%d	Day of the month as a decimal number (01–31).
%D	Equivalent to %m/%d/%y. (In countries other than the USA, %d/%m/%y is common. In an international context, this format is ambiguous and should not be used.)
%e	Similar to %d, the day of the month as a decimal number, but a leading zero is replaced by a space.
%G	ISO 8601 year with the century as a decimal number. The 4-digit year corresponding to the ISO week number (see %V). This format token has the same format and value as %y, except that if the ISO week number belongs to the previous or next year, that year is used instead.
%g	Similar to %G, but without a century; that is, with a 2-digit year (00–99).
%h	Equivalent to %b.

Table 2-77 *Format Token for Date and Time (continued)*

Format Token	Value
%H	Hour as a decimal number using a 24-hour clock (00–23).
%I	Hour as a decimal number using a 12-hour clock (01–12).
%j	Day of the year as a decimal number (001–366).
%k	Hour (24-hour clock) as a decimal number (0–23); single digits are preceded by a blank. (See also %H.)
%l	Hour (12-hour clock) as a decimal number (1–12); single digits are preceded by a blank. (See also %I.)
%m	Month as a decimal number (01–12).
%M	Minute as a decimal number (00–59).
%n	New line character.
%p	Either AM or PM according to the given time value, or the corresponding strings for the current locale. Noon is treated as PM and midnight as AM.
%P	Similar to %p but in lowercase: am or pm or a corresponding string for the current locale.
%r	Time in a.m. or p.m. notation. This format token is equivalent to “%I:%M:%S %p.”
%R	Time in 24-hour notation (%H:%M). For a version including the seconds, see %T below.
%s	Number of seconds since the epoch; that is, since 1970-01-01 00:00:00 UTC.
%S	Second as a decimal number (00–61).
%t	Tab character.
%T	Time in 24-hour notation (%H:%M:%S).
%u	Day of the week as a decimal, 1–7, Monday being 1. See also %w.
%U	Week number of the current year as a decimal number (00–53), starting with the first Sunday as the first day of week 01. See also %V and %W.
%V	ISO 8601:1988 week number of the current year as a decimal number (01–53), where week 1 is the first week that has at least 4 days in the current year, and with Monday as the first day of the week. See also %U and %W.
%w	Day of the week as a decimal (0–6) with Sunday as 0. See also %u.
%W	Week number of the current year as a decimal number (00–53), starting with the first Monday as the first day of week 01.
%x	Date representation without the time.
%X	Time representation without the date.
%y	Year as a decimal number without a century (00–99).
%Y	Year as a decimal number, including the century.
%z	Time zone as an hour offset from GMT. Required to emit RFC822-conformant dates (using %a, %d %b %Y %H:%M:%S %z).
%Z	Time zone or name or abbreviation.
%%	Literal % character.

The Extended Squid log format uses the RFC 981 field of the Squid log format for the username. The Extended Squid format logs the associated username for authentication for each record in the log file, if available. The username is also used for billing purposes.

The W3C Customizable Logging Format is limited in that it was defined from the HTTP web server perspective and does not offer certain web cache-specific custom options such as those supplied by the fixed Squid format. Format tokens that are extensions to the W3C Customized Logging Format support additional Cisco and Squid customized logging fields. These format tokens provide support for a Squid-like logging format from within the W3C customizable token set.

The W3C Customizable Logging Format was extended to include support for the following special token sequence:

```
%...{<translog-token>}C
```

The ellipsis (...) is optional. If specified, it can be a sequence of conditional HTTP response codes separated by commas. The uppercase C defines the extended customizable behavior token set, for which tokens are defined by the <translog-token> directive, which is a two-character token directive.

Table 2-78 lists the existing and new <translog-token> directives from the Extended Squid format, which are not immediately supported by the W3C definitions but are supported in the CDS Release 2.4 software.

Table 2-78 Translog Token Directives

Format Token	Value
%...{es}C	Current time presented as the number of seconds that have elapsed since the Epoch (Jan. 1st. 1970).
%...{em}C	Current number of milliseconds that have elapsed since the Epoch (Jan. 1st. 1970).
%...{te}C	Number of milliseconds that have elapsed until the request was completed.
%...{rd}C	Squid-like cache-status code string (for example, TCP_HIT and TCP_CLIENT_REFRESH_MISS).
%..{cs}C	Number of bytes sent to the client (including the protocol headers).
%...{rh}C	Strict Squid-style hierarchy as it applies to the SE.
%...{rh}SE	Extended Squid-style hierarchy. Same as %...{rh}C except when an outgoing-proxy is explicitly defined and is used to satisfy a request, then the DEFAULT_PARENT/proxy_ip_address is logged instead of the DIRECT/origin_server_ip_address.

Table 2-78 Translog Token Directives (continued)

Format Token	Value
%...{rt}C	MIME type of the object in the response, as specified by any protocol headers that define such MIME types. Currently, Cisco Internet Streamer Release 2.4 software does not support logging the MIME type of the object that is being requested, and a hyphen (-) is logged instead. Note This restriction also applies to the Squid and Extended Squid logging formats. Tip A MIME-type association enables the browser to invoke a particular application when it encounters an object with a particular MIME-type suffix. A set of default association rules covers the common object types on the Internet. You can edit, add, or delete these MIME-type association rules in the browsers. For example, through a MIME-type association, the client browser launches the Adobe Acrobat reader when it encounters a *.pdf file, and it launches the Windows Media Player when it encounters an *.asf or *.asx file.
%...{ru}C	URL being requested including any additional query strings.
%...{as}C	Application-specific information. Certain request handling applications might want to log a certain string here, which is supported as part of the Squid format specification. For example, SmartFilter URL filtering logs information where this token sequence is used.

In addition to the tokens listed in [Table 2-78](#), you can condense multiple %...{xx}C style tokens into a single embedded token sequence within the %...{xx}C style. A limited customized logging string validation mechanism has been implemented for all the %...{xy}C style format tokens. This mechanism ensures that the tokens are valid and rejects invalid tokens. To condense multiple style tokens into a single embedded token sequence, you must specify multiple tokens within the {} braces and prefix each token with the percent (%) symbol as follows:

```
%{rh}C %{rt}C %{as}C
```

can be reexpressed in a condensed embedded token format as the following:

```
%{%rh %rt %as}C
```

The command line syntax accepts single tokens represented as the following:

```
%{%rh}C
```

and

```
%{rh}C
```

as equivalents.

Any character that is not part of an embedded token sequence (for example, the space character) is repeated verbatim in the output file.

The above set of tokens allow you to configure an extended Squid-like format line within the W3C Customizable Logging format specification as follows:

```
%{es}C.%{em}C %{te}C %a %{rd}C/%s %{cs}C %m %{ru}C %u %{rh}C %{rt}C %{as}C
```

The following is an example of a Extended Squid-like format that specifies that user-readable time-stamps are used instead of Squid's "seconds-since-epoch" time-stamp format, and that a configured out-going proxy (as specified by "%...{rH}C") is logged:

```
[%{%d/%b/%Y:%H:%M:%S %z}t] %te}C %a %rd}C/%s %cs}C %m %ru}C %u %rH}C %rt}C
%as}C
```

Unknown or unsupported translog tokens are logged within the log file as the characters that made up the token. For example, `%{xy}C` is logged into the log file as `xy`. All characters outside of a token specification sequence are repeated verbatim within the log file.

Sanitizing Transaction Logs

Use the **sanitized** option to disguise the IP address of clients in the transaction log file. The default is that transaction logs are not sanitized. A sanitized transaction log disguises the network identity of a client by changing the IP address in the transaction logs to 0.0.0.0.

The **no** form of this command disables the sanitize feature. The **transaction-logs sanitize** command does not affect the client IP (`%a`) value associated with a custom log format string that is configured with the CLI (configured with the **transaction-logs format custom string** global configuration command in which the string is the quoted log format string that contains the custom log format). To hide the identity of the client IP in the custom log format, either hard code 0.0.0.0 in the custom log format string or exclude the `%a` token, which represents the client IP, from the format string.

Exporting Transaction Log Files

To facilitate the postprocessing of cache log files, you could export transaction logs to an external host.

This feature allows log files to be exported automatically by FTP to an external host at configurable intervals. The username and password used for FTP are configurable. The directory to which the log files are uploaded is also configurable.

The log files automatically have the following filename:

```
type_ipaddr_yyyymmdd_hhmmss.txt
```

where

- *type* represents the type of log file with *celog* for cache logs such as HTTP, HTTPS, and FTP, and *mms_export* for the WMT logs.
- *ipaddr* represents the SE IP address.
- *yyymmdd_hhmmss* represents the date and time when the log was archived for export.



Note

WMT logs have no .txt extension in the filename.

Exporting and Archiving Intervals

The transaction log archive and export functions are configured with the following commands:

- The **transaction-logs archive interval** global configuration command allows the administrator to specify when the *working.log* file is archived.
- The **transaction-logs export interval** global configuration command allows the administrator to specify when the archived transaction logs are exported.

The following limitations apply:

- When the interval is scheduled in units of hours, the value must divide evenly into 24. For example, the interval can be every 4 hours, but not every 5 hours.
- When the interval is scheduled in units of minutes, the value must divide evenly into 60.
- Only the more common choices of minutes are supported. For example, the interval can be 5 minutes or 10 minutes, but not 6 minutes.

- The selection of interval alignment is limited. If an interval is configured for every 4 hours, it will align with midnight. It cannot align with 12:30 or with 7 a.m.
- The feature does not support different intervals within a 24-hour period. For example, it does not support an interval that is hourly during regular business hours and then every 4 hours during the night.

Transaction Log Archive Filenaming Convention

The archive transaction log file is named as follows for HTTP and WMT caching:

```
celog_10.1.118.5_20001228_235959.txt
```

```
mms_export_10.1.118.5_20001228_235959
```

If the **export compress** feature is enabled when the file is exported, then the file extension will be **.gz** after the file is compressed for the export operation, as shown in the following example:

```
celog_10.1.118.5_20001228_235959.txt.gz
```

```
mms_export_10.1.118.5_20001228_235959.gz
```

[Table 2-82](#) describes the name elements.

Table 2-79 *Archive Log Name Element Descriptions*

Sample of Element	Description
acqdist_	Acquisition and distribution archive log file.
celog_	HTTP caching proxy server archive file.
cifs_server_	Windows file sharing server archive file.
cseaccess	Cisco Streaming Engine archive file.
icap_	ICAP server archive file.
mms_export_	Standard Windows Media Services 4.1 caching proxy server archive file.
mms_export_e_wms_41_	Extended Windows Media Services 4.1 caching proxy server archive file.
mms_export_wms_90_	Standard Windows Media Services 9.0 caching proxy server archive file.
mms_export_e_wms_90_	Extended Windows Media Services 9.0 caching proxy server archive file.
rproxyaccess.log.	RealProxy archive file.
rmsvraccess.log.	RealSubscriber archive file.
tftp_server_	TFTP server archive file.
tvout_	TV-out program archive file.
10.1.118.5_	IP address of the SE creating the archive file.
20001228_	Date on which the archive file was created (yyyy/mm/dd).
235959	Time when the archive file was created (hh/mm/ss).

[Table 2-80](#) lists the directory names and the corresponding examples of the archive filenames.

Table 2-80 *Archive Filename Examples and Directories*

Directory	Archive Filename
logs	celog_10.1.94.4_20050310_231500.txt
logs/export	mms_export_10.1.94.4_20050315_001545
logs/export/extended-wms-41	mms_export_e_wms_41_10.1.94.4_20050315_001545
logs/wms-90	mms_export_wms_90_10.1.94.4_20050315_001545
logs/export/extended-wms-90	mms_export_e_wms_90_10.1.94.4_20050315_001545
logs/acqdist	acqdist_10.1.94.4_20050315_001545
logs/cifs_server	cifs_server_10.1.94.4_20050315_001545
logs/cisco-streaming-engine	cseaccess10.1.94.4_050315000.log
logs/icap	icap_10.1.94.4_20050315_001545
logs/real-proxy	rproxyaccess.log.10.1.94.4_.20050315_001545
logs/real-subscriber	rmsvraccess.log.10.1.94.4_.20050315_001545
logs/tftp_server	tftp_server_10.1.94.4_20050315_001545
logs/tvout	tvout_10.1.94.4_20050315_001545

Compressing Archive Files

The **transaction-logs export compress** option compresses an archive into a gzip file format before exporting it. Compressing the archive file uses less disk space on both the SE and the FTP export server. The compressed file uses less bandwidth when transferred. The archive filename of the compressed file has the extension **.gz**.

Exporting Transaction Logs to External FTP Servers

The **transaction-logs export ftp-server** option can support up to four FTP servers. To export transaction logs, you must first enable the feature and configure the FTP server parameters. The following information is required for each target FTP server:

- FTP server IP address or the hostname
The SE translates the hostname with a DNS lookup and then stores the IP address in the configuration.
- FTP user login and user password
- Path of the directory where transferred files are written
Use a fully qualified path or a relative path for the user login. The user must have write permission to the directory.

Use the **no** form of the **transaction-logs export enable** command to disable the entire transaction logs feature while retaining the rest of the configuration.

Exporting Transaction Logs to External SFTP Servers

Use the **transaction-logs export sftp-server** option to export transaction logs. You must first enable the feature and configure the Secure File Transfer Protocol (SFTP) server parameters. The following information is required for each target SFTP server:

- SFTP server IP address or the hostname

The SE translates the hostname with a DNS lookup and then stores the IP address in the configuration.

- SFTP user login and user password
- Path of the directory where transferred files are written

Use a fully qualified path or a relative path for the user login. The user must have write permission to the directory.

Use the **no** form of the **transaction-logs export enable** command to disable the entire transaction logs feature while retaining the rest of the configuration.

Receiving a Permanent Error from the External FTP Server

A permanent error (Permanent Negative Completion Reply, RFC 959) occurs when the FTP command to the server cannot be accepted, and the action does not take place. Permanent errors can be caused by invalid user logins, invalid user passwords, and attempts to access directories with insufficient permissions.

When an FTP server returns a permanent error to the SE, the export is retried at 10-minute intervals or sooner if the configured export interval is sooner. If the error is a result of a misconfiguration of the **transaction-logs export ftp server** command, then you must re-enter the SE parameters to clear the error condition. The **show statistics transaction-logs** command displays the status of logging attempts to export servers.

The **show statistics transaction-logs** command shows that the SE failed to export archive files.

The **transaction-logs format** command has four options: **extended-squid**, **apache**, and **custom**.

Use the **no** form of the **transaction-logs export enable** command to disable the entire transaction logs feature while retaining the rest of the configuration.

Configuring Intervals Between 1 Hour and 1 Day

The archive or export interval can be set for once a day with a specific time stamp. It can also be set for hour frequencies that align with midnight. For example, every 4 hours means archiving occurs at 0000, 0400, 0800, 1200, and 1600. It is not possible to archive at half-hour intervals such as 0030, 0430, or 0830. The following intervals are acceptable: 1, 2, 3, 4, 6, 8, 12, and 24.

Configuring Intervals of 1 Hour or Less

The interval can be set for once an hour with a minute alignment. It can also be set for frequencies of less than an hour; these frequencies will align with the top of the hour. Every 5 minutes means that archiving will occur at 1700, 1705, and 1710.

Configuring Export Interval on Specific Days

The export interval can be set for specific days of the week at a specific time. One or more days can be specified. The default time is midnight.

You must be aware that archived logs are automatically deleted when free disk space is low. It is important to select an export interval that exports files frequently enough so that files are not automatically removed prior to export.

Monitoring HTTP Request Authentication Failures in Real Time

Cisco Internet Streamer Release 2.4 software supports sending HTTP transaction log messages to a remote syslog server so that you can monitor the remote syslog server for HTTP request authentication failures in real time. This real-time transaction log allows you to monitor transaction logs in real time for particular errors such as HTTP request authentication errors. The existing transaction logging to the local file system remains unchanged.

**Note**

Because system logging (syslog) occurs through UDP, the message transport to the remote syslog host is not reliable.

Examples

The following example shows how to configure an FTP server:

```
ServiceEngine(config)#transaction-logs export ftp-server 10.1.1.1 mylogin mypasswd
/ftpdirectory
```

```
ServiceEngine(config)#transaction-logs export ftp-server myhostname mylogin mypasswd
/ftpdirectory
```

The following example shows how to delete an FTP server:

```
ServiceEngine(config)#no transaction-logs export ftp-server 10.1.1.1
ServiceEngine(config)#no transaction-logs export ftp-server myhostname
```

Use the **no** form of the command to disable the entire transaction log export feature while retaining the rest of the configuration:

```
ServiceEngine(config)#no transaction-logs export enable
```

The following example shows how to change a username, password, or directory:

```
ServiceEngine(config)#transaction-logs export ftp-server 10.1.1.1 mynewname mynewpass
/newftpdirectory
```

**Note**

For security reasons, passwords are never displayed.

The following example shows how to restart the export of archive transaction logs:

```
ServiceEngine(config)# transaction-logs export ftp-server 172.16.10.5
goodlogin pass /ftpdirectory
```

The following example shows how to delete an SFTP server from the current configuration:

```
ServiceEngine(config)# no transaction-logs export sftp-server sftphostname
```

The following examples show how to configure the archiving intervals:

```
ServiceEngine(config)#transaction-logs archive interval every-day
at          Specify the time at which to archive each day
every       Specify the interval in hours. It will align with midnight
```

```
ServiceEngine(config)#transaction-logs archive interval every-day at
<0-23>: Time of day at which to archive (hh:mm)
```

```
ServiceEngine(config)#transaction-logs archive interval every-day every
<1-24> Interval in hours: {1, 2, 3, 4, 6, 8, 12 or 24}
```

The following example shows that the SE has failed to export archive files:

```
ServiceEngine#show statistics transaction-logs
Transaction Log Export Statistics:
```

```
Server:172.16.10.5
  Initial Attempts:1
  Initial Successes:0
  Initial Open Failures:0
  Initial Put Failures:0
  Retry Attempts:0
```

```
Retry Successes:0
Retry Open Failures:0
Retry Put Failures:0
Authentication Failures:1
Invalid Server Directory Failures:0
```

The following example shows how to correct a misconfiguration:

```
ServiceEngine(config)#transaction-logs export ftp-server 10.1.1.1 goodlogin pass
/ftpdirectory
```

The working.log file and archived log files are listed for HTTP and WMT.

The following example shows how to export transaction logs to an SFTP server:

```
ServiceEngine(config)#transaction-logs export sftp-server 10.1.1.100 mylogin mypasswd
/mydir
```

The following example shows how to archive every 4 hours and align with the midnight local time (0000, 0400, 0800, 1200, 1600, and 2000):

```
ServiceEngine(config)#transaction-logs archive interval every-day every 4
```

The following example shows how to export once a day at midnight local time:

```
ServiceEngine(config)#transaction-logs export interval every-day every 24
```

The following example shows how to configure export intervals:

```
ServiceEngine(config)#transaction-logs archive interval every-hour ?
at          Specify the time at which to archive each day
every       Specify interval in minutes. It will align with top of the hour

ServiceEngine(config)#transaction-logs archive interval every-hour at ?
<0-59>      Specify the minute alignment for the hourly archive
ServiceEngine(config)#transaction-logs archive interval every-hour every ?
<2-30>      Interval in minutes: {2, 5, 10, 15, 20, 30}
```

Related Commands

```
clear
show statistics transaction-logs
show transaction-logging
transaction-log force
```

type

To display the contents of a file, use the **type** EXEC command.

type *filename*

Syntax Description	<i>filename</i> Name of file.

Defaults	No default behavior or values.

Command Modes	EXEC

Usage Guidelines	Use this command to display the contents of a file within any SE file directory. This command may be used to monitor features such as transaction logging or system logging (syslog).

Examples	The following example displays the syslog file on the SE:

```
ServiceEngine#type /local1/syslog.txt
```

```
Jan 10 22:02:46 (none) populate_ds: %SE-CLI-5-170050: Cisco Internet Streamer CDS Software
starts booting
Jan 10 22:02:47 (none) create_etc_hosts.sh: %SE-CLI-5-170051: HOSTPLUSDOMAIN: NO-HOSTNAME
Jan 10 22:02:47 NO-HOSTNAME : %SE-CLI-5-170053: Recreated etc_hosts (1, 0)
Jan 10 22:02:48 NO-HOSTNAME Nodemgr: %SE-NODEMGR-5-330082: [CLI_VER_NTP] requests stop
service ntpd
Jan 10 22:02:49 NO-HOSTNAME Nodemgr: %SE-NODEMGR-5-330082: [ver_tvout] requests stop
service tvoutsvr
Jan 10 22:02:50 NO-HOSTNAME Nodemgr: %SE-NODEMGR-5-330084: [ver_rtspg] requests restart
service rtspg
Jan 10 22:02:50 NO-HOSTNAME Nodemgr: %SE-NODEMGR-5-330082: [ver_iptv] requests stop
service sbss
Jan 10 22:02:51 NO-HOSTNAME Nodemgr: %SE-NODEMGR-5-330080: [ver_telnetd] requests start
service telnetd
Jan 10 22:02:52 NO-HOSTNAME Nodemgr: %SE-NODEMGR-5-330082: [ver_wmt] requests stop service
wmt_mms
Jan 10 22:02:53 NO-HOSTNAME Nodemgr: %SE-NODEMGR-5-330082: [ver_wmt] requests stop service
wmt_logd
Jan 10 22:02:55 NO-HOSTNAME Nodemgr: %SE-NODEMGR-5-330082: [Unknown] requests stop service
mcast_sender
Jan 10 22:02:55 NO-HOSTNAME Nodemgr: %SE-NODEMGR-5-330082: [Unknown] requests stop service
mcast_receiver
Jan 10 22:02:56 NO-HOSTNAME Nodemgr: %SE-NODEMGR-5-330024: Service 'populate_ds' exited
normally with code 0
Jan 10 22:02:56 NO-HOSTNAME Nodemgr: %SE-NODEMGR-5-330040: Start service 'parser_server'
using: '/ruby/bin/parser_server' with pid: 1753
Jan 10 22:02:56 NO-HOSTNAME Nodemgr: %SE-NODEMGR-5-330040: Start service
'syslog_bootup_msgs' using: '/ruby/bin/syslog_bootup_msgs' with pid:
1754
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SE-SYS-5-900001: <4>Linux version 2.4.16
(cnbuild@builder2.cisco.com) (gcc version 3.0.4) #1
SMP Fri Jan 7 19:26:58 PST 2005
```

```

Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SE-SYS-5-900001: <6>setup.c: handling
flash window at [15MB..16MB)
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SE-SYS-5-900001: <6>BIOS-provided
physical RAM map:
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SE-SYS-5-900001: <4> BIOS-e820:
0000000000000000 - 0000000000009ec00 (usable)
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SE-SYS-5-900001: <4> BIOS-e820:
0000000000009ec00 - 000000000000a0000 (reserved)
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SE-SYS-5-900001: <4> BIOS-e820:
000000000000e0800 - 00000000000100000 (reserved)
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SE-SYS-5-900001: <4> BIOS-e820:
00000000000100000 - 00000000000f00000 (usable)
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SE-SYS-5-900001: <4> BIOS-e820:
00000000000f00000 - 00000000001000000 (reserved)
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SE-SYS-5-900001: <4> BIOS-e820:
00000000001000000 - 00000000010000000 (usable)
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SE-SYS-5-900001: <4> BIOS-e820:
000000000fff00000 - 00000000100000000 (reserved)
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SE-SYS-5-900001: <6>setup.c: reserved
bootmem for INITRD_START = 0x6000000, INITRD_SIZE = 117
09348
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SE-SYS-5-900001: <4>On node 0 totalpages:
65536
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SE-SYS-5-900001: <4>zone(0): 4096 pages.
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SE-SYS-5-900001: <4>zone(1): 61440 pages.
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SE-SYS-5-900001: <4>zone(2): 0 pages.
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SE-SYS-5-900001: <4>Local APIC disabled
by BIOS -- reenabling.
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SE-SYS-5-900001: <4>Found and enabled
local APIC!
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SE-SYS-5-900001: <4>Kernel command line:
root=/dev/ram ramdisk_size=100000 ramdisk_start=0x60
00000 console=ttyS0,9600n8
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SE-SYS-5-900001: <6>Initializing CPU#0
--More--
.
.

```

Related Commands

cpfile
dir
lls
ls
mkfile

type-tail

To view a specified number of lines of the end of a log file or to view the end of the file continuously as new lines are added to the file, use the **type-tail** command in EXEC mode.

type-tail *filename* [*line* | **follow**]

Syntax Description

<i>filename</i>	File to be examined.
<i>line</i>	(Optional) The number of lines from the end of the file to be displayed (1–65535).
follow	(Optional) Displays the end of the file continuously as new lines are added to the file.

Defaults

Ten lines shown

Command Modes

EXEC

Usage Guidelines

This command allows you to monitor a log file by letting you view the end of the file. You can specify the number of lines at the end of the file that you want to view, or you can follow the last line of the file as it continues to log new information. To stop the last line from continuously scrolling, press **Ctrl-C**.

Examples

The following example shows the list of log files in the /local1 directory:

```
stream-ServiceEngine#ls /local1
WS441
Websense
WebsenseEnterprise
Websense_config_backup
WsInstallLog
badfile.txt
codecoverage
core.stunnel.5.3.0.b100.cnbuild.5381
core_dir
crash
crka.log
cse_live
cse_vod
dbdowngrade.log
dbupgrade.log
downgrade
errorlog
http_authmod.unstrip
index.html
logs
lost+found
netscape-401-proxy
netscape-401-proxy1
netscape-dump
newwebsense
oldWsInstallLog
preload_dir
proxy-basic1
```



```

proxy1
proxy2
proxy3
proxy4
proxy5
proxy6
proxy7
proxy8
proxyreply
proxyreply-407
real_vod
ruby.bin.cli_fix
ruby.bin.no_ws_fix
ruby.bin.ws_edir_fix
sa
service_logs
smartfilter
smfnaveen
superwebsense
syslog.txt
syslog.txt.1
syslog.txt.2
temp
two.txt
url.txt
urllist.txt
var
vpd.properties
websense.pre-200
webtarball44
webtarball520
wmt_vod
ws_upgrade.log

```

The following example displays the last ten lines of the syslog.txt file. In this example, the number of lines to display is not specified; however, ten lines is the default.

```

stream-ServiceEngine#type-tail /local1/syslog.txt
Oct  8 21:49:15 stream-ce syslog: (26830)TRCE:input_serv.c:83-> select_with
return 0, ready = 0
Oct  8 21:49:15 stream-ce syslog: (26832)TRCE:al_master.c:246-> select_with
return 0, ready = 0
Oct  8 21:49:15 stream-ce syslog: (26832)TRCE:in_mms.c:1747-> tv = NULL
Oct  8 21:49:17 stream-ce syslog: (26830)TRCE:input_serv.c:83-> select_with
return 0, ready = 0
Oct  8 21:49:17 stream-ce syslog: (26832)TRCE:al_master.c:246-> select_with
return 0, ready = 0
Oct  8 21:49:17 stream-ce syslog: (26832)TRCE:in_mms.c:1747-> tv = NULL
Oct  8 21:49:19 stream-ce syslog: (26830)TRCE:input_serv.c:83-> select_with
return 0, ready = 0
Oct  8 21:49:19 stream-ce syslog: (26832)TRCE:al_master.c:246-> select_with
return 0, ready = 0
Oct  8 21:49:19 stream-ce syslog: (26832)TRCE:in_mms.c:1747-> tv = NULL
Oct  8 21:49:21 stream-ce syslog: (26830)TRCE:input_serv.c:83-> select_with
return 0, ready = 0

```

The following example displays the last 20 lines of the syslog.txt file:

```

stream-ServiceEngine#type-tail /local1/syslog.txt 20
Oct  8 21:49:11 stream-ce syslog: (26832)TRCE:al_master.c:246-> select_with
return 0, ready = 0
Oct  8 21:49:11 stream-ce syslog: (26832)TRCE:in_mms.c:1747-> tv = NULL
Oct  8 21:49:13 stream-ce syslog: (26830)TRCE:input_serv.c:83-> select_with
return 0, ready = 0

```

```

Oct  8 21:49:13 stream-ce syslog:(26832)TRCE:al_master.c:246-> select_with
return 0, ready = 0
Oct  8 21:49:13 stream-ce syslog:(26832)TRCE:in_mms.c:1747-> tv = NULL
Oct  8 21:49:15 stream-ce syslog:(26830)TRCE:input_serv.c:83-> select_with
return 0, ready = 0
Oct  8 21:49:15 stream-ce syslog:(26832)TRCE:al_master.c:246-> select_with
return 0, ready = 0
Oct  8 21:49:15 stream-ce syslog:(26832)TRCE:in_mms.c:1747-> tv = NULL
Oct  8 21:49:17 stream-ce syslog:(26830)TRCE:input_serv.c:83-> select_with
return 0, ready = 0
Oct  8 21:49:17 stream-ce syslog:(26832)TRCE:al_master.c:246-> select_with
return 0, ready = 0
Oct  8 21:49:17 stream-ce syslog:(26832)TRCE:in_mms.c:1747-> tv = NULL
Oct  8 21:49:19 stream-ce syslog:(26830)TRCE:input_serv.c:83-> select_with
return 0, ready = 0
Oct  8 21:49:19 stream-ce syslog:(26832)TRCE:al_master.c:246-> select_with
return 0, ready = 0
Oct  8 21:49:19 stream-ce syslog:(26832)TRCE:in_mms.c:1747-> tv = NULL
Oct  8 21:49:21 stream-ce syslog:(26830)TRCE:input_serv.c:83-> select_with
return 0, ready = 0
Oct  8 21:49:21 stream-ce syslog:(26832)TRCE:al_master.c:246-> select_with
return 0, ready = 0
Oct  8 21:49:21 stream-ce syslog:(26832)TRCE:in_mms.c:1747-> tv = NULL
Oct  8 21:49:23 stream-ce syslog:(26830)TRCE:input_serv.c:83-> select_with
return 0, ready = 0
Oct  8 21:49:23 stream-ce syslog:(26832)TRCE:al_master.c:246-> select_with
return 0, ready = 0
Oct  8 21:49:23 stream-ce syslog:(26832)TRCE:in_mms.c:1747-> tv = NULL

```

The following example follows the file as it grows:

```

stream-ServiceEngine#type-tail /local1/syslog.txt ?
<1-65535> The numbers of lines from end
follow Follow the file as it grows
<cr>
stream-ServiceEngine#type-tail /local1/syslog.txt follow
Oct  8 21:49:39 stream-ce syslog:(26832)TRCE:in_mms.c:1747-> tv = NULL
Oct  8 21:49:41 stream-ce syslog:(26830)TRCE:input_serv.c:83-> select_with
return 0, ready = 0
Oct  8 21:49:41 stream-ce syslog:(26832)TRCE:al_master.c:246-> select_with
return 0, ready = 0
Oct  8 21:49:41 stream-ce syslog:(26832)TRCE:in_mms.c:1747-> tv = NULL
Oct  8 21:49:43 stream-ce syslog:(26830)TRCE:input_serv.c:83-> select_with
return 0, ready = 0
Oct  8 21:49:43 stream-ce syslog:(26832)TRCE:al_master.c:246-> select_with
return 0, ready = 0
Oct  8 21:49:43 stream-ce syslog:(26832)TRCE:in_mms.c:1747-> tv = NULL
Oct  8 21:49:45 stream-ce syslog:(26830)TRCE:input_serv.c:83-> select_with
return 0, ready = 0
Oct  8 21:49:45 stream-ce syslog:(26832)TRCE:al_master.c:246-> select_with
return 0, ready = 0
Oct  8 21:49:45 stream-ce syslog:(26832)TRCE:in_mms.c:1747-> tv = NULL
Oct  8 21:49:47 stream-ce syslog:(26830)TRCE:input_serv.c:83-> select_with
return 0, ready = 0
Oct  8 21:49:47 stream-ce syslog:(26832)TRCE:al_master.c:246-> select_with
return 0, ready = 0
Oct  8 21:49:47 stream-ce syslog:(26832)TRCE:in_mms.c:1747-> tv = NULL
Oct  8 21:49:49 stream-ce syslog:(26830)TRCE:input_serv.c:83-> select_with
return 0, ready = 0
Oct  8 21:49:49 stream-ce syslog:(26832)TRCE:al_master.c:246-> select_with
return 0, ready = 0
Oct  8 21:49:49 stream-ce syslog:(26832)TRCE:in_mms.c:1747-> tv = NULL

```

undebug

To disable debugging functions, use the **undebug** EXEC command.

undebug *option*

Syntax Description	This command has no arguments or keywords.

Defaults	No default behavior or values.

Command Modes	EXEC

Usage Guidelines	We recommend that you use the debug and undebug commands only at the direction of Cisco TAC. See the “debug” section on page 2-70 for more information about debug functions.

Related Commands	debug no debug show debugging

url-signature

The CDS uses a combination of key owners, key ID numbers, and a word value to generate URL signature keys. To configure the url signature, use the **url-signature** global configuration command.

url-signature key-id-owner *num* **key-id-number** *num* {**key** *word* | **public key** *url* [**symmetric key** *word* | **private key** *url*]}

no url-signature key-id-owner *num* **key-id-number** *num*

Syntax Description

key-id-owner	Configures the owner ID for this key.
<i>num</i>	Specifies the ID for the owner of this key (1-32).
key-id-number	Configures the number ID for this key.
<i>num</i>	Specifies the ID for the number of this key (1-16).
key	Configures the encryption key for signing a URL.
<i>word</i>	Text of encryption key (16 characters maximum, no spaces).
public-key	Configures the Public Key file location (PEM).
<i>url</i>	The URL from where the Public Key file can be downloaded (54 characters maximum).
symmetric-key	(Optional) Configure the Symmetric Key.
<i>word</i>	The Symmetric Key (Must be 16 characters, no spaces).
private-Key	(Optional) Configures the Private Key file location (PEM).
<i>url</i>	The URL from where the Private Key file can be downloaded (54 characters maximum).

Command Modes

Global configuration

Usage Guidelines

Service Rules for Directing Requests to a Policy Server

If your network is configured to work with Camiant PCMM-compliant third-party policy servers for servicing requests that require guaranteed bandwidth, you can use the following rule patterns and rule actions to filter the requests and to direct them to the policy server. The rule patterns and rule actions also enable you to generate URL signatures in the response for a valid request for a Windows Media metafile (.asx file extension), Movie Streamer file, or Flash Media Streaming file, and to validate the URL signature on incoming requests to the SE. URL signature key authentication is implemented by using the generate-url-signature and validate-url-signature rule actions that can be applied to specific rule patterns.



Note

Movie Streamer and Flash Media Streaming support URL signing. Flash Media Streaming only supports the following actions: allow, block, and validate-url-signature.

The following table lists the rule patterns that support the use-icap-service rule action for directing requests that require guaranteed bandwidth to the third-party policy server:

Rule Pattern	Description
url-regex	Filters the request based on any regular expression in the URL.
domain	Filters the request based on the domain name specified.
src-ip	Filters the request based on the IP address of the source.
header-field user-agent	Filters the request based on the user agent specified in the request header.
header-field referer	Filters the request based on the referer in the request header.
header-field request-line	Filters the request based on the request line in the request header.

You can set the use-icap-service rule action for any of the rule patterns above. If the request matches the parameters that you have set for the rule pattern, then the SE redirects the request to the third-party policy server using ICAP services. However, you must make sure that your network is configured to interoperate with the third-party policy server using ICAP services. You can set up the necessary ICAP configurations from the ICAP Services page. You can also use the rule pattern and rule action to generate URL signatures in the response for a valid request for a Windows Media metafile. You can use the following rule patterns to filter out requests for which you want to generate a URL signature key:

Rule Pattern	Description
url-regex	Filters the request based on any regular expression in the URL.
domain	Filters the request based on the domain name specified.

For the rule patterns mentioned above, you can set the following rule actions:

Rule Action	Description
generate-url-signature	Generates the URL signatures in the Windows Media metafile response associated with pre-positioned content, based on the SE configuration for the URL signature and this rule action.
validate-url-signature	Validates the URL signature for a request by using the configuration on your SE for the URL signature and allows the request processing to proceed for this request.



Note

When configuring service rules, you must configure the same service rules on all SEs participating in a delivery service in order for the service rules to be fully implemented. The rule action must be common for all client requests because the SR may redirect a client request to any SE in a delivery service depending on threshold conditions.

URL Signing Components

However, because any of these strings in the URL could potentially be edited manually and circumvented by any knowledgeable user, it is important to generate and attach a signature to the URL. This can be achieved by attaching a keyed hash to the URL, using a secret key shared only between the signer (the portal) and the validating component (CDS).

The URL signing script offers three different versions:

- MD5 hash algorithm
- SHA-1 hash algorithm
- SHA-1 hash algorithm with the protocol removed from the beginning of the URL

When a URL is signed for RTSP and a player does a fallback to HTTP for the same URL, the validation fails because the URL signature includes RTSP. If the URL signature does not include the protocol, the fallback URL is validated correctly even though the protocol is HTTP.

If you do not specify a version for the script, MD5 is used and the SIGV string in the script is not added.

At the portal, URLs can be signed for a particular user (client IP address) and expiry time using a URL signing script. The URL signing script example included in this section requires Python 2.3.4 or higher.

Following is an example of the URL signing script using the MD5 security hash algorithm:

```
python cds-ims-urlsign.py http://www.cisco.com/index.html 8.1.0.4 200000 1 2 cisco
```

An example of the resulting signed URL follows:

```
http://www.cisco.com/index.html?IS=0&ET=1241194518&CIP=8.1.0.4&KO=1&KN=2&US=deebacde45bf716071c8b2fecaa755b9
```

If you specify version 1 for the script, SHA-1 is used and the SIGV=1 string is added.

Following is an example of the URL signing script using the SHA-1 security hash algorithm:

```
python cds-ims-urlsign.py http://www.cisco.com/index.html 8.1.0.4 200000 1 2 cisco 1
```

An example of the resulting signed URL follows:

```
http://www.cisco.com/index.html?SIGV=1&IS=0&ET=1241194679&CIP=8.1.0.4&KO=1&KN=2&US=8349348ffac7987d11203122a98e7e64e410fa18
```

If you specify version 2 for the script, SHA-1 is used. The protocol from the beginning of the URL is also removed before the signature is generated, and the SIGV=2 string is added. The protocol is RTSP, HTTP, or RTMP. The URL is signed without the protocol, but the final signed URL is printed with the protocol.

Following is an example of the URL signing script using the SHA-1 security hash algorithm with version 2 specified:

```
python cds-ims-urlsign.py http://www.cisco.com/index.html 8.1.0.4 200000 1 2 cisco 2
```

An example of the resulting signed URL follows:

```
http://www.cisco.com/index.html?SIGV=2&IS=0&ET=1241194783&CIP=8.1.0.4&KO=1&KN=2&US=68b5f5ed97d1255a0ec42a42a4f779e794df679c
```

For additional information on URL Signing, see the “Configuring URL Signing” section and the “URL Signing and Validation” appendix in the *Cisco Internet Streamer CDS 2.4 Software Configuration Guide*.

Examples

Following is an example of generating and encrypting the public key and private key using the **url-signature** command:

```
ServiceEngine(config)#url-signature key-id-owner 1 key-id-number 10 public-key
http://1.1.1.1/ec_pub_key private-key http://1.1.1.1/ec_pub_key symmetric-key
```

Following is an example of the URL signing script using the MD5 security hash algorithm:

```
python cds-ims-urlsign.py http://www.cisco.com/index.html 8.1.0.4 200000 1 2 cisco
```

An example of the resulting signed URL follows:

```
http://www.cisco.com/index.html?IS=0&ET=1241194518&CIP=8.1.0.4&KO=1&KN=2&US=deebacde45bf716071c8b2fecaa755b9
```

If you specify version 1 for the script, SHA-1 is used and the SIGV=1 string is added.

Following is an example of the URL signing script using the SHA-1 security hash algorithm:

```
python cds-ims-urlsign.py http://www.cisco.com/index.html 8.1.0.4 200000 1 2 cisco 1
```

An example of the resulting signed URL follows:

```
http://www.cisco.com/index.html?SIGV=1&IS=0&ET=1241194679&CIP=8.1.0.4&KO=1&KN=2&US=8349348ffac7987d11203122a98e7e64e410fa18
```

If you specify version 2 for the script, SHA-1 is used. The protocol from the beginning of the URL is also removed before the signature is generated, and the SIGV=2 string is added. The protocol is RTSP, HTTP, or RTMP. The URL is signed without the protocol, but the final signed URL is printed with the protocol.

Following is an example of the URL signing script using the SHA-1 security hash algorithm with version 2 specified:

```
python cds-ims-urlsign.py http://www.cisco.com/index.html 8.1.0.4 200000 1 2 cisco 2
```

An example of the resulting signed URL follows:

```
http://www.cisco.com/index.html?SIGV=2&IS=0&ET=1241194783&CIP=8.1.0.4&KO=1&KN=2&US=68b5f5ed97d1255a0ec42a42a4f779e794df679c
```

username

To establish username authentication, use the **username** global configuration command.

username *name* { **cifs-password** | **samba-password** } { **0** *plainword* | **1** *lancrypto ncrypto* | *cleartext* } | **password** { **0** *plainword* | **1** *cryptoword* | *cleartext* } [**uid** *uid*] | **privilege** { **0** | **15** }

no username *name*

Syntax Description

<i>name</i>	Username.
cifs-password	Sets the Windows user password.
samba-password	Deprecated, same as cifs-password .
0	Specifies a clear-text password. This is the default password setting.
<i>plainword</i>	Clear-text user password.
1	Specifies a type 1 encrypted password.
<i>lancrypto</i>	Encrypted password for LAN Manager networks.
<i>ncrypto</i>	Encrypted password for Windows NT networks.
<i>cleartext</i>	Unencrypted (clear-text) password for Windows NT networks.
password	Sets the user password.
<i>cryptoword</i>	Encrypted user password.
uid	Sets the user ID for a clear-text password or an encrypted password.
<i>uid</i>	Encrypted password user ID (2001–65535).
privilege	Sets the user privilege level.
0	Sets the user privilege level for a normal user.
15	Sets the user privilege level for a superuser.

Defaults

The **password** value is set to 0 (clear text) by default.

Default administrator account:

- **Uid:** 0
- **Username:** admin
- **Password:** default
- **Privilege:** superuser (15)

Command Modes

Global configuration

Usage Guidelines

The **username** global configuration command changes the password and privilege level for existing user accounts.

User Authentication

User access is controlled at the authentication level. For every HTTP or HTTPS request that applies to the administrative interface, including every CLI and API request that arrives at the CDS network devices, the authentication level has visibility into the supplied username and password. Based on CLI-configured parameters, a decision is then made to either accept or reject the request. This decision is made either by checking local authentication or by performing a query against a remote authentication server. The authentication level is decoupled from the authorization level, and there is no concept of role or domain at the authentication level.

When local CLI authentication is used, all configured users can be displayed by entering the **show running-config** command. Normally, only administrative users need to have username authentication configured.



Note

Every CDS network device should have an administrative password that can override the default password.

User Authorization

Domains and roles are applied by the CDSM at the authorization level. Requests must be accepted by the authentication level before they are considered by the authorization level. The authorization level regulates the access to resources based on the CDSM GUI role and domain configuration.

Regardless of the authentication mechanism, all user authorization configuration is visible in the GUI.

Examples

When you first connect an CDS device to an CDS network, you should immediately change the password for the username *admin*, which has the password *default*, and the privilege level superuser.

The following example shows how to change the password:

```
ServiceEngine(config)#username admin password yoursecret
```

The following example shows how passwords and privilege levels are reconfigured:

```
ServiceEngine#show user username abeddoe
Uid          : 2003
Username     : abeddoe
Password     : ghQ.GyGhP96K6
Privilege    : normal user
ServiceEngine#show user username bwhidney
Uid          : 2002
Username     : bwhidney
Password     : bhlohIbIwAMOk
Privilege    : normal user
ServiceEngine(config)#username bwhidney password 1 victoria
ServiceEngine(config)#username abeddoe privilege 15
User's privilege changed to super user (=15)
ServiceEngine#show user username abeddoe
Uid          : 2003
Username     : abeddoe
Password     : ghQ.GyGhP96K6
Privilege    : super user

ServiceEngine#show user username bwhidney
Uid          : 2002
Username     : bwhidney
Password     : mhYwYw.7PlLd6
Privilege    : normal user
```

■ username

Related Commands

show user
show users

whoami

To display the username of the current user, use the **whoami** EXEC command.

whoami

Syntax Description	This command has no arguments or keywords.

Defaults	No default behavior or values.

Command Modes	EXEC

Usage Guidelines	Use this command to display the username of the current user.

Examples	The following example displays the username of the user who has logged in to the SE:

```
ServiceEngine#whoami  
admin
```

Related Commands	pwd

wmt

To configure Windows Media Technologies (WMT), use the **wmt** global configuration command. To negate these actions, use the **no** form of this command.

wmt accelerate {proxy-cache | vod} enable

wmt advanced client {maximum-packet-size *number* | idle-timeout *number*}

wmt advanced server {log-forwarding enable | inactivity-timeout *number*}

wmt cache {age-multiplier *number* | enable | max-obj-size *size* | max-ttl {days *number* | hours *number* | minutes *number* | seconds *number*} | min-ttl *number* | reval-each-request}

wmt disallowed-client-protocols {http [rtspt | rtspu] | rtspt [http | rtspu] | rtspu [http | rtspt]}

wmt enable

wmt fast-cache {enable | max-delivery-rate *number*}

wmt fast-start {enable | max-bandwidth *number*}

wmt http allow extension *file_extensions*

wmt max-concurrent-sessions *number*

wmt proxy outgoing {http | rtsp} host {hostname | ip-address} port

wmt transaction-logs format {extended {wms-41 | wms-90} | wms-41 | wms-90}

no wmt {accelerate {proxy-cache | vod} enable | advanced {client {maximum-packet-size *number* | idle-timeout} | server {log-forwarding | inactivity-timeout} enable} | cache {age-multiplier *number* | enable | max-obj-size *size* | max-ttl {days *number* | hours *number* | minutes *number* | seconds *number*} | min-ttl *number* | reval-each-request} | disallowed-client-protocols {http [rtspt | rtspu] | rtspt [http | rtspu] | rtspu [http | rtspt]} | enable | fast-cache {enable | max-delivery-rate *number*} | fast-start {enable | max-bandwidth *number*} | http allow extension *file_extensions* | max-concurrent-sessions | proxy outgoing {http | rtsp} | transaction-logs format {extended {wms-41 | wms-90} | wms-41 | wms-90}}

Syntax Description

accelerate	Configures the WMT streaming acceleration.
enable	Enables the performance improvement for live splitting.
proxy-cache	Configures the performance improvement for proxy caching.
enable	Enables the performance improvement for proxy caching.
vod	Sets the SE to accelerate the performance of the video on demand.
enable	Enables the performance improvement for the video on demand.
advanced	Configures WMT advanced settings.
client	Configures WMT advanced client features on the SE.
maximum-packet-size	Specifies the client maximum packet size (WMT maximum IP packet size), used in Virtual Private Network (VPN) environments.

<i>number</i>	Maximum packet size of WMT stream in bytes (512–2048).
idle-timeout	Specifies the maximum amount of time that the SE is to wait for a response from a WMT client before timing out the connection.
<i>number</i>	Timeout value in seconds (30–300).
server	Configures WMT advanced server features on the SE.
log-forwarding	Specifies whether the Windows Media transaction logs should be sent to the upstream WMT server or upstream SEs. This setting applies to all protocols, such as HTTP, RTSPT, and RTSPU.
inactivity-timeout	Specifies the server data channel inactivity timeout.
<i>number</i>	Server data channel inactivity timeout (60–65535).
cache	Configures the WMT cache.
age-multiplier	Specifies the WMT caching heuristic modifiers.
<i>number</i>	Expiration time as a percentage of their age (0–100).
enable	Enables the WMT media cache.
max-obj-size	Sets the maximum size of the object to be cached.
<i>size</i>	Object size in megabytes (1–1000000). The default is 1024 megabytes.
max-ttl	Specifies the maximum time to live for objects in the cache.
days	Specifies the maximum time to live units in days.
<i>number</i>	Maximum time to live (1–1825).
hours	Specifies the maximum time to live units in hours.
<i>number</i>	Maximum time to live (1–43800)
minutes	Specifies the maximum time to live units in minutes.
<i>number</i>	Maximum time to live (1–2628000).
seconds	Specifies the maximum time to live units in seconds.
<i>number</i>	Maximum time to live (1–157680000).
min-ttl	Specifies the minimum time to live for objects in the cache.
<i>number</i>	Minimum time to live (0–86400).
reval-each-request	Revalidates cache on every request.
disallowed-client-protocols	Specifies disallowed WMT client protocols.
http	Disallows streaming over the HTTP protocol (http://).
rtspt	Disallows streaming over the RTSPT protocol (rtspt://).
rtspu	Disallows streaming over the RTSPU protocol (rtspu://).
enable	Enables the WMT server.
fast-cache	Configures WMT Fast Cache. Fast Cache is supported for MMS-over-HTTP only.
enable	Enables WMT Fast Cache.
max-delivery-rate	Configures the maximum delivery rate allowed per media player when Fast Cache is used to serve packets to the media player.
<i>number</i>	Maximum delivery rate per player when Fast Cache is used to serve packets to the media player, expressed as a multiple of the normal delivery rate of a media stream (1–65535).
fast-start	Configures WMT Fast Start.

enable	Enables WMT Fast Start.
max-bandwidth	Configures the maximum burst bandwidth allowed per media player when Fast Start is used to serve packets to the media player.
<i>number</i>	Limit for maximum burst bandwidth allowed per player when Fast Start is used to serve packets to the media player. The default is 3500 kbps.
http	Sets HTTP configurations.
allow	Configures the HTTP filename extensions to be served.
extension	Sets the HTTP filename extensions to be served.
<i>file_extensions</i>	Filename extensions to be served. A maximum of 20 filename extensions is allowed, with a maximum of 10 characters per extension.
max-concurrent-sessions	Configures the maximum number of unicast clients that can be served concurrently.
<i>number</i>	Limit for incoming unicast requests; this limit is subject to physical resources on the platform (1–8000).
proxy	Configures a proxy.
outgoing	Configures an outgoing proxy.
http	Configures an outgoing HTTP proxy server for Windows Media requests.
rtsp	Configures an RTSP outgoing server for WMT RTSP requests from Windows Media 9 players.
host	Configures the host of an outgoing MMS-over-HTTP proxy.
<i>hostname</i>	Hostname of an outgoing proxy.
<i>ip-address</i>	IP address of an outgoing proxy.
<i>port</i>	Port number of an outgoing proxy (1–65535).
transaction-logs	Configures the logging format of the WMT transaction logs.
format	Sets the format for WMT transaction logs.
extended	Specifies the WMT-extended configuration for transaction logs. Enables username logging in the WMT transaction log.
wms-41	Sets the WMT to generate transaction logs in the extended Windows Media Services version 4.1 format.
wms-90	Sets the WMT to generate transaction logs in the extended Windows Media Services Version 9.0 format.
wms-41	Sets the WMT to generate transaction logs in the standard Windows Media Services Version 4.1 format.
wms-90	Sets the WMT to generate transaction logs in the standard Windows Media Services Version 9.0 format.

Defaults

wmt: disabled
advanced client maximum-packet-size: 1500 bytes
advanced client idle-timeout: 60 seconds
advanced server log-forwarding: enabled

wmt cache max-ttl days: 1 day
wmt cache max-ttl hours: 72 hours
wmt cache max-ttl minutes: 4320 minutes
wmt cache max-ttl seconds: 259200 seconds
wmt cache min-ttl: 60 minutes
wmt fast-cache: enabled
wmt fast-start: enabled
max-object-size: 1 GB
wmt http allow extension *file_extensions:* asf, none, nsc, wma, wmv

Command Modes Global configuration

Usage Guidelines The Windows Media Services (WMS) is the Microsoft streaming solution for creating, distributing, and playing back digital media files on the Internet. Windows Media Services 9 Series (WMS 9) is the new Windows Media solutions from Microsoft.

Enabling WMT on the Service Engine

Before enabling licenses for streaming media services on an SE, make sure that your SE clock and calendar settings are correct; otherwise, you will see an error message and the services will fail to install. Use the **show clock** EXEC command to display the system clock. To set the system clock, use the **clock set** EXEC command.

Enabling Conventional WMT Proxy Service

During conventional proxy caching, the user media player is pointed to the SE to access the streaming media. Before enabling conventional WMT proxy service, be sure you have fulfilled the following requirements:

- You have a Microsoft WMT license key.
- You have the IP address of the SE.

Enabling Fast Cache

Fast Cache allows streaming of content to the Windows Media Player's cache as fast as the network allows, reducing the likelihood of an interruption in play due to network problems. When used with the Windows Media Player 9 Series, Fast Cache provides a way to stream content to clients faster than the data rate specified by the stream format. For example, with Fast Cache enabled, the server can transmit a 128-kbps stream at 700 kbps. In Windows Media Player, the stream is still rendered at the specified data rate, but the media player can buffer a much larger portion of the content before rendering it. This buffering allows the client to handle variable network conditions without impacting the playback quality of on-demand content.

Enabling Fast Start

Fast Start helps reduce buffering time. Typically, Windows Media Player must buffer a certain amount of data before it can start rendering content. If the clients connecting to the SE are using Windows Media Player for Windows XP or a later version of Windows Media Player, Fast Start can be used to provide

data directly to the buffer at speeds higher than the bit rate of the content requested. This buffering enables users to start receiving content more quickly. After the initial buffer requirement has been fulfilled, on-demand content is streamed at the bit rate defined by the content stream.

**Note**

Fast Start is not available to the first client connecting to a live stream.

When Fast Start is enabled on the SE, the increased bandwidth that Fast Start initially uses to send data to the media players can overburden a network if many media players connect to the stream at the same time. To reduce the risk of network congestion, use the **wmt fast-start max-bandwidth** global configuration command to limit the amount of bandwidth that Fast Start can use to stream content to each media player.

Adding or Removing WMT HTTP Allowed Filename Extensions

SEs use a list of filename extensions to decide whether a type of media file should be served by WMT. Typically, SEs are shipped with a default list of filename extensions to be served by WMT.

The default list in the SE contains the following filename extensions:

- asf
- none
- nsc
- wma
- wmv

**Note**

The default list of filename extensions includes “none” to enable SEs to serve media files without file extensions, such as URLs of live encoders. The filename extension nsc is included in the list to enable SEs to multicast media files.

Use the **wmt http allow extension *file_extensions*** global configuration command to add new filename extensions to the list. Use the **no wmt http allow extension *file_extensions*** command to remove filename extensions from the list.

The following restrictions apply to adding new filename extensions to the list:

- You cannot have more than 20 extensions in the list of allowed filename extensions.
- Filename extensions must be alphanumeric, and the first character of every extension must be a letter.
- You cannot have more than ten characters in a filename extension.

WMT Unique Stream Key

Normally, a caching proxy uses the URL string as the content identifier, so that a cache hit occurs when the request URL matches the content URL. This process is often unreliable, because some websites use dynamically generated URLs, which create different URL strings for the same content. When the URL string is used as the content identifier in this case, the likelihood of a cache hit is reduced. The unique stream key produces an identifier that is based on domain name, file size, bit rate, and other content-specific properties. This identifier is almost always unique for a piece of content. Using the unique stream key feature increases the likelihood of a cache hit.

Configuring WMT Multicasting

An SE can receive and deliver WMT streaming content through IP multicast as described in the next few sections.

Unicast-in multicast-out multicast delivery enables you to distribute streaming media efficiently by allowing different devices on the IP multicast to receive a single stream of media content from the SE simultaneously. This delivery mechanism can save significant network bandwidth consumption, because a single stream is sent to many devices, rather than sending a single stream to a single device every time that this stream is requested. This multicast delivery feature is enabled by setting up a multicast address on the SE to which different devices, configured to receive the content from the same channel, can subscribe. The delivering device sends the content to the multicast address set up at the SE, from which it becomes available to all subscribed receiving devices.

Multicast-in multicast-out multicast receive enables you to receive multicast WMT streams delivered through IP multicasting and then relay them to end users through another delivery channel (unicast or multicast).

The two WMT multicast-out features combined enable you to receive and deliver WMT streaming media content through IP multicasting and to do conversions from multicast to unicast (and vice versa).

The multicast-in unicast-out scenario enables you to create a broadcasting publishing point to deliver an incoming stream live to requesting clients using multicast as the source of the streaming media.

WMT Multicast Logging

Use the **log** option to provide multicast statistics to multicast server administrators. These statistics include a multicast IP address, a port number, a start time, and a number of clients. When configuring this option, you can choose to provide either a local URL where the multicast logging statistics can be sent, or an external fully qualified server URL that can receive these statistics. The multicast logging URL option can point to the multicast server or to any web server that can process the posted information from the users who subscribed to the multicast address.

Configuring Multicast-In Multicast-Out

In this multicasting scenario, a description file *.nsc is created that is accessible through multicast-out to clients. This scenario is similar to the unicast-in multicast-out scenario except that the input source is multicast. The clients use this description file to subscribe to the multicast.

Configuring Multicast to SE and Multicast to Client

In the Internet Streamer CDS 2.4 release, Multicast to SE and Multicast to client options were added. The administrator can configure inter-SE multicast for live programs if the network is multicast enabled. If the network is not multicast enabled, the result is undefined and streaming may not work as expected. Therefore, this requires a special configuration on the Live Programs page to turn this feature on and off.

To enable multicast delivery to the SEs for a program, you must choose multicast as a delivery mechanism. Choose Services > Live Video > Live Programs > Live Streaming. The Live Stream Settings page is displayed. Check the Enable Multicast Delivery to SE check box and click Submit.

Configuring Multicast-In Unicast-Out

In this scenario, a unicast-out publishing point is created to deliver the incoming stream live to requesting clients.

Configuring Unicast-In Unicast-Out

Unicast-in unicast-out provides a point-to-point connection between the client and the SE. The advantage of unicasting when streaming media over a network is that only a single stream needs to be pulled over the network between the origin server and SE, but that stream can be delivered to multiple

clients in a nonmulticast environment. A server running Windows Media Services can provide a unicast video stream to multiple clients through a single stream delivered to the SE. Typically, unicast-in unicast-out is used to broadcast live events.

In this scenario, unicast-in unicast-out provides a point-to-point connection between the client and the SE. The SE makes a single connection to the media server. Multiple requests for the same stream can be split by the SE so that each client receives a distinct data stream directly from the SE, while the SE maintains its single stream connection to the media server.

You can configure unicast-in unicast-out using live splitting without any configuration. The SE acts as a proxy. When clients request the same unicast URL, the SE proxy automatically splits the stream from the source to the clients.

Configuring Outgoing WMT Proxy Servers

You can specify the external WMT server that the SE should use as its upstream WMT server. The SE contacts the specified outgoing proxy server upon a cache miss (if the SE does not have the requested WMT content already stored in its local cache).

Configuring WMT Transaction Logs

WMT transaction logs allow content providers to track what content customers viewed, how long they viewed it, and the quality of transmission. The Internet Streamer CDS software uses the enhanced logging support provided by Windows Media Services 9 Series in addition to the Windows Media Services Version 4.1 logging format.

The following transaction log formats are supported for WMT:

- Standard Windows Media Services 4.1
- Extended Windows Media Services 4.1
- Standard Windows Media Services 9.0
- Extended Windows Media Services 9.0



Note

For RTSP, when you choose the **Repeat** option from the Play menu in the Windows Media player to play media files continuously in a loop, an extra entry is logged in the transaction logs for each playback of the file. This situation occurs with the WMT RTSPU protocol due to the behavior of the Windows Media player.

The SE's transaction logging format for WMT streaming is consistent with that of the Windows Media Services and the World Wide Web Consortium (W3C)-compliant log format. A log line is written for every stream accessed by the client. The location of the log is not configurable. These logs can be exported using FTP. When transaction logging is enabled, daemons create a separate working.log file in /local1/logs/export for WMT transactions.

All client information in the transaction logs is sent to the origin server by default.

Log Formats Accepted by Windows Media Services 9

Windows Media Players connect to a Windows Media Server using the following protocols:

- Windows Media Players earlier than Version 9.0 (Windows Media 6 and 7 Players) use HTTP 1.0 or the MMS protocol.
- Windows Media 9 Players use HTTP 1.0, HTTP 1.1, and RTSP.

Depending on the version of the Windows Media Player, logs are sent in different formats, such as text, binary, or Extensible Markup Language (XML). See [Table 2-81](#).

Table 2-81 Log Formats Accepted by Windows Media Services 9

Protocol	Player and Distributor	Log Type
HTTP/1.0	Windows Media Player earlier than Version 9.0 (for example, Windows Media 6.4 or 7.0 Players) SE (caching and proxy server) is running Windows Media Services Version 9.0 and streaming from a WMT server that is running Windows Media Services 4.1	World Wide Web Consortium (W3C) standard space-delimited text log
MMS	Windows Media Player earlier than Version 9.0 (for example, Windows Media 6.4 or 7.0 Players)	Binary structure log
HTTP/1.1	Windows Media Player Version 9.0 Distribution server is running Windows Media Services 9.0 SE (caching and proxy server) is running Windows Media Services 9.0	XML structure log
RTSP	Windows Media Player Version 9.0 Distribution server is running Windows Media Services 9.0 SE (caching and proxy server) is running Windows Media Services 9.0	XML structure log

The posted XML log file from the Windows Media Player to the SE (Windows Media Server) can be parsed and saved to the normal WMT transaction logs that are stored on the SE.

To specify the format for the WMT transaction logs on SEs, use the **wmt transaction-logs format** global configuration command. By default, the standard Windows Media Services 4.1 logging format is used (no SE-specific details are logged).

When you use the extended format in Windows Media Services 4.1 and 9.0, the SE includes the following three additional fields in the transaction log:

- SE-action—cache hit, cache miss, VoD, or live create
- SE-bytes—number of bytes served by the SE in the case of a cache hit
- username (username of the person who made the WMT request when Microsoft Negotiate authentication, Microsoft Digest authentication, and basic authentication are used)

**Note**

Microsoft Negotiate authentication is an authentication method in which the WMS Negotiate Authentication plug-in is used to authenticate the client. This method of authentication uses the client's logon credentials. It uses the encrypted password and username that the user entered during the login process.

Microsoft Digest authentication is an authentication method in which an initial authentication of

the client is performed when the server receives the first challenge response from the client. After the server verifies that the client has not been authenticated yet, it accesses the services of a domain controller to perform the initial authentication of the client. When the initial authentication of the client is successfully completed, the server receives a Digest session key. The server caches the session key and uses it to authenticate subsequent requests for resources from the authenticated client.

If the SE is configured to use the extended format of WMT transaction logging and the extended WMT logging feature is enabled, then the SE logs usernames for any authenticated WMT requests. Usernames are logged for Negotiate, Digest, and basic authentication.

**Note**

Negotiate and Digest authentication is applicable for the HTTP protocol only.

By default, the extended WMT logging feature is disabled. If the extended logging format is enabled (using the **wmt transaction-logs format extended** global configuration command) but the extended WMT logging feature is disabled, the username field in the WMT transaction log will be empty.

**Note**

The SE logs usernames associated with authenticated WMT requests only when the extended logging formats (extended wms-41 and extended wms-90) are used.

WMT Multicast Logging

WMT logs are logged to a working log on the local disk in one of the following files, depending upon where the sysfs is mounted on the SE:

- The file named /local1/logs/export/working.log
- The file named /local2/logs/export/working.log

Forwarding WMT Logs to Upstream Servers

You can decide whether you want this SE to forward its WMT logs to the upstream server (a Windows Media server or another SE). By default, SEs forward their WMT logs to the upstream server. This feature applies to all of the supported protocols. To disable this feature and configure the SE to not forward its WMT logs to the upstream server, enter the **no wmt advanced server log-forwarding enable** global configuration command. To re-enable this feature, enter the **wmt advanced server log-forwarding enable** global configuration command.

Examples

The following example displays request statistics. In this example, the statistics reported are the total number of requests served, type of content (live or VoD), transport protocol, and source of content:

```
ServiceEngine#show statistics wmt requests
```

```
Unicast Requests Statistics
```

```
=====
```

```
Total unicast requests received: 0
```

```
-----
```

	Total	% of Total Unicast Requests
	-----	-----
Streaming Requests served:	0	0.00%
Mcast nsc file Request:	0	0.00%

```

Authenticate Requests:      0          0.00%
Requests error:            0          0.00%

                                Total          % of Total
                                Streaming Requests
-----

By Type of Content
-----
    Live content:          0          0.00%
    On-Demand Content:    0          0.00%

By Transport Protocol
-----
    HTTP:                 0          0.00%
    RTSPT:                0          0.00%
    RTSPU:                0          0.00%

By Source of Content
-----
    Local:                0          0.00%
    Remote HTTP:          0          0.00%
    Remote RTSP:          0          0.00%
    Multicast:            0          0.00%

CDN-Related WMT Requests
-----
    CDN Content Hits:      0          0.00%
    CDN Content Misses:    0          0.00%
    CDN Content Live:      0          0.00%
    CDN Content Errors:    0          0.00%

Fast Streaming related WMT Requests
-----
    Normal Speed:          0          0.00%
    Fast Start Only:       0          0.00%
    Fast Cache Only:       0          0.00%
    Fast Start and Fast Cache: 0          0.00%

                                Total          % of Total
                                Authenticated Requests
-----

By Type of Authentication
-----
    Negotiate:            0          0.00%
    Digest:               0          0.00%
    Basic:                0          0.00%

```

The following example displays the multicast logging statistics sent to the multicast server:

```

10.1.101.2 2003-05-11 13:39:21 - asfm://239.1.4.5:4000 0 30 1 200
{5DC90EEB-CEB1-467C-9F7A-BCF5EEDE3FF} 10.1.0.3055 en-US - - wmpplayer.exe 10.1.0.3055
Windows_2000 10.0.0.2195 Pentium 0 152543 65389 asfm UDP WINDOWS_MEDIA_AUDIO_V2
MICROSOFT_MPEG-4_VIDEO_CODEC_V3 http://172.16.192.91/cisco.nsc - 166245 - 176 0 0 0 0 0 01
0 100 239.1.4.5 - - -

```

The format of the example shown is as follows:

```

c-ip date time c-dns cs-uri-stem c-starttime x-duration c-rate c-status c-playerid
c-playerversion c-playerlanguage cs(User-Agent) cs(Referer) c-hostexe c-hostexever c-os
c-osversion c-cpu filelength filesize avgbandwidth protocol transport audiocodec
videocodec channelURL sc-bytes c-bytes s-pkts-sent c-pkts-received c-pkts-lost-client

```

```
c-pkts-lost-net c-pkts-lost-cont-net c-resendreqs c-pkts-recovered-ECC
c-pkts-recovered-resent c-buffercount c-totalbuffertime c-quality s-ip s-dns
s-totalclients s-cpu-util SE-action SE-bytes Username
```

Table 2-82 describes the fields shown in this example.

Table 2-82 wmt multicast logging Field Descriptions

Field	Description
c-ip	IP address of the client computer. A client that is not connected properly provides a client proxy server IP address, not the client IP address.
date	Date (according to Greenwich mean time) when an entry is generated in the log file.
time	Time (according to Greenwich mean time) when an entry is generated in the log file.
c-dns	Domain Name Server (DNS) name of the client computer.
cs-uri-stem	Name of the file that is playing: an .asf file for a unicast and an .asx file for a multicast.
c-starttime	Time stamp (in seconds) of the stream when an entry is generated in the log file.
x-duration	Length of time that a client played content before a client event (FF, REW, pause, stop, or jump to marker). A log entry is generated whenever one of these client events occur.
c-rate	Mode of Windows Media Player when the last command event was sent: 1 = Windows Media Player was paused or stopped during a play, fast-forward, rewind, or marker jump operation. -5 = Windows Media Player was rewound from a play, stop, or pause operation. 5 = Windows Media Player was fast-forwarded from a play, stop, or pause operation.
c-status	Codes that describe client status. Mapped to HTTP/1.1 and RTSP client status codes described in RFC 2068 and RFC 2326. Windows Media Services includes the extensible client status codes 480 (simultaneous client connections exceeded the maximum client limit of the server) and 483 (stream exceeded maximum file bit-rate limit of the server).
c-playerid	Globally unique identifier (GUID) of the player.
c-playerversion	Version number of the player.
c-playerlanguage	Language country code of the client computer.
cs(User-Agent)	Browser type used if Windows Media Player was embedded in a browser.
cs(Referer)	URL of the web page in which Windows Media Player was embedded (if it was embedded).
c-hostexe	Host application; for example, a web page in a browser (iexplore.exe), a Microsoft Visual Basic applet (vb.exe), or standalone Microsoft Windows Media Player (mplayer2.exe).
c-hostexever	Version number of the host application.
c-os	Operating system of the client computer.

Table 2-82 *wmt multicast logging Field Descriptions (continued)*

Field	Description
c-osversion	Operating system version number of the client computer.
c-cpu	CPU type of the client computer.
filelength	Length of the file (in seconds). This value is 0 for a live stream.
filesize	Size of the file (in bytes). This value is 0 for a live stream.
avgbandwidth	Average bandwidth (in bits per second) at which the client was connected to the server.
protocol	Protocol used to access the stream: HTTP, or ASFM (multicast protocol).
transport	Transport protocol used to deliver the stream (UDP, TCP, or UDP over IP multicast).
audiocodec	Audio codec used in the stream.
videocodec	Video codec used to encode the stream.
channelURL	URL to the .nsc file. A unicast client information log file records a hyphen (-) for this field.
sc-bytes	Bytes sent by the server to the client.
c-bytes	Number of bytes received by the client from the server. For unicast, the c-bytes value and sc-bytes value must be identical. If not, packet loss has occurred.
s-pkts-sent	Total number of packets sent by the server.
c-pkts-received	Number of packets from the server (s-pkts-sent) that are received correctly by the client on the first try.
c-pkts-lost-client	Number of packets lost during transmission from the server to the client and not recovered at the client layer through an error correction or at the network layer through User Datagram Protocol (UDP) resends.
c-pkts-lost-net	Number of packets lost on the network layer.
c-pkts-lost-cont-net	Maximum number of continuously lost packets on the network layer during a transmission from the server to the client.
c-resendreqs	Number of client requests to receive new packets. This field contains a value only if the client is using UDP resend.
c-pkts-recovered-ECC	Number of packets repaired and recovered on the client layer. Packets repaired and recovered at the client layer are equal to the difference between c-pkts-lost-net and c-pkts-lost-client.
c-pkts-recovered-resent	Number of packets recovered because they were resent using UDP.
c-buffercount	Number of times that the client buffered while playing the stream.
c-totalbuffertime	Time (in seconds) that the client used to buffer the stream. If the client buffers the stream more than once before a log entry is generated, c-totalbuffertime is the total amount of time that the client spent buffering the stream.

Table 2-82 *wmt multicast logging Field Descriptions (continued)*

Field	Description
c-quality	The percentage of packets that were received by the client, indicating the quality of the stream. If cPacketsRendered is all packets received by the client, including packets recovered by error correction and UDP resend (c-pkts-received + c-pkts-recovered-ECC + c-pkts-recovered-resent), then c-quality can be calculated as: $[\text{cPacketsRendered} / (\text{cPacketsRendered} + \text{c-pkts-lost-client})] * 100$.
s-ip	Server IP address.
s-dns	Server DNS.
s-totalclients	Clients connected to the server (but not necessarily receiving streams).
s-cpu-util	Average load on the server processor as a percentage (0–100%). If multiple processors exist, this value is the average for all processors.
SE-action	Action performed by the SE.
SE-bytes	Number of bytes received by the SE.
Username	Username required to access the streaming media retrieved by the WMT player.

The following example adds the filename extension mp3 to the list of filename extensions to be served by WMT:

```
ServiceEngine#wmt http allow extension mp3
```

The **show wmt http allow extension EXEC** command shows the filename extensions included in the list after you have added or deleted filename extensions.

The following example shows that the filename extension mp3 has been added to the list of file extensions:

```
ServiceEngine#show wmt http allow extension
```

```
WMT http extensions allowed :
asf mp3 none nsc wma wmv
```

The following example shows that an SE at a branch office is configured to send all its WMT cache miss traffic to a central SE at 172.16.30.30 through port 8080:

```
ServiceEngine(config)# wmt proxy outgoing http host 172.16.30.30 8080
```

The following example shows that an SE at a branch office is configured to send all its cache miss traffic to a central SE at 172.16.30.31 through port 1700:

```
ServiceEngine(config)# wmt proxy outgoing http host 172.16.30.31 1700
```

The following example sets the SE to generate WMT transaction logs in the extended Windows Media Services, Version 9.0 format:

```
ServiceEngine#wmt transaction-logs format extended wms-90
```

The following example enables the logging of usernames to the WMT transaction log:

```
ServiceEngine#wmt extended transaction-log enable
```

Related Commands

clear
show running-config
show tech-support
show statistics wmt
show wmt
wmt (EXEC mode)

write

To save startup configurations, use the **write** EXEC command.

write [erase | memory | terminal]

Syntax Description

erase	(Optional) Erases the startup configuration from NVRAM.
memory	(Optional) Writes the configuration to NVRAM. This setting is the default.
terminal	(Optional) Writes the configuration to a terminal session.

Defaults

The configuration is written to NVRAM by default.

Command Modes

EXEC

Usage Guidelines

Use this command to either save running configurations to NVRAM or erase memory configurations. Following a **write erase** command, no configuration is held in memory, and a prompt for configuration specifics occurs after you reboot the SE.

Use the **write terminal** command to display the current running configuration in the terminal session window. The equivalent command is **show running-config**.

The **write memory** command saves modified Websense configuration files (the eimserver.ini, config.xml, and websense.ini files and the Blockpages directory) across disk reconfiguration and Internet Streamer CDS software release upgrades.



Note

Clicking the **Save Changes** button from the Websense Enterprise Manager window does not save the Websense configuration modifications across device reboots. You need to use the **write memory** command to save the Websense configuration changes across reboots.

You must execute the **write memory** command in order to save the most recent configuration modifications, including websense.ini file modifications and Websense URL filtering configuration changes. The **write memory** command enables the changes made from the external Websense Manager GUI to be saved across disk reconfiguration and upgrades (which might erase disk content).

The Websense configurations from the last use of the **write memory** command are retained under the following situations:

- If the **write memory** command is not used before a reboot but after a disk reconfiguration or an Internet Streamer CDS software upgrade that erases disk content.
- If you are using the CLI and did not answer “yes” when asked if you wanted to save the configurations at the reload prompt.

However, if the **write memory** command has never been used before, then default configurations will be applied when the content in the /local1/WebsenseEnterprise/EIM directory on the SE is erased.

Examples

The following command saves the running configuration to NVRAM:

```
ServiceEngine#write memory
```

Related Commands

copy
show running-config

■ write



APPENDIX A

Acronyms

Table A-1 defines the acronyms and abbreviations that are used in this publication.

Table A-1 **List of Acronyms**

Acronym	Expansion
AAA	authentication, authorization, and accounting
ACL	access control list
ACPI	Advanced Configuration and Power Interface
API	application program interface
ARP	Address Resolution Protocol
AUP	acceptable use policy
BA	Behavior Aggregate
BIOS	basic input/output system
CAR	Committed Access Rate
CD	Carrier Detect
CDE	Content Delivery Engine
CDNFS	CDS network file system; also pre-positioned file system
CDS	Content Delivery System
CDSM	Content Delivery System Manager
CIFS	Common Internet File System
CLF	Common Log format
CLI	command-line interface
CMS	Centralized Management System
CoS	class of service
CSS	Content Services Switch
CTE	chunked transfer encoding
DC	domain controller
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DSCP	differentiated services code point

Table A-1 **List of Acronyms (continued)**

Acronym	Expansion
DSL	Digital Subscriber Line
ECN	Explicit Congestion Notification
EIM	employee Internet management
EULA	end user license agreement
FEC	forward error correction
FQDN	fully qualified domain name
FTP	File Transfer Protocol
GMT	Greenwich Mean Time
GRE	generic routing encapsulation
GUI	graphical user interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
IANA	Internet Assigned Numbers Authority
ICP	Internet Cache Protocol
ICAP	Internet Content Adaptation Protocol
ICMP	Internet Control Message Protocol
IDE	Integrated Drive Electronics
IFP	Internet Filtering Protocol
IPV6	Internet Protocol Version 6
IIS	Internet Information Services or Internet Information Server (Microsoft)
IMS	if-modified-since
LDAP	Lightweight Directory Access Protocol
LCM	local/central management
LRU	least-recently-used
MAC	Media Access Control
MIB	Management Information Base
MOTD	message-of-the-day
MSFC	Multilayer Switch Feature Card
MTU	maximum transmission unit
NACK	negative acknowledgement
NAS	network attached storage; network access server
NAT	Network Address Translation
NFS	Network File System
NIC	Network Information Center
NNTP	Network News Transport Protocol
NTP	Network Time Protocol

Table A-1 **List of Acronyms (continued)**

Acronym	Expansion
NTSC	National Television Systems Committee
NVRAM	nonvolatile random-access memory
PAC	proxy autoconfiguration
PAL	Phase Alternating Line
PAWS	Protection Against Wrapped Sequence
PBR	policy-based routing
PDC	primary domain controller
PEM	Privacy Enhanced Mail
PFC	Policy Feature Card
PGM	Pragmatic General Multicast
PHB	Per Hop Behavior
PID	process identifier
PKCS	Public Key Cryptography Standards
PPP	Point-to-Point Protocol
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RBCP	Router Blade Configuration Protocol
RCP	Remote Copy Program
REA	remote execution agent
RPC	remote procedure call
RSA	Rivest, Shamir, Adelman
RSVP	Resource Reservation Protocol
RTP	Real-Time Transport Protocol
RTSP	Real-Time Streaming Protocol
SAN	Storage Area Network
SASL	Secure Authentication and Security Layer
SATA	Serial Advanced Technology Attachment
SCSI	Small Computer Systems Interface
SDP	Session Description Protocol
SE	Service Engine
SE-NM	Service Engine Network Module
SFTP	Secure File Transfer Protocol
SLA	service level agreement
SLIP	Serial Line Internet Protocol
SMART	Self Monitoring, Analysis, and Reporting Technology
SMB	Server Message Blocks (protocol)

Table A-1 **List of Acronyms (continued)**

Acronym	Expansion
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SPE	Synchronous Payload Envelope
SR	Service Router
SRAM	static random-access memory
SSH	Secure Shell
SSL	Secure Sockets Layer
swfs	software file system
sysfs	system file system
TAC	Technical Assistance Center
TACACS+	Terminal Access Controller Access Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial File Transfer Protocol
ToS	Type of Service
TPS	transactions per second
UDI	unique device identifier
UDP	User Datagram Protocol
UNC	uniform naming convention
UNS	unified name space
UTC	Coordinated Universal Time
VBR	variable bit rate
VOD	video on demand
W3C	World Wide Web Consortium
WFQ	Weighted Fair Queueing
WMS 9	Windows Media Services 9 Series
WMT	Windows Media Technologies
WRED	Weighted Random Early Detection
XML	Extensible Markup Language



APPENDIX B

Standard Time Zones

[Table B-1](#) lists all the standard time zones that you can configure on a CDE and the offset from Coordinated Universal Time (UTC) for each standard time zone. The offset (ahead or behind) UTC in hours, as displayed in [Table B-1](#), is in effect during winter time. During summer time or daylight saving time, the offset may be different from the values in the table and are calculated and displayed accordingly by the system clock.



Note

The time zone entry is case sensitive and must be specified in the exact notation listed in the following time zone table. When you use a time zone entry from the following time zone table, the system is automatically adjusted for daylight saving time.

Table B-1 *List of Standard Time Zones and Offsets from UTC*

Time Zone	Offset from UTC
Africa/Abidjan	0
Africa/Accra	0
Africa/Addis_Ababa	+3
Africa/Algiers	+1
Africa/Asmera	+3
Africa/Bamako	0
Africa/Bangui	+1
Africa/Banjul	0
Africa/Bissau	0
Africa/Blantyre	+2
Africa/Brazzaville	+1
Africa/Bujumbura	+2
Africa/Cairo	+2
Africa/Casablanca	0
Africa/Ceuta	+1
Africa/Conakry	0
Africa/Dakar	0
Africa/Dar_es_Salaam	+3

Table B-1 *List of Standard Time Zones and Offsets from UTC (continued)*

Time Zone	Offset from UTC
Africa/Djibouti	+3
Africa/Douala	+3
Africa/El_Aaiun	+1
Africa/Freetown	0
Africa/Gaborone	+2
Africa/Harare	+2
Africa/Johannesburg	+2
Africa/Kampala	+3
Africa/Khartoum	+3
Africa/Kigali	+2
Africa/Kinshasa	+1
Africa/Lagos	+1
Africa/Libreville	+1
Africa/Lome	0
Africa/Luanda	+1
Africa/Lubumbashi	+2
Africa/Lusaka	+2
Africa/Malabo	+1
Africa/Maputo	+2
Africa/Maseru	+2
Africa/Mbabane	+2
Africa/Mogadishu	+3
Africa/Monrovia	0
Africa/Nairobi	+3
Africa/Ndjamena	+1
Africa/Niamey	+1
Africa/Nouakchott	0
Africa/Ouagadougou	0
Africa/Porto-Novo	+1
Africa/Sao_Tome	0
Africa/Timbuktu	0
Africa/Tripoli	+2
Africa/Tunis	+1
Africa/Windhoek	+1
America/Anguilla	-4
America/Antigua	-4

Table B-1 *List of Standard Time Zones and Offsets from UTC (continued)*

Time Zone	Offset from UTC
America/Araguaina	−3
America/Aruba	−4
America/Asuncion	−4
America/Barbados	−4
America/Belem	−3
America/Belize	−6
America/Boa_Vista	−4
America/Bogota	−5
America/Boise	−7
America/Buenos_Aires	−3
America/Cambridge_Bay	−7
America/Cancun	−6
America/Caracas	−4
America/Catamarca	−3
America/Cayenne	−3
America/Cayman	−5
America/Chihuahua	−7
America/Cordoba	−3
America/Costa_Rica	−6
America/Cuiaba	−4
America/Curacao	−4
America/Dawson	−8
America/Dawson_Creek	−7
America/Dominica	−4
America/Eirunepe	−5
America/El_Salvador	−6
America/Fortaleza	−3
America/Glace_Bay	−4
America/Godthab	−3
America/Goose_Bay	−4
America/Grand_Turk	−5
America/Grenada	−4
America/Guadeloupe	−4
America/Guatemala	−6
America/Guayaquil	−5
America/Guyana	−4

Table B-1 *List of Standard Time Zones and Offsets from UTC (continued)*

Time Zone	Offset from UTC
America/Hermosillo	-7
America/Indiana/Marengo	-5
America/Indiana/Vevay	-5
America/Indiana/Indianapolis	-5
America/Indiana/Knox	-5
America/Inuvik	-7
America/Iqaluit	-5
America/Jujuy	-3
America/Juneau	-9
America/Kentucky/Monticello	-5
America/Kentucky/Louisville	-5
America/La_Paz	-4
America/Lima	-5
America/Louisville	-8
America/Maceio	-3
America/Managua	-6
America/Martinique	-4
America/Mendoza	-3
America/Menominee	-6
America/Merida	-6
America/Miquelon	-3
America/Monterrey	-6
America/Montevideo	-3
America/Montserrat	-4
America/Nassau	-5
America/Nipigon	-5
America/Nome	-9
America/Panama	-5
America/Pangnirtung	-3
America/Paramaribo	-3
America/Port-au-Prince	-5
America/Port_of_Spain	-4
America/Porto_Velho	-4
America/Rainy_River	-6
America/Rankin_Inlet	-6
America/Recife	-3

Table B-1 *List of Standard Time Zones and Offsets from UTC (continued)*

Time Zone	Offset from UTC
America/Rosario	−3
America/Santo_Domingo	−4
America/Scoresbysund	−1
America/St_Kitts	−4
America/St_Lucia	−4
America/St_Vincent	−4
America/Swift_Current	−6
America/Tegucigalpa	−6
America/Thule	−4
America/Thunder_Bay	−5
America/Tortola	−4
America/Virgin	−4
America/St_Thomas	−4
America/Yakutat	−9
America/Yellowknife	−7
America/Porto_Acre	−5
America/Rio_Branco	−5
America/Noronha	−2
America/Sao_Paulo	−3
America/Manaus	−4
America/Winnipeg	−6
America/Montreal	−5
America/Edmonton	−7
America/St_Johns	−3.30
America/Vancouver	−8
America/Whitehorse	−8
America/Santiago	−4
America/Havana	−5
America/Jamaica	−5
America/Ensenada	−8
America/Tijuana	−8
America/Mazatlan	−7
America/Mexico_City	−6
America/Puerto_Rico	−4
America/Halifax	−4
America/Regina	−6

Table B-1 *List of Standard Time Zones and Offsets from UTC (continued)*

Time Zone	Offset from UTC
America/Anchorage	−9
America/Adak	−10
America/Atka	−10
America/Phoenix	−7
America/Chicago	−6
America/Fort_Wayne	−5
America/Indianapolis	−5
America/Knox_IN	−5
America/Detroit	−7
America/Denver	−5
America/Shiprock	−7
America/Los_Angeles	−8
America/New_York	−5
Antarctica/Casey	+8
Antarctica/Davis	+7
Antarctica/DumontDUrville	+10
Antarctica/Mawson	+6
Antarctica/Palmer	−4
Antarctica/South_Pole	+12
Antarctica/McMurdo	+12
Antarctica/Syowa	+3
Antarctica/Vostok	+6
Arctic/Longyearbyen	+1
Asia/Aden	+3
Asia/Almaty	+6
Asia/Amman	+2
Asia/Anadyr	+12
Asia/Aqtau	+4
Asia/Aqtobe	+5
Asia/Ashkhabad	+5
Asia/Ashgabat	+5
Asia/Baghdad	+3
Asia/Bahrain	+3
Asia/Baku	+4
Asia/Bangkok	+7
Asia/Beirut	+2

Table B-1 *List of Standard Time Zones and Offsets from UTC (continued)*

Time Zone	Offset from UTC
Asia/Bishkek	+5
Asia/Brunei	+8
Asia/Calcutta	+5.30
Asia/Chungking	+8
Asia/Colombo	+6
Asia/Damascus	+2
Asia/Dhaka	+6
Asia/Dacca	+6
Asia/Dili	+9
Asia/Dubai	+4
Asia/Dushanbe	+5
Asia/Gaza	+2
Asia/Harbin	+8
Asia/Hovd	+7
Asia/Irkutsk	+8
Asia/Jakarta	+7
Asia/Jayapura	+9
Asia/Kabul	+4.30
Asia/Kamchatka	+12
Asia/Karachi	+5
Asia/Kashgar	+8
Asia/Katmandu	+5.45
Asia/Krasnoyarsk	+7
Asia/Kuala_Lumpur	+8
Asia/Kuching	+8
Asia/Kuwait	+3
Asia/Macao	+8
Asia/Magadan	+11
Asia/Manila	+8
Asia/Muscat	+4
Asia/Novosibirsk	+6
Asia/Omsk	+6
Asia/Phnom_Penh	+7
Asia/Pontianak	+7
Asia/Pyongyang	+9
Asia/Qatar	+3

Table B-1 *List of Standard Time Zones and Offsets from UTC (continued)*

Time Zone	Offset from UTC
Asia/Rangoon	+6.30
Asia/Riyadh	+3
Asia/Saigon	+7
Asia/Samarkand	+5
Asia/Tashkent	+5
Asia/Tbilisi	+3
Asia/Thimphu	+6
Asia/Thimbu	+6
Asia/Ujung_Pandang	+8
Asia/Ulan_Bator	+8
Asia/Ulaanbaatar	+8
Asia/Urumqi	+8
Asia/Vientiane	+7
Asia/Vladivostok	+10
Asia/Yakutsk	+9
Asia/Yekaterinburg	+5
Asia/Yerevan	+4
Asia/Nicosia	+2
Asia/Hong_Kong	+8
Asia/Tehran	+3.30
Asia/Jerusalem	+2
Asia/Tel_Aviv	+2
Asia/Tokyo	+9
Asia/Riyadh87	+3.07
Asia/Riyadh88	+3.07
Asia/Riyadh89	+3.07
Asia/Shanghai	+8
Asia/Taipei	+8
Asia/Seoul	+9
Asia/Singapore	+8
Asia/Istanbul	+2
Atlantic/Azores	-1
Atlantic/Bermuda	-4
Atlantic/Canary	0
Atlantic/Cape_Verde	-1
Atlantic/Faeroe	0

Table B-1 *List of Standard Time Zones and Offsets from UTC (continued)*

Time Zone	Offset from UTC
Atlantic/Madeira	0
Atlantic/South_Georgia	−2
Atlantic/St_Helena	0
Atlantic/Stanley	−4
Atlantic/Jan_Mayen	+1
Atlantic/Reykjavik	0
Australia/Lindeman	+10
Australia/Lord_Howe	+10.30
Australia/LHI	+10.30
Australia/North	+9.30
Australia/Darwin	+9.30
Australia/Queensland	+10
Australia/Brisbane	+10
Australia/South	+9.30
Australia/Adelaide	+9.30
Australia/Sydney	+10
Australia/ACT	+10
Australia/Canberra	+10
Australia/NSW	+10
Australia/Tasmania	+10
Australia/Hobart	+10
Australia/Victoria	+10
Australia/Melbourne	+10
Australia/West	+8
Australia/Perth	+8
Australia/Yancowinna	+9.30
Australia/Broken_Hill	+9.30
Brazil/Acre	−5
Brazil/DeNoronha	−2
Brazil/East	−3
Brazil/West	−4
CET	+1
Canada/Central	−6
Canada/Eastern	−5
Canada/Mountain	−7
Canada/Newfoundland	−3.30

Table B-1 *List of Standard Time Zones and Offsets from UTC (continued)*

Time Zone	Offset from UTC
Canada/Pacific	−8
Canada/Yukon	−8
Canada/Atlantic	−4
Canada/East-Saskatchewan	−6
Canada/Saskatchewan	−6
Chile/Continental	−4
Chile/EasterIsland	−6
Cuba	−5
EET	+2
Egypt	+2
Europe/Amsterdam	+1
Europe/Andorra	+1
Europe/Athens	+2
Europe/Belfast	0
Europe/Berlin	+1
Europe/Brussels	+1
Europe/Bucharest	+2
Europe/Budapest	+1
Europe/Copenhagen	+1
Europe/Dublin	0
Europe/Gibraltar	0
Europe/Helsinki	+2
Europe/Kaliningrad	+2
Europe/Kiev	+2
Europe/Luxembourg	+1
Europe/Madrid	+1
Europe/Malta	+1
Europe/Minsk	+2
Europe/Monaco	+1
Europe/Nicosia	+2
Europe/Oslo	+1
Europe/Paris	+1
Europe/Prague	+1
Europe/Bratislava	+1
Europe/Riga	+2
Europe/Samara	+4

Table B-1 *List of Standard Time Zones and Offsets from UTC (continued)*

Time Zone	Offset from UTC
Europe/Simferopol	+2
Europe/Sofia	+2
Europe/Stockholm	+1
Europe/Tallinn	+2
Europe/Tirane	+1
Europe/Tiraspol	+2
Europe/Chisinau	+2
Europe/Uzhgorod	+2
Europe/Vaduz	+1
Europe/Vatican	+1
Eire	0
GB-Eire	0
GB	0
Greenwich	0
GMT	0
GMT+0	0
GMT-0	0
GMT0	0
Hongkong	+8
Iceland	0
Indian/Antananarivo	+3
Indian/Chagos	+6
Indian/Christmas	+7
Indian/Cocos	+6.30
Indian/Comoro	+3
Indian/Kerguelen	+5
Indian/Mahe	+4
Indian/Maldives	+5
Indian/Mauritius	+4
Indian/Mayotte	+3
Indian/Reunion	+4
Iran	+3.30
Israel	+2
Jamaica	-5
Japan	+9
Libya	+2

Table B-1 *List of Standard Time Zones and Offsets from UTC (continued)*

Time Zone	Offset from UTC
MET	+1
Mexico/BajaNorte	−8
Mexico/BajaSur	−7
Mexico/General	−6
Mideast/Riyadh87	+3.07
Mideast/Riyadh88	+3.07
Mideast/Riyadh89	+3.07
PRC	+8
Pacific/Apia	−11
Pacific/Auckland	+12
Pacific/Chatham	+12.45
Pacific/Easter	−6
Pacific/Efate	+11
Pacific/Enderbury	+13
Pacific/Fakaofu	−10
Pacific/Fiji	+12
Pacific/Funafuti	+12
Pacific/Galapagos	−6
Pacific/Guadalcanal	+11
Pacific/Guam	+10
Pacific/Johnston	−10
Pacific/Kiritimati	+14
Pacific/Kosrae	+11
Pacific/Kwajalein	+12
Pacific/Majuro	+12
Pacific/Marquesas	−9.30
Pacific/Midway	−11
Pacific/Nauru	+12
Pacific/Niue	−11
Pacific/Norfolk	+11.30
Pacific/Noumea	+11
Pacific/Palau	+9
Pacific/Ponape	+11
Pacific/Port_Moresby	+10
Pacific/Rarotonga	−10
Pacific/Saipan	+10

Table B-1 *List of Standard Time Zones and Offsets from UTC (continued)*

Time Zone	Offset from UTC
Pacific/Tahiti	−10
Pacific/Tarawa	+12
Pacific/Tongatapu	+13
Pacific/Truk	+10
Pacific/Wake	+12
Pacific/Wallis	+12
Pacific/Yap	+10
Pacific/Pitcairn	−8
Pacific/Gambier	−9
Pacific/Honolulu	−10
Pacific/Pago_Pago	−11
Pacific/Samoa	−11
NZ	+12
NZ-CHAT	+12.45
Kwajalein	+12
Poland	+1
Portugal	0
ROC	+8
ROK	+9
Singapore	+8
Turkey	+2
UCT	0
US/Alaska	−9
US/Aleutian	−10
US/Arizona	−7
US/Central	−6
US/East-Indiana	−5
US/Hawaii	−10
US/Indiana-Starke	−5
US/Michigan	−5
US/Mountain	−7
US/Pacific	−8
US/Samoa	−11
US/Eastern	−5
MST	+7
CST6CDT	−6

Table B-1 *List of Standard Time Zones and Offsets from UTC (continued)*

Time Zone	Offset from UTC
EST	−5
HST	−10
MST7MDT	+7
Navajo	−7
PST8PDT	−8
W-SU	+3
WET	0
Zulu	0
UTC	0
Universal	0
EST5EDT	−5



I N D E X

Symbols

- ! (exclamation point) [417, 426](#)
- (hyphen) [106, 426, 431, 463](#)
- ... (ellipsis) [426, 430](#)
- .bin files
 - installing [119](#)
- .nsc file [370](#)
- .pax files
 - installing [119](#)
- / (slash) [43](#)
- ? (question mark) [105](#)

A

- aaa accounting
 - statistics for [335](#)
- access lists
 - configuration, displaying [198](#)
 - configuring [15](#)
 - enabling [15](#)
 - group names [16](#)
 - interfaces and applications
 - applying to [130](#)
 - status [254](#)
 - statistics
 - clearing [50](#)
 - displaying [297](#)
- ACLs
 - See IP ACLs
- ACPI
 - models supporting [377](#)
- acquirer

- delivery service information and content acquisition progress, displaying [199](#)
- delivery service statistics, displaying [298](#)
- starting and stopping acquisition on a specific delivery service [17](#)
- acquisition and distribution
 - starting and stopping [21](#)
- action rule
 - configuring [186](#)
- address translation tables [204](#)
- administrative login authentication and authorization
 - default [26](#)
 - local database
 - description of [27](#)
- RADIUS
 - enabling and disabling [169](#)
 - overview of [28](#)
- TACACS+
 - enabling and disabling [399](#)
- administrative privileges
 - users, clearing [52](#)
- alarm information
 - for all alarms [201](#)
 - for critical alarms [202](#)
 - for major alarms [202](#)
 - for minor alarms [202](#)
- alarm overload [22](#)
- alarms
 - displaying status and history [201](#)
- alarm traps
 - configuring [383](#)
 - generating [383](#)
- Apache CLF transaction log format [426](#)
- applications

- applying access lists to [130](#)
- archive log file
 - compressing [434](#)
 - marking beginning and end [426](#)
 - maximum size [426](#)
 - naming convention [433](#)
- ARP table, displaying [204](#)
- authentication
 - access lists, enabling [15](#)
 - configuration, displaying [205](#)
 - configuring [25](#)
 - outgoing proxy [19](#)
 - server redundancy [27](#)
 - statistics
 - clearing [50](#)
 - displaying [300](#)
 - users
 - creating [448](#)
 - local [26](#)
 - TACACS+ [26](#)
- authentication command [27](#)
- authorization
 - administrative login authorization [25](#)

B

- bandwidth
 - displaying [207](#)
 - interface, configuring [34](#)
 - network resources and [31](#)
 - setting for streaming media [31](#)
- bandwidth configuration
 - incoming and outgoing [32](#)
- banners
 - configuration of [35](#)
 - displaying [209](#)
 - enabling [36](#)
 - types of
 - EXEC [36](#)

- login [36](#)
- motd [36](#)
- basic configuration settings
 - setting up [197](#)
- bit rate
 - displaying [210](#)
 - HTTP and WMT, configuring [38](#)

C

- cache
 - clearing [49](#)
 - content [41](#)
- caching
 - HTTP
 - configuring [108](#)
 - objects [49](#)
 - matching against parameters for requests [186](#)
- caching services
 - setting up [197](#)
- calendar
 - setting [53](#)
- CAR
 - IP precedence
 - ToS [127](#)
- CDN file system
 - See cdnfs
- cdnfs
 - information, displaying [213](#)
 - statistics, displaying [301](#)
- CDS
 - installing [119](#)
- Centralized Management System
 - See CMS
- Cisco script
 - executing [192](#)
- Cisco Streaming Engine server
 - live streaming with [180](#)
- Cisco Technical Assistance Center (TAC) [355](#)

- classification
 - IP precedence
 - ToS field [127](#)
 - clock
 - clearing and setting [53](#)
 - daylight saving and local time, setting [55](#)
 - displaying standard timezones [214](#)
 - Service Engine, synchronizing [157](#)
 - software time and date, setting [159](#)
 - system clock settings, displaying [214](#)
 - UTC current time of day, setting [56](#)
 - UTC offset, setting [56](#)
 - CMS
 - database, configuring [59](#)
 - enabling [62](#)
 - maintenance routines, scheduling [62](#)
 - process information, displaying [217](#)
 - cold restart [174](#)
 - command-line processing [1](#)
 - command modes
 - EXEC [3](#)
 - global configuration [3](#)
 - interface configuration [4](#)
 - command syntax [4](#)
 - configuration modes
 - extended ACL [131](#)
 - ICAP service [4](#)
 - standard ACL [131](#)
 - configuring
 - alarm traps [383](#)
 - disk space allocation [84](#)
 - RADIUS authentication [28](#)
 - console
 - setting length of display [410](#)
 - content acquisition
 - database cleanup [21](#)
 - starting and stopping [21](#)
 - Content Delivery System Manager
 - configuring IP address [46](#)
 - disk space allocation [85](#)
 - primary role [58](#)
 - SSL [59](#)
 - standby role [46](#)
 - copying
 - configuration data [66](#)
 - files [68, 69](#)
 - image data [66](#)
 - crossdomain support [195](#)
 - custom transaction log format [426](#)
-
- ## D
- database cleanup
 - content acquisition and distribution [21](#)
 - date and time
 - setting [159](#)
 - daylight saving time
 - setting [55](#)
 - debug
 - disabling [443](#)
 - enabled options, displaying [220](#)
 - software functions [70](#)
 - debug cdnfs command [75](#)
 - default gateway
 - defining [123](#)
 - removing [123](#)
 - default status
 - restoring [176](#)
 - deleting
 - directories [78, 179](#)
 - directory trees [78](#)
 - files [77](#)
 - delivery service distribution
 - information, displaying [227](#)
 - device mode
 - and linked CLI commands [1](#)
 - configuring [79](#)
 - displaying [221](#)

devices
 shutting down [377](#)
 DHCP services
 enabling [120](#)
 differentiated service model
 classification [127](#)
 directories
 changing [43](#)
 creating [147](#)
 deleting [78, 179](#)
 files, viewing [81, 141](#)
 disk drives
 error handling thresholds
 description of [89](#)
 specifying [89](#)
 disks
 configuring [84](#)
 space allocation [84](#)
 details, viewing [224](#)
 partitions, removing [176](#)
 space allocation [84](#)
 space-allocation guidelines [85](#)
 disk space allocated to system use [85](#)
 distribution
 delivery service, displaying [227](#)
 statistics
 displaying [227](#)
 DNS lookup [93](#)
 domain name
 resolving to IP address [93](#)
 DSCP
 setting [122](#)
 dumping network traffic [403](#)
 DWRED
 IP precedence
 ToS [127](#)

E

echo packets
 sending [160](#)
 ellipsis (...) [426, 430](#)
 embedded database parameters
 configuring [58](#)
 enabling
 login authentication and authorization [25](#)
 RADIUS authentication and authorization [170](#)
 rules processing [184](#)
 TACACS+ authentication and authorization [399](#)
 exclamation point (!) [417, 426](#)
 EXEC command mode
 described [3](#)
 returning to [97](#)
 exiting
 from configuration modes [97](#)
 from privileged EXEC mode [83](#)
 exporting transaction logs
 forced [419](#)
 to FTP server [434](#)
 to SFTP server [434](#)
 extended access lists [131](#)
 extended IP ACLs
 configuration examples [137](#)
 configuring [132](#)
 ICMP message types [135](#)
 supported keywords [134](#)
 TCP keywords [134](#)
 Extended Squid transaction log format [426](#)
 external FTP server
 exporting transaction logs to [434](#)
 permanent error from [435](#)

F

failover
 for administrative login authentication [27](#)

Fast Cache

- enabling [455](#)

Fast Start

- enabling [455](#)

file

- copying [69](#)
- creating [148, 419](#)
- deleting [77](#)
- displaying name [141, 438](#)
- management [43](#)
- renaming [175](#)

flash memory

- configuring upon reload [174](#)
- data, removing [176](#)
- version and usage, displaying [237](#)

FTP

- access lists [132](#)

FTP over HTTP

- Rules Template and [186](#)

FTP servers

- exporting transaction logs to [434](#)

G

Gigabit Ethernet

- configuring [120](#)
- negating interface configuration command [156](#)

global configuration command mode

- entering [65](#)
- exiting [95](#)
- negating command [154](#)
- setting [65](#)

global configuration mode

- description [3](#)

GMT

- changing local time in content to [17](#)
- UTC and [56](#)

Greenwich Mean Time

- See GMT

group names

- access lists [16](#)

H

hardware interface

- displaying information [249](#)
- shutting down [376](#)

hardware status, displaying [241](#)help system [6, 105](#)

history

- statistics, clearing [50](#)

hostname

- of Service Engine [106](#)
- resolving to IP address [93](#)

hosts

- name servers and IP addresses, displaying [244](#)

HTTP

- bit rate, setting [38](#)

object cache

- clearing [49](#)
- configuring [108](#)

proxy

- support for root Service Engine [19](#)

- related parameters, configuring [107](#)

statistics

- displaying [245](#)

- statistics, displaying [308](#)

- status codes [426](#)

- transaction logging [426](#)

- users, managing [449](#)

HTTPS

- Rules Template with [186](#)

- hyphen (-) [106, 426](#)

I
ICAP [112](#)

- configuration
 - displaying [247](#)
 - services
 - configuring [115](#)
 - statistics
 - displaying [312](#)
 - working with third-party applications [112](#)
 - ICAP service configuration mode [4](#)
 - ICMP
 - access lists [132](#)
 - keywords for message type and code [135](#)
 - statistics
 - clearing [50](#)
 - displaying [315](#)
 - image data
 - copying [66](#)
 - initial network device settings
 - changing [122](#)
 - installing system image [119](#)
 - interface
 - bandwidth [34](#)
 - configuring [120](#)
 - displaying hardware status [249](#)
 - standby [294](#)
 - interface configuration command mode [4](#)
 - Internet Content Adaptation Protocol
 - See ICAP
 - Internet socket connection statistics
 - displaying [326](#)
 - inventory information
 - displaying [252](#)
 - IP ACLs
 - activating on an interface [137](#)
 - clearing IP ACL counter [50](#)
 - creating and modifying [130](#)
 - description of [133](#)
 - extended configuration mode
 - accessing [132](#)
 - extended IP ACLs [134](#)
 - standard configuration mode
 - accessing [131](#)
 - standard IP ACLs [134](#)
 - typical uses of [133](#)
 - IP address
 - Content Delivery System Manager, configuring [46](#)
 - starting autodiscovery utility [123](#)
 - statistics, clearing [50](#)
 - IP default domain name
 - defining [123](#)
 - removing [123](#)
 - IP default gateway
 - defining [123](#)
 - removing [123](#)
 - IP precedence
 - edge function [127](#)
 - ToS field
 - classification [127](#)
 - IP route table, displaying [256](#)
 - IP statistics
 - displaying [321](#)
-
- ## K
- kernel debugger [139](#)
 - keystroke combinations, CLI [2](#)
-
- ## L
- Last-Modified-Time [17](#)
 - launching
 - Setup utility [197](#)
 - LDAP
 - parameters, displaying [257](#)
 - lists
 - directory names [141](#)
 - file [146](#)
 - live events

- about [267](#)
- configuration requirements [268](#)
- live streaming
 - with Cisco Streaming Engine [180](#)
- live stream interruptions [268](#)
- load balancing
 - for Port Channel [162](#)
- local time, changing to GMT [17](#)
- log file
 - number of lines to view [440](#)
- log files
 - exporting [432](#)
 - restarting the export of [436](#)
- logging
 - clearing syslog messages [50](#)
 - configuring [142](#)
 - file rotation of logs [144](#)
 - RealProxy errors [145](#)
 - WMT multicast [452](#)
- logging in
 - to Service Engine
 - using SSH [396](#)
 - using Telnet [409](#)
- login authentication [26](#)

M

- mapping syslog priority levels to RealProxy error codes [145](#)
- MIB view
 - defining [394](#)
- modes
 - command
 - EXEC [3](#)
 - global configuration [3](#)
 - interface configuration [4](#)
 - configuration
 - extended ACL [4](#)
 - HTTP server [4](#)

- ICAP service [4](#)
 - standard ACL [4](#)
- multicast
 - disabling backup senders [63](#)
 - overview [457](#)
 - WMT, logging [457](#)
- multicast cloud, displaying information [227](#)
- multicast logging
 - WMT [457, 460](#)

N

- NAT
 - configuring [98](#)
 - negating interface configurations [156](#)
- Network Address Translation
 - See NAT
- network connectivity
 - testing [160](#)
- network host name
 - Service Engine [106](#)
- network interfaces
 - configuring for DHCP [120](#)
 - EtherChannel [120](#)
- Network Time Protocol
 - See NTP
- network traffic
 - dumping [403](#)
- node
 - activating [59](#)
 - communication over secure channels [58](#)
- NTP
 - configuring and enabling [157](#)
 - setting software time and date [159](#)
 - status, displaying [262](#)
 - system clock, synchronizing [157](#)
- number of lines displayed [410](#)
- NVRAM
 - configuration stored, displaying [295](#)

startup configuration, writing or erasing [466](#)

O

offset from UTC [1](#)
 online help [105](#)
 outgoing proxy
 authentication [19](#)

P

pacing bit rate
 HTTP and WMT [38](#)
 patterns
 lists described [187](#)
 rules for lists [186](#)
 searching in files [100](#)
 permanent errors
 FTP server [435](#)
 ping [160](#)
 policies
 and the Rules Template [186](#)
 Port Channel
 configuring [120](#)
 load-balancing options [162](#)
 negating interface configuration [156](#)
 powering off [377](#)
 present working directory
 information, displaying [141, 165](#)
 preserving configurations on device restore [176](#)
 preserving data on device restore [176](#)
 primary Content Delivery System Manager [46](#)
 primary interface
 changing to a different interface [163](#)
 configuring for Ethernet [163](#)
 privileged level EXEC commands
 accessing [94](#)
 disabling [83](#)

processes
 CPU or memory, displaying [264](#)
 programs
 displaying [266](#)
 live [267](#)
 movie streamer rebroadcast [268](#)
 WMT rebroadcast
 about [268](#)

Q

question mark (?) [105](#)
 QuickTime [180](#)

R

RADIUS authentication
 configuring [28](#)
 overview [28](#)
 RADIUS key
 specifying on Service Engine [28](#)
 RADIUS server
 authentication [168](#)
 excluding domains [169](#)
 information, displaying [273](#)
 parameters, configuring [168](#)
 statistics
 clearing [51](#)
 displaying [328](#)
 RADIUS servers
 as authentication servers [28](#)
 authentication settings [28](#)
 RealProxy
 access control [182](#)
 error logging [145](#)
 Real-Time Streaming Protocol
 See RTSP
 rebooting Service Engine [174](#)

- regular pattern expression
 - searching [100](#)
- reload [174](#)
- reloading
 - Service Engine
 - automatic reload option [89](#)
- reloading Service Engine
 - automatic reload option [89](#)
- remote host route trace [415, 418](#)
- removing
 - nodes from the CDS network [59](#)
- renaming a file [175](#)
- replication status and statistics, displaying [329](#)
- resetting
 - device to default condition [176](#)
- restart, cold [174](#)
- restoring
 - device to default condition [176](#)
- retransmit count
 - for RADIUS server authentication [28](#)
- rotated log files [144](#)
- routes
 - displaying table [256](#)
 - traceroute6 [418](#)
 - tracing [415](#)
- RTSP
 - configurations and license agreements [277](#)
 - gateway overview [181](#)
 - Rules Template [186](#)
- RTSP gateway
 - purpose of [181](#)
- rule actions
 - supported action and pattern combinations [187](#)
- rules
 - clearing statistics [51](#)
 - configuration, displaying [278](#)
 - general and specific commands [183](#)
 - matching against regular expressions [186](#)
 - setting filters [183](#)

See also Rules Template

- Rules Template
 - actions
 - description [187](#)
 - patterns
 - description [188](#)
- running configuration, displaying current profile [280](#)
- running statistics, clearing [51](#)

S

- saving
 - configuration changes [6](#)
 - file system contents [174](#)
- scheduled WMT rebroadcasts
 - about [268](#)
- script
 - executing [192](#)
- secret keys
 - RADIUS [28, 169](#)
 - TACACS+ [400](#)
- Secure Shell
 - See SSH
- send echo packets (ping) [160](#)
- Service Engine
 - automatic reload [89](#)
- Service Routers
 - crossdomain support [195](#)
 - disk space allocation [85](#)
- services
 - access lists [130](#)
 - information [287](#)
 - statistics [332](#)
- setup
 - configuring [197](#)
- shutting down
 - Content Delivery System Managers [377](#)
 - Program Managers [377](#)
 - Service Engines [377](#)

- Service Routers [377](#)
- shutting down hardware interfaces [376](#)
- slash (/) [43](#)
- SNMP
 - communications status, displaying [289](#)
 - host trap recipient, setting [387](#)
 - security model group, defining [385](#)
 - server user, defining [392](#)
 - statistics
 - clearing [51](#)
 - statistics, displaying [333](#)
 - system location string, setting [389](#)
 - system notify inform string, configuring [390](#)
 - system server contact string, setting [382](#)
 - traps, enabling [383](#)
 - Version 2 MIB view, defining [394](#)
- SNMP traps
 - configuring [383](#)
 - disabling [383](#)
 - enabling [383](#)
- socket connection
 - statistics, displaying [326](#)
- software clock
 - setting [159](#)
- Squid transaction log format [426](#)
- SSH
 - configuration and status, displaying [293](#)
 - enabling daemon [396](#)
 - session timeout [96](#)
- standard access lists
 - creating [131](#)
- standard time zones
 - and offsets from UTC [1](#)
 - list of [1](#)
- standard timezones, displaying [214](#)
- standby Content Delivery System Manager [46](#)
- standby interface
 - displaying information [294](#)
- startup configuration
 - displaying [295](#)
- static IP routing
 - configuring [124](#)
- statistics
 - clearing [49, 50](#)
- storage
 - pre-positioned CDS network content [44](#)
- streaming media players
 - IP/TV Viewer [267](#)
 - QuickTime [267](#)
- subdirectories
 - viewing names [141](#)
- summer daylight saving time
 - setting [55](#)
- synchronizing
 - cdnfs [45](#)
 - system clock [157](#)
- syslog
 - configuration, displaying [259](#)
 - configuring [142](#)
 - RealProxy priority level error mapping [145](#)
 - sysfs location [144](#)
- syslog hosts, configuring [144](#)
- system clock
 - synchronized by time server [157](#)
- system disk space usage [85](#)
- system hardware
 - displaying status [241](#)
- system help [6](#)
- system image
 - installing [119](#)
- system inventory
 - displaying [252](#)
- system logging
 - configuring [144](#)
 - to console [142](#)
 - to disk [142](#)
 - to remote hosts [144](#)

T

TAC

viewing technical support information [355](#)

TACACS+

authentication information, displaying [353](#)

configuring server parameters [399](#)

statistics

clearing [51](#)

displaying [335](#)

TCP

access lists [132](#)

keywords and port numbers [134](#)

statistics

clearing [51](#)

technical support information

viewing [355](#)

Telnet services

configuration, displaying [361](#)

enabling [409](#)

session timeout [4, 96](#)

terminal

setting number of lines to be displayed [410](#)

testing

connectivity of URLs

for FTP-over-HTTP [412](#)

for HTTP [412](#)

test-url command

troubleshooting

with the HTTP CLI client [412](#)

TFTP

access lists [132](#)

thresholds

disk error handling [89](#)

time, correcting [17](#)

time and date

setting [159](#)

timeout intervals

for RADIUS server authentication [28](#)

timeout of a nonresponsive host [160](#)

time zone

offset setting [56](#)

setting [55](#)

time zones

list of [1](#)

token strings [426](#)

ToS

classification [127](#)

setting [122](#)

trace the route of remote host [415, 418](#)

transaction logging

archive file naming convention [433](#)

archiving working log files [51](#)

authentication [109](#)

clearing log export statistics [51](#)

compressing archive files [434](#)

configuration and archived files, displaying [362](#)

configuring and enabling [421](#)

exporting [434](#)

forcing archive or export [419](#)

formats [426](#)

log export statistics, displaying [345](#)

permanent errors from external server [435](#)

transaction logs

archiving of [432](#)

clearing [49](#)

displaying configuration of [362](#)

exporting [432](#)

sanitizing [432](#)

traps

enabling [383](#)

troubleshooting

with ping [160](#)

with Telnet client [408](#)

with the HTTP CLI client [412](#)

with traceroute [415](#)

U

- UDI compliance [252](#)
- UDP
 - access lists [132](#)
 - keywords and port numbers [134](#)
 - statistics
 - clearing [51](#)
 - displaying [347](#)
- undoing global configuration commands [154](#)
- Universal Coordinated Time
 - See UTC [1](#)
- updating the calendar [53](#)
- URL signature [444](#)
 - shared key [445](#)
- user authentication
 - local [26](#)
 - RADIUS [26](#)
- user-level EXEC command mode [3](#)
- users
 - administrative and authenticated, displaying [368](#)
 - authenticated users, clearing [51](#)
 - authentication [448](#)
 - defining for SNMP server [392](#)
 - removing data from disk [176](#)
 - user identification number and name, displaying [367](#)
- UTC
 - and standard time zones [1](#)
 - clock EXEC command [56](#)
 - offsets from [1](#)

V

- variable bit rates [39](#)
- version
 - displaying information about [369](#)

W

- WFQ
 - IP precedence
 - ToS [127](#)
- WMT
 - bit rate, setting [38](#)
 - configuration and license information, displaying [370](#)
 - configuring [452](#)
 - conventional proxy service [455](#)
 - enabling [455](#)
 - Fast Cache
 - enabling [455](#)
 - Fast Start
 - enabling [455](#)
 - multicast
 - logging [457](#)
 - overview [457](#)
 - multicast-in and multicast-out [457](#)
 - multicast-in and unicast-out [457](#)
 - multicast logging [457, 460](#)
 - statistics
 - clearing [51](#)
 - displaying [348](#)
 - unicast-out and multicast-in [457](#)
- WMT caching proxy
 - variable bit rates [39](#)
- WMT error logging [75](#)
- WMT live splitting [458](#)
- WMT multicast-in multicast-out
 - description of [457](#)
- WMT multicast-in unicast-out [457](#)
- WMT multicasts, types of
 - multicast-in multicast-out [457](#)
 - multicast-in unicast-out [457](#)
- WMT rebroadcasts [268](#)
- WMT streaming and caching
 - displaying WMT statistics [348](#)

WMT transaction logs

formats accepted by Windows Media Services 9 [458](#)

logging usernames [460](#)

specifying format of [458](#)

WMT unicast-in unicast-out

description of [457](#)

working.log file [426](#)

