Cisco Internet Streamer CDS 3.2 Command Reference

March 2013

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-29022-01

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

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

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

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

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

OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned 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. (1110R)

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 3.2 Command Reference
© 2004–2013 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface xv

Document Revision History xv

Document Organization xv

Audience xvi

Conventions xvi

Related Documentation xvii

Obtaining Documentation and Submitting a Service Request xvii

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 1-5

System Help 1-6

Filtering Output Using Output Modifiers 1-6

Saving Configuration Changes 1-6

CHAPTER 2 **Cisco Internet Streamer CDS Release 3.2 Software Commands** 2-1

aaa 2-23

access-lists 2-27

acquirer (EXEC) 2-30

acquirer (Global configuration) 2-33

acquisition-distribution 2-35

alarm 2-37

area nssa 2-39

area stub 2-40

asset 2-41

authsvr 2-42

bandwidth (Global configuration) 2-44
bandwidth (interface configuration) 2-47
banner 2-49
bitrate 2-52
blink 2-55
bootstrap-node 2-56
cache 2-58
capability 2-62
cd 2-63
cdn-select 2-64
cdnfs 2-65
cdsm 2-68
clear cache 2-71
clear content 2-73
clear ip 2-75
clear ipv6 2-77
clear isis 2-78
clear logging 2-80
clear service-router 2-81
clear srp database offline 2-82
clear srp descriptor 2-83
clear srp neighbor 2-85
clear srp resource 2-88
clear srp route 2-90
clear statistics 2-92
clear transaction-logs 2-97
clear users 2-98
clear wmt 2-99
clock (EXEC) 2-100
clock (Global configuration) 2-102
cms (EXEC) 2-105
cms (Global configuration) 2-109
configure 2-112
contentmgr 2-113
content-mgr disk-info force-reset 2-116

content-origin 2-117
copy 2-118
cpfile 2-121
debug 2-122
debug ip bgp 2-133
debug ip ospf 2-135
debug ip proximity 2-138
debug ip rib 2-139
debug isis 2-141
debug srp 2-142
delfile 2-144
deltree 2-145
device 2-146
dir 2-148
direct-server-return 2-149
disable 2-150
disk (EXEC) 2-151
disk (Global configuration) 2-156
distribution 2-160
dnslookup 2-164
domain 2-165
enable 2-166
enable password 2-167
end 2-168
exec-timeout 2-169
exit 2-170
expert-mode password 2-171
external-ip 2-172
find-pattern 2-174
flash-media-streaming 2-176
flooding 2-179
geo-location-server 2-180
gulp 2-181
help 2-184
hostname 2-185

install **2-186**
interface **2-187**
ip (Global configuration) **2-192**
ip (Interface configuration) **2-198**
ip access-list **2-201**
ip ospf priority **2-209**
ip rib route **2-210**
ip router isis **2-212**
ipv6 **2-213**
isis **2-217**
is-type **2-220**
kernel **2-222**
key **2-223**
key-string **2-224**
key chain **2-225**
lacp **2-227**
line **2-229**
lls **3-230**
location community **3-231**
log-adjacency-changes **3-234**
logging **3-235**
log-neighbor-changes **3-239**
ls **3-240**
lsp-mtu **3-241**
mkdir **3-242**
mkfile **3-243**
model **3-244**
movie-streamer **3-245**
mtu **3-248**
multicast (Global Configuration) **3-249**
multicast (EXEC Configuration) **3-252**
neighbor **3-259**
net **3-262**
netmon **3-263**
netstatr **3-264**

network area 3-265
no (Global configuration) 3-267
no (interface configuration) 3-269
ntp 3-270
ntpdate 3-272
ping 3-273
ping srp 3-274
ping6 3-275
port-channel 3-276
primary-interface 3-278
proximity algorithm bgp 3-280
proximity engine enable 3-286
pwd 3-289
radius-server 3-290
rcp 3-294
reload 3-295
rename 3-296
restore 3-297
rmdir 3-300
router bgp 3-301
router isis 3-302
router ospf 3-304
router srp 3-306
rtsp 3-307
rule 3-310
script 3-321
service 3-322
service-router 3-323
setup 3-339
show aaa 3-340
show access-lists 300 3-343
show acquirer 3-344
show alarms 3-346
show arp 3-349
show authentication 3-350

show authsvr 3-351
show bandwidth 3-352
show banner 3-354
show bitrate 3-355
show cache 3-356
show cache-router 3-358
show capability 3-359
show cdn-select 3-360
show cdnfs 3-361
show clock 3-363
show cms 3-366
show content 3-368
show content-mgr 3-371
show content-origin 3-374
show debugging 3-376
show debugging srp 3-379
show device-mode 3-380
show direct-server-return 3-382
show disks 3-383
show distribution 3-387
show flash 3-399
show flash-media-streaming 3-401
show ftp 3-403
show hardware 3-404
show hosts 3-410
show interface 3-411
show inventory 3-416
show ip access-list 3-418
show ip bgp 3-420
show ip bgp all 3-422
show ip bgp community 3-423
show ip bgp ipv4 unicast 3-425
show ip bgp memory 3-426
show ip bgp neighbors 3-427
show ip bgp nexthop-database 3-429

show ip bgp summary 3-430
show ip interface 3-431
show ip ospf 3-432
show ip ospf border-routers 3-434
show ip ospf database 3-435
show ip ospf interface 3-441
show ip ospf memory 3-443
show ip ospf neighbor 3-445
show ip ospf request-list 3-447
show ip ospf retransmission-list 3-448
show ip ospf route 3-449
show ip ospf rspf route 3-451
show ip ospf traffic 3-453
show ip proximity algorithm 3-455
show ip proximity servers 3-456
show ip rib clients 3-457
show ip rib memory 3-458
show ip rib recursive-next-hop 3-460
show ip rib route 3-461
show ip rib unresolved-next-hop 3-463
show ip routes 3-464
show ip static route 3-466
show ipv6 3-467
show isis adjacency 3-469
show isis clns route 3-471
show isis database 3-472
show isis hostname-table 3-476
show isis interface 3-477
show isis ip route 3-480
show isis ip rspf route 3-482
show isis memory 3-484
show isis process 3-485
show isis rrm 3-486
show isis spf-log 3-487
show isis srm 3-489

show isis ssn 3-490
show key chain 3-491
show lacp 3-492
show logging 3-494
show movie-streamer 3-496
show multicast 3-497
show ntp 3-498
show processes 3-500
show programs 3-502
show radius-server 3-508
show rcp 3-510
show rtsp 3-511
show rule 3-512
show running-config 3-514
show service-router 3-518
show services 3-524
show snmp 3-526
show srp database 3-530
show srp leafset 3-537
show srp memory 3-539
show srp multicast database 3-540
show srp neighbor 3-543
show srp process 3-546
show srp replica-set 3-547
show srp route 3-548
show srp subscribers 3-550
show ssh 3-551
show standby 3-552
show startup-config 3-553
show statistics aaa 3-556
show statistics access-lists 300 3-557
show statistics acquirer 3-558
show statistics admission 3-561
show statistics authsvr 3-563
show statistics cdn-select 3-566

show statistics cdnfs 3-567
show statistics content-mgr 3-569
show statistics distribution 4-571
show statistics flash-media-streaming 4-574
show statistics icmp 4-583
show statistics ip 4-589
show statistics isis 4-593
show statistics movie-streamer 4-595
show statistics netstat 4-598
show statistics radius 4-599
show statistics replication 4-600
show statistics service-router 4-604
show statistics services 4-609
show statistics snmp 4-610
show statistics srp 4-612
show statistics tacacs 4-613
show statistics tcp 4-614
show statistics transaction-logs 4-623
show statistics udp 4-625
show statistics web-engine 4-626
show statistics wmt 4-635
show tacacs 4-641
show tech-support 4-643
show telnet 4-649
show transaction-logging 4-650
show url-signature 4-654
show user 4-655
show users 4-656
show version 4-657
show web-engine 4-659
show wmt 4-661
shutdown (interface configuration) 4-667
shutdown (EXEC) 4-668
snmp-server community 4-676
snmp-server contact 4-677

snmp-server enable traps 4-678
snmp-server group 4-680
snmp-server host 4-682
snmp-server location 4-685
snmp-server notify inform 4-686
snmp-server user 4-688
snmp-server view 4-690
splunk-uf-monitor 4-692
ss 4-694
sshd 4-696
streaming-interface 4-698
sysreport 4-699
tacacs 4-700
tcpdump 4-704
tcpmon 4-709
tcp timestamp 4-711
telnet 4-712
telnet enable 4-713
terminal 4-714
test-url 4-715
top 4-719
traceroute 4-720
traceroute srp 4-723
traceroute6 4-724
transaction-log force 4-725
transaction-logs 4-727
type 4-741
type-tail 4-743
undebug 4-746
url-signature 4-748
username 4-752
web-engine (EXEC) 4-755
web-engine (Global configuration) 4-758
whoami 4-764
wmt 4-765

write 4-779

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 xv
- Document Organization, page xv
- Audience, page xvi
- Conventions, page xvi
- Related Documentation, page xvii
- Obtaining Documentation and Submitting a Service Request, page xvii

Document Revision History

Table 1 records the technical changes to the Document Revision History.

Table 1 Document Revision History

Document Version	Date	Change Summary
OL-29022-01	September 14, 2012	Updated for Release 3.1.1 with multicast feature.
OL-27518-01	August 27, 2012	This is the first release of this document.

Document Organization

Table 2 describes the organization of the document.

Table 2 Document Organization

Chapter	Description
Chapter 1, "Command-Line Interface Command Summary"	This chapter describes how to use the CDS[1] CLI[2] to configure software features.
Chapter 2, "Cisco Internet Streamer CDS Release 3.2 Software Commands"	This chapter provides a complete list of Cisco Internet Streamer commands, listed alphabetically.

Table 2 Document Organization (continued)

Chapter	Description
Appendix A, "Acronyms"	This appendix lists the abbreviations and acronyms used in this guide.
Appendix B, "Standard Time Zones"	This appendix lists all the standard time zones that you can configure on a CDE[3] and the offset from UTC[4] for each standard time zone.

1. CDS = content delivery system
2. CLI = command-line interface
3. CDE = content delivery engine
4. UTC = coordinated universal time

Audience

This guide is for the networking professional using Cisco Internet Streamer CDS Release 3.2. Before using this guide, you should have experience working with the Cisco Internet Streamer CDS and the concepts and terminology of Ethernet and local area networking.

Conventions

This publication uses various 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 3.2 Software Configuration Guide*
- *Cisco Internet Streamer CDS 3.2 Alarms and Error Messages Guide*
- *Cisco Content Delivery Engine 205/220/250/420 Hardware Installation Guide*
- *Regulatory Compliance and Safety Information for the Cisco Content Delivery Engines*
- *Cisco Content Delivery System 3.x Documentation Roadmap*
- *Cisco Internet Streamer CDS 3.2 Quick Start Guide*
- *Cisco Internet Streamer CDS 3.2 API Guide*
- *Release Notes for Cisco Internet Streamer CDS 3.2.1*

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

These documents provide complete information about the installation and service of the C200 and C210 and are available from cisco.com.

- Cisco UCS C200 Installation and Service Guide

http://www.cisco.com/en/US/docs/unified_computing/ucs/c/hw/C200M1/install/c200M1.html

- Cisco UCS C210 Installation and Service Guide

http://www.cisco.com/en/US/docs/unified_computing/ucs/c/hw/C210M1/install/C210M1.html

The Cisco UCS C-Series Rack Servers documentation is available from cisco.com at:

http://www.cisco.com/en/US/products/ps10493/prod_installation_guides_list.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 1-5
- System Help, page 1-6
- Filtering Output Using Output Modifiers, 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 that us in effect. Use the **device mode** Global configuration command to change the current device mode to another configuration. Use the **show device-mode** command to display the current device configuration.

To determine if a specific command is available for a specific device type, see Table 2-1.

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 Combination	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 entered.
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 made when entering a command; re-enter the command after using this key.

Using Command Modes

The CLI for Cisco Internet Streamer CDS Release 3.2 software is similar to the CLI for the Cisco IOS software. Both the Cisco IOS software and the CDS CLI are organized into different commands 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 3.2 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 question mark (**?**) 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 several 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 access control list (ACL) configuration mode	**ip access-list standard**
Extended ACL configuration mode	**ip access-list extended**
Internet Content Adaptation Protocol (ICAP) service configuration mode	**icap service**
Open Shortest Path First (OSPF) configuration mode	**router ospf**
Service Routing Protocol (SRP) configuration mode	**router srp**
Border Gateway Protocol (BGP) configuration mode	**router bgp**
Intermediate System -to-Intermediate System (IS-IS) configuration mode	**router isis**

To work with these configuration modes, enter the appropriate command from the Global configuration mode prompt. The CLI can enter 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, "Cisco Internet Streamer CDS Release 3.2 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.

For example, if 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-calendarRead the calendar and update system clock
  setSet the time and date
  update-calendarUpdate the calendar with system clock
```

Filtering Output Using Output Modifiers

Many commands produce lengthy output that may use several screens to display. Using output modifiers, you can filter this output to show only the information that you want to see.

The following three output modifiers are available:

- begin regular-expression—Displays the first line in which a match of the regular expression is found and all lines that follow.
- include regular-expression—Displays all lines in which a match of the regular expression is found.
- exclude regular-expression—Displays all lines except those in which a match of the regular expression is found.

To use one of these output modifiers, type the command followed by the pipe symbol (|), the modifier, and the regular expression that you want to search for or filter. A regular expression is a case-sensitive alphanumeric pattern. It can be a single character or number, a phrase, or a more complex string.

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 about the running and saved configuration modes.

CHAPTER 2

Cisco Internet Streamer CDS Release 3.2 Software Commands

This chapter contains an alphabetical listing of all the commands in Cisco Internet Streamer CDS Release 3.2 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 (config) 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 (config-if) 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—Several 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 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
aaa	Specifies accounting, authentication and authorization methods.	Global configuration	All
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	Configures alarms.	Global configuration	All
area nssa	Configures an area as an NSSA[1].	OSPF configuration	SR
area stub	Defines an area as a stub area.	OSPF configuration	SR
asset	Configures the CISCO-ENTITY-ASSET-MIB.	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[2] 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 MOTD[3] banners.	Global configuration	All
bitrate	Configures the maximum pacing bit rate for the Movie Streamer and configures WMT bit-rate settings.	Global configuration	SE
blink	Identifies physical devices by blinking their LED(s).	Privileged-level EXEC	All
bootstrap-node	Configures a bootstrap node IP address.	SRP configuration	SR
cache	Specifies the cache commands.	Global configuration	SE
capability	Modifies the capability configuration.	Global configuration	SE

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
cd	Changes the directory.	User-level EXEC and privileged-level EXEC	All
cdn-select	Enables the CDN Selector for third-party service selection.	Global Configuration	SR
cdnfs	Manages the Internet Streamer CDNFS[4].	Privileged-level EXEC	SE
cdsm	Configures the CDSM IP address and primary or standby role settings.	Global configuration	All
clear cache	Clears the HTTP object cache.	Privileged-level EXEC	SE, SR
clear content	Clears the URL content.	Privileged-level EXEC	SE, SR
clear ip	Clears the IP configuration.	Privileged-level EXEC	All
clear ipv6	Clears the IPv6 configuration.	Privileged-level EXEC	All
clear isis	Clears the IS-IS Routing for IP.	Privileged-level EXEC	SR
clear logging	Clears the syslog messages saved in the disk file.	Privileged-level EXEC	All
clear service-router	Clears the Service Router.	Privileged-level EXEC	SR
clear srp database offline	Clears the SRP database while it is offline.	Privileged-level EXEC	SR
clear srp descriptor	Deletes a single descriptor or all descriptors from the service routing layer.	Privileged-level EXEC	SR
clear srp neighbor	Removes a neighbor Proximity Engine from the neighbor list of the local Proximity Engine.	Privileged-level EXEC	SR
clear srp resource	Deletes a resource from a descriptor in the service routing layer.	Privileged-level EXEC	SR
clear srp route	Deletes a single route entry from the DHT routing table of the local Proximity Engine.	Privileged-level EXEC	SR
clear statistics	Clears the statistics.	Privileged-level EXEC	All
clear transaction-logs	Clears and archives the working transaction logs.	Privileged-level EXEC	SE, SR
clear users	Clears the connections (login) of authenticated users.	Privileged-level EXEC	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
clear wmt	Clears the WMT streams.	Privileged-level EXEC	SE
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 CMS[5]-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
configure[6]	Enters configuration mode from privileged EXEC mode.	Privileged-level EXEC	All
contentmgr	Configures the Content Manager.	Global configuration	SE
content-mgr disk-info force-reset	Forces the Content Manager to reset the disk share memory information.	User-level EXEC and privileged-level EXEC	SE
content-origin	Supports multiple origin servers within a content origin.	Global configuration	SE
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 and privileged-level EXEC	All
debug	Configures the debugging options.	Privileged-level EXEC	All
debug ip bgp	Displays information related to the BGP process.	Privileged-level EXEC	SR
debug ip ospf	Displays information related to the OSPF process.	Privileged-level EXEC	SR
debug ip proximity	Debugs the transport layer of proximity process.	Privileged-level EXEC	SR
debug ip rib	Turns on proximity debugging information.	Privileged-level EXEC	SR
debug isis	Displays information related to the IS-IS process.	Privileged-level EXEC	SR
debug srp	Turns on SRP debugging information.	Privileged-level EXEC	SR
delfile	Deletes a file.	User-level EXEC and privileged-level EXEC	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
deltree	Deletes a directory and its subdirectories.	User-level EXEC and privileged-level EXEC	All
device	Configures the mode of operation on a device.	Global configuration	All
dir	Displays the list of files in a directory.	User-level EXEC and privileged-level EXEC	All
direct-server-return	Enables 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
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
dnslookup	Resolves a host or domain name to an IP address.	User-level EXEC and privileged-level EXEC	All
domain	Sets the domain ID for the SRP.	SRP configuration	SR
enable[6]	Accesses the privileged EXEC commands.	User-level EXEC and privileged-level EXEC	All
enable password	Changes the enable password.	Global configuration	All
end	Exits configuration and privileged EXEC modes.	Global configuration	All
exec-timeout	Configures the length of time that an inactive Telnet or SSH[7] session remains open.	Global configuration	All
exit	Exits from interface, Global configuration, or privileged EXEC modes.	All	All
expert-mode password	Sets the expert-mode password.	Global configuration	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

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
flash-media-streaming	Enables and configures Flash Media Streaming.	Global configuration	SE, SR
flooding	Sets the flooding threshold for SRP multicast.	SRP configuration	SR
geo-location-server	Redirects requests to different CDNs based on the geographic location of the client.	Global configuration	SR
gulp	Captures lossless gigabit packets and writes them to disk.	Privileged-level EXEC	SE
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
install	Installs a new version of the caching application.	Privileged-level EXEC	All
interface[6]	Configures a Gigabit Ethernet or port channel interface. Provides access to interface configuration mode.	Global configuration	All
ip (Global configuration)	Configures the Internet Protocol.	Global configuration	All
ip (Interface configuration)	Configures the interface Internet Protocol.	Interface configuration	All
ip access-list[6]	Creates and modifies the access lists for controlling access to interfaces or applications. Provides access to ACL configuration mode.	Global configuration	All
ip ospf priority	Sets the router priority, which helps determine the designated router for this network.	Interface configuration mode under OSPF configuration	SR
ip rib route	Configures unicast static routes for the Proximity Engine.	Global configuration	SR
ip router isis	Specifies the interfaces to be used for routing IS-IS.	Interface configuration mode under IS-IS configuration mode	SR
ipv6	Specifies the default gateway's IPv6 address.	Global configuration	SE
isis	Configures IS-IS routing for IP.	Interface configuration mode under IS-IS configuration	SR

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
is-type	Configures a Proximity Engine to act as a Level 1 (intra-area) router, as both a Level 1 router and a Level 2 (interarea) router, or as an inter-area router only.	IS-IS configuration	SR
kernel	Configures the kernel.	Global configuration	All
key	Creates a key ID and enters into key ID configuration submode.	Key chain submode	SR
key-string	Creates a key string to be used for authentication.	Key ID configuration submode	SR
key chain	Creates a key chain and enters into key chain configuration submode.	Global configuration	SR
lacp[8]	Turns on LACP.	Interface configuration	All
line	Specifies the terminal line settings.	Global configuration	All
lls	Displays the files in a long-list format.	User-level EXEC and privileged-level EXEC	All
location community	Configures the community values that are associated with a Proximity Engine.	BGP configuration	SR
log-adjacency-changes	Configures the router to send a syslog message when an IS-IS neighbor goes up or down.	BGP, IS-IS and OSPF configuration	SR
logging	Configures syslog[9].	Global configuration	All
log-neighbor-changes	Enables logging of BGP neighbor resets.	BGP configuration	SR
ls	Lists the files and subdirectories in a directory.	User-level EXEC and privileged-level EXEC	All
lsp-mtu	Sets the maximum transmission unit MTU[10] size of IS-IS LSPs.	IS-IS configuration	SR
mkdir	Makes a directory.	User-level EXEC and privileged-level EXEC	All
mkfile	Makes a file (for testing).	User-level EXEC and privileged-level EXEC	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
model	Changes the CDE250 platform model number after a remanufacturing or rescue process.	User-level EXEC and privileged-level EXEC	All
movie-streamer	Enables and configures the Movie Streamer server.	Global configuration	SE
multicast (Global Configuration)	Configures multicast options.	Global configuration	SE
multicast (EXEC Configuration)	Generate multicast packets and tests connectivity through multicast routers.	User-level EXEC and privileged-level EXEC	SE, CDSM
mtu	Sets the interface maximum transmission unit packet size.	Interface configuration	All
neighbor	Configures the BGP neighbors.	BGP configuration	SR
net	Configures an IS-IS NET[11] for a CLNS[12] routing process.	IS-IS configuration	SR
netmon	Displays the transmit and receive activity on an interface.	Privileged-level EXEC	SE
netstatr	Displays the rate of change of netstat statistics.	Privileged-level EXEC	SE
network area	Defines the interfaces on which OSPF runs and defines the area ID for those interfaces.	OSPF configuration	SR
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 and privileged-level EXEC	All
ping srp	Pings the SRP ring.	User-level EXEC and privileged-level EXEC	SR
ping6	Pings the IPv6 address.	User-level EXEC and privileged-level EXEC	SE
port-channel	Configures the port channel load balancing options.	Global configuration	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
primary-interface	Configures a primary interface for the Internet Streamer CDS network to be a Gigabit Ethernet or port channel interface.	Global configuration	All
proximity algorithm bgp	Enables a BGP proximity algorithm option for the Proximity Engine.	Global configuration	SR
proximity engine enable	Enables the Proximity Engine.	Global Configuration	SR
pwd	Displays the present working directory.	User-level EXEC and privileged-level EXEC	All
radius-server	Configures the RADIUS authentication.	Global configuration	All
rcp	Enables RCP.	Global configuration	All
reload	Halts a device and performs a cold restart.	Privileged-level EXEC	All
rename	Renames a file.	User-level EXEC and privileged-level EXEC	All
restore	Restores a device to its manufactured default status.	Privileged-level EXEC	All
rmdir	Removes a directory.	User-level EXEC and privileged-level EXEC	All
router bgp	Configures a BGP routing process.	Global configuration	SR
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.	Global configuration	SR
router ospf	Enables the OSPF[13] routing process.	Global configuration	SR
router srp	Enters SRP configuration mode.	Global configuration	SR
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	Specifies the type of service.	Privileged-level EXEC	All
service-router	Configures service routing.	Global configuration	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
setup	Configures the basic configuration settings and a set of commonly used caching services.	Privileged-level EXEC	All
show aaa	Displays the accounting, authentication, and authorization configuration.	User-level EXEC and privileged-level EXEC	All
show access-lists 300	Displays the access control list configuration.	User-level EXEC and 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 and privileged-level EXEC	SE
show alarms	Displays information on various types of alarms, their status, and history.	User-level EXEC and privileged-level EXEC	All
show arp	Displays the Address Resolution Protocol entries.	User-level EXEC and privileged-level EXEC	All
show authentication	Displays the authentication configuration.	User-level EXEC and privileged-level EXEC	All
show authsvr	Displays the Authorization Server status.	User-level EXEC and privileged-level EXEC	SE
show bandwidth	Displays the bandwidth allocated to a particular device.	User-level EXEC and privileged-level EXEC	SE, SR
show banner	Displays information on various types of banners.	User-level EXEC and privileged-level EXEC	All
show bitrate	Displays the SE bit-rate configuration.	User-level EXEC and privileged-level EXEC	SE, SR
show cache	Displays a list of cached contents.	User-level EXEC and privileged-level EXEC	SE
show cache-router	Displays cache-route information for various Protocol Engines.	User-level EXEC and privileged-level EXEC	SE
show capability	Displays information for the Cap-X profile ID.	User-level EXEC and privileged-level EXEC	SE

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
show cdn-select	Displays the status of the CDN Selector.	User-level EXEC and privileged-level EXEC	SR
show cdnfs	Displays the Internet Streamer CDS network file system information.	User-level EXEC and privileged-level EXEC	CDSM, SE
show clock	Displays the system clock.	User-level EXEC and privileged-level EXEC	All
show cms	Displays the Centralized Management System protocol, embedded database content, maintenance status, and other information.	User-level EXEC and privileged-level EXEC	All
show content	Displays all content entries in the CDS.	User-level EXEC and privileged-level EXEC	SE
show content-mgr	Displays all content management information in the CDS.	User-level EXEC and privileged-level EXEC	SE
show content-origin	Displays information about the NAS[14] mount.	User-level EXEC and privileged-level EXEC	SE
show debugging	Displays the state of each debugging option.	User-level EXEC and privileged-level EXEC	All
show debugging srp	Displays the debug flags that are turned on for the SRP.	Privileged-level EXEC	SR
show device-mode	Displays the configured or current mode of a CDSM, SE, or SR device.	User-level EXEC and privileged-level EXEC	All
show direct-server-return	Displays the Direct Server return information.	User-level EXEC and privileged-level EXEC	SE, SR
show disks	Displays the disk configurations.	User-level EXEC and privileged-level EXEC	All
show distribution	Displays the distribution information for a specified delivery service.	User-level EXEC and privileged-level EXEC	SE
show flash	Displays the flash memory information.	User-level EXEC and privileged-level EXEC	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
show flash-media-streaming	Displays the Flash Media Streaming information.	User-level EXEC and privileged-level EXEC	SE, SR
show ftp	Displays the caching configuration of the FTP[15].	User-level EXEC and privileged-level EXEC	All
show hardware	Displays the system hardware information.	User-level EXEC and privileged-level EXEC	All
show hosts	Displays the IP domain name, name servers, IP addresses, and host table.	User-level EXEC and privileged-level EXEC	All
show interface	Displays the hardware interface information.	User-level EXEC and privileged-level EXEC	All
show inventory	Displays the system inventory information.	User-level EXEC and 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 and privileged-level EXEC	All
show ip bgp	Displays the contents of a particular host in the BGP routing table.	User-level EXEC and privileged-level EXEC	SR
show ip bgp all	Displays the contents of the BGP routing table.	User-level EXEC and privileged-level EXEC	SR
show ip bgp community	Displays BGP routes that match a specified BGP community string.	User-level EXEC and privileged-level EXEC	SR
show ip bgp ipv4 unicast	Displays information relating to all IPV4 unicast routes in the BGP routing table.	User-level EXEC and privileged-level EXEC	SR
show ip bgp memory	Displays memory usage information of the running BGP daemon.	User-level EXEC and privileged-level EXEC	SR
show ip bgp neighbors	Displays information about the TCP and BGP connections to neighbors.	User-level EXEC and privileged-level EXEC	SR
show ip bgp nexthop-database	Displays the next-hop database information in the BGP routing table.	User-level EXEC and privileged-level EXEC	SR

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
show ip bgp summary	Displays the status of all BGP connections.	User-level EXEC and privileged-level EXEC	SR
show ip interface	Displays the IP interface state and its address and mask for all interfaces.	User-level EXEC and privileged-level EXEC	SR
show ip ospf	Displays general information about OSPF routing processes.	User-level EXEC and privileged-level EXEC	SR
show ip ospf border-routers	Displays general information about OSPF border routers.	User-level EXEC and privileged-level EXEC	SR
show ip ospf database	Displays information specific to the OSPF database for a specific router.	User-level EXEC and privileged-level EXEC	SR
show ip ospf interface	Displays OSPF-related interface information.	User-level EXEC and privileged-level EXEC	SR
show ip ospf memory	Displays memory usage of the OSPF process.	User-level EXEC and privileged-level EXEC	SR
show ip ospf neighbor	Displays OSPF neighbor information.	User-level EXEC and privileged-level EXEC	SR
show ip ospf request-list	Displays a list of all LSAs[16] requested by a router.	User-level EXEC and privileged-level EXEC	SR
show ip ospf retransmission-list	Displays a list of all LSAs waiting to be re-sent.	User-level EXEC and privileged-level EXEC	SR
show ip ospf route	Displays the OSPF RSPF route for OSPF routes.	User-level EXEC and privileged-level EXEC	SR
show ip ospf rspf route	Displays OSPF RSPF[17] from specific routers.	User-level EXEC and privileged-level EXEC	SR
show ip ospf traffic	Displays OSPF traffic statistics.	User-level EXEC and privileged-level EXEC	SR
show ip proximity algorithm	Displays the proximity algorithm options currently in use by this Proximity Engine.	User-level EXEC and privileged-level EXEC	SR

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
show ip proximity servers	Displays the interface addresses and hostnames of the proximity servers currently in use by this Proximity Engine.	User-level EXEC and privileged-level EXEC	SR
show ip rib clients	Displays details of all the routing protocol instances that are clients of the RIB.	User-level EXEC and privileged-level EXEC	SR
show ip rib memory	Displays the memory usage information of the RIB.	User-level EXEC and privileged-level EXEC	SR
show ip rib recursive-next-hop	Displays IP recursive next-hop information from the RIB.	User-level EXEC and privileged-level EXEC	SR
show ip rib route	Displays IP RIB route information.	User-level EXEC and privileged-level EXEC	SR
show ip rib unresolved-next-hop	Displays unresolved next-hop information from the RIB.	User-level EXEC and privileged-level EXEC	SR
show ip routes	Displays the IP routing table.	User-level EXEC and privileged-level EXEC	All
show ip static route	Displays IP static route information.	User-level EXEC and privileged-level EXEC	SR
show ipv6	Displays IPv6 information.	User-level EXEC and privileged-level EXEC	All
show isis adjacency	Displays IS-IS adjacencies.	User-level EXEC and privileged-level EXEC	SR
show isis clns route	Displays one or all the destinations to which the router knows how to route CLNS packets.	User-level EXEC and privileged-level EXEC	SR
show isis database	Displays the IS-IS link-state database.	User-level EXEC and privileged-level EXEC	SR
show isis hostname-table	Displays the router-name-to-system-ID mapping table entries for an IS-IS router.	User-level EXEC and privileged-level EXEC	SR
show isis interface	Displays information about the IS-IS interfaces.	User-level EXEC and privileged-level EXEC	SR

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
show isis ip route	Displays the Intermediate IS-IS RSPF route for IS-IS learned routes.	User-level EXEC and privileged-level EXEC	SR
show isis ip rspf route	Displays the Intermediate IS-IS RSPF route for IS-IS learned routes.	User-level EXEC and privileged-level EXEC	SR
show isis memory	Displays memory usage information for an IS-IS instance.	User-level EXEC and privileged-level EXEC	SR
show isis process	Displays summary information about an IS-IS instance.	User-level EXEC and privileged-level EXEC	SR
show isis rrm	Displays IS-IS RRM[18] information.	User-level EXEC and privileged-level EXEC	SR
show isis spf-log	Displays how often and why the router has run a full SPF[19] calculation.	User-level EXEC and privileged-level EXEC	SR
show isis srm	Displays SRM[20] information for an IS-IS process.	Privileged-level EXEC	SR
show isis ssn	Displays SSN[21] information for an IS-IS process.	User-level EXEC and privileged-level EXEC	SR
show key chain	Displays the key chains in the system.	User-level EXEC and privileged-level EXEC	SR
show lacp	Displays LACP information.	User-level EXEC and privileged-level EXEC	All
show logging	Displays the system logging configuration.	User-level EXEC and privileged-level EXEC	All
show movie-streamer	Displays the Movie Streamer configuration.	User-level EXEC and privileged-level EXEC	SE
show multicast	Displays whether or not the multicast sender and receiver are enabled.	User-level EXEC and privileged-level EXEC	SE
show ntp	Displays the Network Time Protocol configuration status.	User-level EXEC and privileged-level EXEC	All
show processes	Displays the process status.	User-level EXEC and privileged-level EXEC	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
show programs	Displays the scheduled programs.	User-level EXEC and privileged-level EXEC	SE
show radius-server	Displays the RADIUS server information.	User-level EXEC and privileged-level EXEC	All
show rcp	Displays RCP information	User-level EXEC and privileged-level EXEC	All
show rtsp	Displays the RTSP configurations.	User-level EXEC and privileged-level EXEC	SE
show rule	Displays the Rules Template configuration information.	User-level EXEC and privileged-level EXEC	SE
show running-config	Displays the current operating configuration.	User-level EXEC and privileged-level EXEC	All
show service-router	Displays the Service Router configuration.	User-level EXEC and privileged-level EXEC	All
show services	Displays the services-related information.	User-level EXEC and privileged-level EXEC	All
show snmp	Displays the SNMP parameters.	User-level EXEC and privileged-level EXEC	All
show srp database	Displays the descriptor-related information saved in the descriptor database.	Privileged-level EXEC	SR
show srp leafset	Displays SRP leafset information.	Privileged-level EXEC	SR
show srp memory	Displays SRP memory usage information.	Privileged-level EXEC	SR
show srp multicast database	Displays multicast database information for an SRP process.	Privileged-level EXEC	SR
show srp neighbor	Displays SRP neighbor information.	Privileged-level EXEC	SR
show srp process	Displays the basic configurations for SRP.	Privileged-level EXEC	SR
show srp replica-set	Displays the replica-set information for a Proximity Engine.	Privileged-level EXEC	SR

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
show srp route	Displays route information for a Proximity Engine to its neighbor nodes on the same DHT network.	Privileged-level EXEC	SR
show srp subscribers	Displays SRP multicast group subscriber information.	Privileged-level EXEC	SR
show ssh	Displays the Secure Shell status and configuration.	User-level EXEC and privileged-level EXEC	All
show standby	Displays the information related to the standby interface.	User-level EXEC and privileged-level EXEC	All
show startup-config	Displays the startup configuration.	User-level EXEC and privileged-level EXEC	All
show statistics aaa	Displays accounting, authentication, and authorization statistics.	User-level EXEC and privileged-level EXEC	All
show statistics access-lists 300	Displays the access control list statistics.	User-level EXEC and privileged-level EXEC	SE
show statistics acquirer	Displays the SE acquirer delivery service statistics.	User-level EXEC and privileged-level EXEC	SE
show statistics admission	Displays admission control statistics.	User-level EXEC and privileged-level EXEC	SE, CDSM
show statistics authsvr	Displays the Authentication Server statistics.	User-level EXEC and privileged-level EXEC	SE
show statistics cdn-select	Displays the statistics for the CDN Selector.	User-level EXEC and privileged-level EXEC	SR
show statistics cdnfs	Displays the SE Internet Streamer CDS network file system statistics.	User-level EXEC and privileged-level EXEC	SE
show statistics content-mgr	Displays the Content Manager statistics.	User-level EXEC and privileged-level EXEC	SE
show statistics distribution	Displays the simplified statistics for content distribution components.	User-level EXEC and privileged-level EXEC	SE
show statistics flash-media-streaming	Displays the statistics for Flash Media Streaming.	User-level EXEC and privileged-level EXEC	SE

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
show statistics icmp	Displays the Internet Control Message Protocol statistics.	User-level EXEC and privileged-level EXEC	All
show statistics ip	Displays the Internet Protocol statistics.	User-level EXEC and privileged-level EXEC	All
show statistics isis	Displays IS-IS traffic counters.	User-level EXEC and privileged-level EXEC	SR
show statistics movie-streamer	Displays statistics for the Movie Streamer.	User-level EXEC and privileged-level EXEC	SE
show statistics netstat	Displays the Internet socket connection statistics.	User-level EXEC and privileged-level EXEC	All
show statistics radius	Displays the RADIUS authentication statistics.	User-level EXEC and privileged-level EXEC	All
show statistics replication	Displays the delivery service replication status and related statistical data.	User-level EXEC and privileged-level EXEC	CDSM, SR
show statistics service-router	Displays the Service Router statistics.	User-level EXEC and privileged-level EXEC	SR
show statistics services	Displays the services statistics.	User-level EXEC and privileged-level EXEC	All
show statistics snmp	Displays the SNMP statistics.	User-level EXEC and privileged-level EXEC	All
show statistics srp	Displays SRP statistics information.	Privileged-level EXEC	SR
show statistics tacacs	Displays the Service Engine TACACS+ authentication and authorization statistics.	User-level EXEC and privileged-level EXEC	All
show statistics tcp	Displays the Transmission Control Protocol statistics.	User-level EXEC and privileged-level EXEC	All
show statistics transaction-logs	Displays the transaction log export statistics.	User-level EXEC and privileged-level EXEC	SE
show statistics udp	Displays the User Datagram Protocol statistics.	User-level EXEC and privileged-level EXEC	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
show statistics web-engine	Displays the Web Engine statistics.	User-level EXEC and privileged-level EXEC	SE
show statistics wmt	Displays the Windows Media Technologies statistics.	User-level EXEC and privileged-level EXEC	SE
show tacacs	Displays TACACS+ authentication protocol configuration information.	User-level EXEC and privileged-level EXEC	All
show tech-support	Displays the system information for Cisco technical support.	User-level EXEC and privileged-level EXEC	All
show telnet	Displays the Telnet services configuration.	User-level EXEC and privileged-level EXEC	All
show transaction-logging	Displays the transaction logging information.	User-level EXEC and privileged-level EXEC	SE
show url-signature	Displays the URL signature information.	User-level EXEC and privileged-level EXEC	SE
show user	Displays the user identification number and username information.	User-level EXEC and privileged-level EXEC	All
show users	Displays the specified users.	User-level EXEC and privileged-level EXEC	All
show version	Displays the software version.	User-level EXEC and privileged-level EXEC	All
show web-engine	Displays the Web Engine information.	User-level EXEC and privileged-level EXEC	SE
show wmt	Displays the WMT configuration.	User-level EXEC and privileged-level EXEC	SE
shutdown (interface configuration)	Shuts down the specified interface.	Interface configuration	All
shutdown (EXEC)	Shuts down the device (stops all applications and operating system).	Privileged-level EXEC	All
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

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
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 an SNMPv2[22] MIB view.	Global configuration	All
splunk-uf-monitor	Configure Splunk Universal Forwarder monitoring,	Global configuration	SE, SR
ss	Dumps socket statistics.	Privileged-level EXEC	SE
sshd	Configures the SSH service parameters.	Global configuration	All
streaming-interface	Configures the streaming interface.	Global configuration	SE
sysreport	Saves the sysreport to 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
tcpmon	Searches all TCP connections.	Privileged-level EXEC	SE
tcp timestamp	Enables and disables TCP timestamp.	Global configuration	All
telnet	Starts the Telnet client.	User-level EXEC and privileged-level EXEC	All
telnet enable	Enables the Telnet services.	Global configuration	All
terminal	Sets the terminal output commands.	User-level EXEC and privileged-level EXEC	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
test-url	Tests the accessibility of a URL using FTP, HTTP, or HTTPS.	User-level EXEC and privileged-level EXEC	SE, SR
top	Displays a dynamic real-time view of a running CDS.	Privileged-level EXEC	All
traceroute	Traces the route to a remote host.	User-level EXEC and privileged-level EXEC	All
traceroute srp	Traces the route of the SRP ring.	User-level EXEC and privileged-level EXEC	SR
traceroute6	Traces the route to a remote IPv6-enabled host.	User-level EXEC and privileged-level EXEC	SE, SR
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 and privileged-level EXEC	All
type-tail	Displays the last several lines of a file.	User-level EXEC and privileged-level EXEC	All
undebug	Disables debugging functions.	Privileged-level EXEC	All
url-signature	Configures the URL signature.	Global configuration	SE
username	Establishes the username authentication.	Global configuration	All
web-engine (EXEC)	Configures the Web Engine.	User-level EXEC	SE
web-engine (Global configuration)	Configures the Web Engine caching parameters and disables revalidation.	Global configuration	SE
whoami	Displays the current user's name.	User-level EXEC and 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. NSSA = not-so-stubby area

2. WMT = Windows Media Technologies
3. MOTD = message-of-the-day
4. CDNFS = CDS network file system
5. CMS = centralized management system
6. Commands used to access configuration modes.
7. SSH = secure shell
8. Link Aggregation Control Protocol
9. syslog = system logging
10. MTU = maximum transmission unit
11. NET = network entity title
12. CLNS = Connectionless Network Service
13. OSPF = Open Shortest Path First
14. Network-attached Storage
15. FTP = File Transfer Protocol
16. LSAs = link-state advertisements
17. RSPF = reverse shortest path first
18. RRM = received routing message
19. SPF = Shortest Path First
20. SRM = send routing message
21. SSN = send sequence number
22. SNMPv2 = SNMP Version 2

aaa

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

aaa {**accounting** {**commands** {**0** {**start-stop tacacs +** | **stop-only tacacs+**} | **15** {**start-stop tacacs +** | **stop-only tacacs+**}} | **exec** {**start-stop tacacs +** | **stop-only tacacs+**} | **system** {**start-stop tacacs +** | **stop-only tacacs+**}} | **authentication** {**enable** {**primary** | **secondary** | **tertiary**} | **radius** {**primary** | **secondary** | **tertiary**} | **tacacs+** {**primary** | **secondary** | **tertiary**}} | **login** {**fail-over server-unreachable** | **local** {**primary** | **secondary** | **tertiary**} | **radius** {**primary** | **secondary** | **tertiary**} | **tacacs+** {**primary** | **secondary** | **tertiary**}} | **authorization** {**commands** {**0 tacacs+** [**if-authenticated**] | **15 tacacs+** [**if-authenticated**]} | **config-commands** | **console** | **exec** {**local** {**primary** | **secondary** | **tertiary**} | **radius** {**primary** | **secondary** | **tertiary**} | **tacacs+** {**primary** | **secondary** | **tertiary**}}}}

no aaa {**accounting** {**commands** {**0** {**start-stop tacacs +** | **stop-only tacacs+**} | **15** {**start-stop tacacs +** | **stop-only tacacs+**}} | **exec** {**start-stop tacacs +** | **stop-only tacacs+**} | **system** {**start-stop tacacs +** | **stop-only tacacs+**}} | **authentication** {**enable** {**enable** {**primary** | **secondary** | **tertiary**} | **radius** {**primary** | **secondary** | **tertiary**} | **tacacs+** {**primary** | **secondary** | **tertiary**}} | **login** {**fail-over server-unreachable** | **local** {**primary** | **secondary** | **tertiary**} | **radius** {**primary** | **secondary** | **tertiary**} | **tacacs+** {**primary** | **secondary** | **tertiary**}} | **authorization** {**commands** {**0 tacacs+** [**if-authenticated**] | **15 tacacs+** [**if-authenticated**]} | **config-commands** | **console** | **exec** {**local** {**primary** | **secondary** | **tertiary**} | **radius** {**primary** | **secondary** | **tertiary**} | **tacacs+** {**primary** | **secondary** | **tertiary**}}}}

Syntax Description

accounting	Sets the Accounting configurations parameters.
commands	Configures exec (shell) commands.
0	Enables level for normal user.
start-stop	Records start and stop without waiting.
tacacs+	Uses Tacacs+ hosts for accounting.
stop-only	Records stop when service terminates.
15	Enables level for super user.
exec	Starts an exec (shell).
system	Configures System events.
authentication	Sets the Authentication configurations parameters.
enable	Sets authentication for enable.
enable	Uses enable password for authentication.
primary	Sets authentication method as primary.
secondary	Sets authentication method as secondary.
tertiary	Sets authentication method as tertiary.
radius	Uses Radius hosts for authentication.
tacacs+	Uses Tacacs+ hosts for authentication.
login	Sets authentication for logins.
fail-over	Specifies a condition to switch to a local authentication scheme.
server-unreachable	Fail-over if server is unreachable.

local	Uses local username authentication.
radius	Uses Radius hosts for authentication.
tacacs+	Uses Tacacs+ hosts for authentication.
authorization	Sets the Authorization configurations parameters.
commands	Configures exec (shell) commands.
0	Enables level for normal user.
tacacs+	Uses Tacacs+ hosts for authorization.
15	Enables level for super user.
config-commands	Sets configuration mode commands.
console	Sets all commands on the console line.
local	Uses local username authorization.
primary	Sets authorization method as primary.
secondary	Sets authorization method as secondary.
tertiary	Sets authorization method as tertiary.
radius	Uses Radius hosts for authorization.
tacacs+	Uses Tacacs+ hosts for authorization Tacacs+ hosts for authorization.

Command Defaults

aaa authorization config-commands: disabled

Command Modes

Global configuration

Usage Guidelines

The **aaa accounting commands** command enables accounting using TACACS+ for normal and supper users.

The **aaa accounting exec** command enables accounting records for user EXEC terminal sessions on the Tacacs+ server, including username, date, start, and stop times.

The **aaa accounting system** command enables accounting of the system events, such as system reboot, NIC interface up or down, accounting configuration enabled or disabled, and using TACACS+.

The **aaa authentication login** command enables authentication using TACACS+ or the RADIUS server to determine if the user has access permission on the SE. The local authentication uses the local database for authentication, if configured. This can be enabled to provide a fallback in case of TACACS+ or Radius server failure.

If there are multi-authentication methods configured, the SE tries to authenticating the user through all configured methods, one by one, until one of them succeeds. The authentication order complies with the priority specified (primary, secondary, then tertiary). If the primary is empty, the secondary is considered as primary, and so on.

If the configured TACACS+ or Radius server is unreachable, use the **aaa authentication login fail-over server-unreachable** command to switch off the TACACS+ or Radius server, and enable fail-over to use the local password file for authentication.

The **aaa authentication enable** command enables authentication using TACACS+ or the RADIUS server to determine if the normal user can enter the privileged exec mode. Alternatively, the enable authentication method uses the local database (the enable password) for authentication.

The **aaa authorization** command enables authorization using the TACACS+ server to determine if the specified user can execute commands or not. In case the configured TACACS+ server is unreachable, the **if-authenticated** option can switch off the TACACS+ server and authorization is granted to anyone who is authenticated.

Note The following commands bypass authorization and accounting:

CTRL+C, CTRL+Z, exit, end, and all of configuration commands for entering submode, for example, interface GigabitEthernet 1/0.

The **aaa authorization config-commands** command reestablishes the default created when the **aaa authorization commands** command was issued.

If the **aaa authorization commands level method** command is enabled, all commands, including configuration commands, are authorized using the method specified for the specified user. To bypass the configuration commands, using the **no aaa authorization config-commands** command stops the network access server from attempting configuration command authorization.

After the **no** form of this command is entered, AAA authorization of configuration commands is completely disabled. Take care before entering the **no** form of this command because it potentially reduces the amount of administrative control on configuration commands.

Use the **aaa authorization config-commands** command if, after using the **no** form of this command, you need to reestablish the default set by the **aaa authorization commands** level method command.

Note This command is disabled by default. You get the same result if you (1) do not configure this command, or (2) configure the **no aaa authorization config-commands**.

The **aaa authorization console** command applies authorization to a console. To disable the authorization, use the **no** form of this command.

The **no aaa authorization console** command is the default, and the authorization that is configured on the console line always succeeds. If you do not want the default, you need to configure the **aaa authorization console** command.

The **aaa authorization exec** command enables authorization using the TACACS+ or RADIUS server to determine if the user can startup an exec (shell). The local authentication uses the local database for authorization, if configured. This can be enabled to provide a fallback in case the TACACS+ or Radius server fails.

If you are trying to disable the **aaa authorization exec** command, at least one authorization method must be selected (local is the default). At least one authentication method must be selected for login.

Note As long as the login authentication fail-over is enabled, it is applied to the exec authorization as well. In other words, the local database is used for authorization as well if the remote severs is unreachable.

Examples

The following configures accounting commands for a normal user using Tacacs+ hosts:

```
ServiceEngine(config)# aaa accounting commands 0 start-stop tacacs+
```

The following example enables/disables authentication for login:

```
ServiceEngine(config)# aaa authentication login
```

The following example applies authorization to a console:

```
ServiceEngine(config)# aaa authorization console
```

Related Commands

Command	Description
enable password	Changes the password.
show aaa	Shows the AAA configuration for a different service.
show statistics aaa	Shows the AAA statistics.

access-lists

To configure access control list (ACL) entries, use the **access-lists** command in Global configuration mode. 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 ACL record within the access list.
number	(Optional) Position number within the ACL. The range is from 1 to 4294967294.
groupname	Name of the group that is permitted or denied from accessing the Internet using an SE.
permit	Specifies the permission action.
enable	Enables the ACL.

Command Defaults

None

Command Modes

Global configuration (config) mode.

Usage Guidelines

You can configure group authorization using an ACL only after a user has been authenticated against an LDAP HTTP-request Authentication Server. The use of this list configures group privileges when members of the group are accessing content provided by an 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 an SE. For instance, use the **access-lists 300 deny groupname marketing** command to prevent any user from the marketing group from accessing content through an 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.

The ACL 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 strin*g is a case-sensitive string with mixed-case alphanumeric characters.
- 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.

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

For Windows-based user groups, 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.

Wildcards

The **access-list** command does not use a netmask; it uses a wildcard bitmask. The source and destination IP and wildcard usage is as follows:

- **source_ip**—Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source:
  - Use a 32-bit quantity in four-part dotted decimal format.
  - Use the **any** keyword => source and source-wildcard of 0.0.0.0 255.255.255.255.
  - Use the **host** keyword => specific source and source_wildcard equal 0.0.0.0.
- **source-wildcard**—Wildcard bits to be applied to source. Each wildcard bit set to 0 indicates the corresponding bit position in the source. Each wildcard bit set to 1 indicates that both a 0 bit and a 1 bit in the corresponding position of the IP address of the packet is considered a match to this access list entry.

  To specify the source wildcard, use a 32-bit quantity in four-part dotted decimal format. Place 1s in the bit positions you want to ignore.

Note Wildcard bits set to 1 need not be contiguous in the source wildcard. For example, a source wildcard of 0.255.0.64 would be valid.

Examples

The following example shows how to display the configuration of the ACL 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 acme1
    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 ACL 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 ACL by using the **clear statistics access-lists 300** command:

```
ServiceEngine# clear statistics access-lists 300
ServiceEngine(config)# access-lists 300 permit groupname acme1 position 2
```

Related Commands

Command	Description
show access-lists 300	Displays the ACL configuration.
show statistics access-list 300	Displays the ACL statistics.

acquirer (EXEC)

To start or stop content acquisition on a specified acquirer delivery service, use the **acquirer** command in EXEC configuration mode. 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 the Last-Modified-Time attributes in the local time format.
delivery-service-id	(Optional) Sets the delivery service number identifier.
delivery-service-num	(Optional) Delivery service number. The range is from 0 to 4294967295.
delivery-service-name	(Optional) Sets the delivery service name descriptor.
delivery-service-name	(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.
url	URL to be tested. **Note** For the 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 (SE) is tested. Use this option only when the HTTP protocol is used.
url	(Optional) 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.
smb-options	(Optional) 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.

Command Defaults

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

Command Modes

EXEC configuration mode.

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.

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 Content Acquirer unless you specify the delivery service ID or name.

SEs 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* command in EXEC configuration mode to test whether a URL is accessible or not. The actual content is dumped into the /dev/null path.

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

Command	Description
show acquirer	Displays the acquirer delivery service information and progress for a specified delivery service number or name.
show statistics acquirer	Displays the SE acquirer delivery service statistics.

acquirer (Global configuration)

To provide authentication when the acquirer obtains content through a proxy server, use the **acquirer** command in Global configuration mode. 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 that the acquirer can obtain content through a proxy server.
outgoing	Enables authentication for a nontransparent proxy server.
hostname	Hostname of a nontransparent proxy server.
ip-address	IP address of a nontransparent proxy server.
port-num	Port number of a nontransparent proxy server. The range is from 1 to 65535.
username	Username for authentication using a maximum of 256 characters.
password	Allows the use of a password for authentication.
password	Password for authentication using a maximum of 256 characters.

Command Defaults

None

Command Modes

Global configuration (config) mode.

Usage Guidelines

Use the **acquirer proxy authentication outgoing** Global configuration command to configure authentication when you enable content acquisition through a proxy server. 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 fails.

Acquisition through a proxy server can be configured when the Content Acquirer 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 Content Acquirer 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. If you need to configure the SE to use the proxy for both caching and prepositioned 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 prepositioned 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 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 Content Acquirer 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* command in Global configuration mode in the Content Acquirer 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, the message "`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

Command	Description
http proxy outgoing	Configures an SE to direct all HTTP miss traffic to a parent cache.
show acquirer	Displays the acquirer delivery service information and progress for a specified delivery service number or name.

acquisition-distribution

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

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.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

When you use the **acquisition-distribution database-cleanup** command, the acquisition and distribution database is checked to ensure that all prepositioned content is available in Cisco Network File System (CDNFS). If any prepositioned content is found to be missing from CDNFS, the content is replicated to all SEs in the Internet Streamer CDS network. Content Acquirers 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 shows how to start the acquisition and distribution database cleanup process:

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

The following example shows how to start the acquisition and distribution process:

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

The following example shows how to stop the acquisition and distribution process:

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

Related Commands

Command	Description
cdnfs cleanup	Cleans up the content of deleted channels from the acquisition and distribution database.

show acquirer	Displays the acquirer delivery service information and progress for a specified delivery service number or name.
show distribution	Displays the distribution information for a specified delivery service.

alarm

To configure alarms, use the **alarm** command in Global configuration mode. To disable alarms, use the **no** form of this command.

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

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

Syntax Description

admin-shutdown-alarm	Generates a linkdown alarm when an interface shuts down.
enable	Enables admin shutdown alarm overload detection.
overload-detect	Specifies alarm overload configuration.
clear	Specifies the threshold below which the alarm overload state on an SE is cleared and the Simple Network Management Protocol (SNMP) traps and alarm notifications to the Centralized Management System (CMS) resume. **Note** The **alarm overload-detect clear** command 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	Enables the detection of alarm overload situations.

Command Defaults

admin-shutdown-alarm: disabled

raise: 10 alarms per second

clear: 1 alarm per second

Command Modes

Global configuration (config) mode.

Usage Guidelines

The **alarm admin-shutdown-alarm** command must be enabled for an admin-shutdown alarm to take effect. If an admin-shutdown alarm occurs, disabling this option does not clear the outstanding alarm properly. There are two ways to avoid this situation:

- Clear the outstanding admin-shutdown alarm first before disabling this option.
- Disable this option and reboot, which clears this alarm.

When multiple applications running on an SE experience problems at the same time, numerous alarms are set off simultaneously, and an SE may stop responding. Use the **alarm overload-detect** 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, an SE enters an alarm overload state until the number of alarms drops down to the number defined in the **clear**.

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

- 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.
- Alarm overload clear notification is sent.
- 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 an SE. The **show alarms** and **show alarms history** command in EXEC configuration modes display all the alarms even in the alarm overload state.

Examples

The following example shows how to generate a linkdown alarm when an interface shuts down:

```
ServiceEngine(config)# alarm admin-shutdown-alarm enable
```

The following example shows how to enable the detection of alarm overload:

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

The following example shows how to set the threshold for triggering the alarm overload at 100 alarms per second:

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

The following example shows how to set the level for clearing the alarm overload at 10 alarms per second:

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

Related Commands

Command	Description
show alarms	Displays information on various types of alarms, their status, and history.
show alarm status	Displays the status of various alarms and alarm overload settings.

area nssa

To configure an area as a not-so-stubby area (NSSA), use the **area nssa** router configuration command. To remove the NSSA distinction from the area, use the **no** form of this command.

area *area-id* **nssa**

no area *area-id* **nssa**

Syntax Description

area-id	Identifier of the area for which authentication is to be enabled. The identifier can be specified as either a decimal value or an IP address (ID range is from 0 to 4294967295).

Command Defaults

No NSSA area is defined.

Command Modes

OSPF configuration (config-ospf) mode.

Usage Guidelines

This command is used to configure an area as a NSSA. The area ID range is given as 0 to 4294967295, but area 0 cannot be configured as an NSSA area.

Examples

In the following example area 1 is configured as an NSSA area:

```
ServiceRouter(config)# router ospf
ServiceRouter(config-ospf)# network 192.168.20.0 0.0.0.255 area 1
ServiceRouter(config-ospf)# area 1 nssa
ServiceRouter(config-ospf)#
```

area stub

To define an area as a stub area, use the **area stub** router configuration command. To disable this function, use the **no** form of this command

area *area-id* **stub**

no area *area-id* **stub**

Syntax Description

area-id	Identifier for the stub area. The identifier can be specified as either a decimal value or an IP address (ID range is from 0 to 4294967295).

Command Defaults

No stub area is defined.

Command Modes

OSPF configuration (config-ospf) mode.

Usage Guidelines

This command is used to define an area as a stub area. The area ID range is given as 0 to 4294967295, but area 0 cannot be configured as a stub area.

Examples

The following example shows how to configure area 1 as a stub area:

```
ServiceRouter(config)# router ospf
ServiceRouter(config-ospf)# network 192.168.20.0 0.0.0.255 area 1
ServiceRouter(config-ospf)# area 1 stub
ServiceRouter(config-ospf)#
```

asset

To configure the CISCO-ENTITY-ASSET-MIB, use the **asset** command in Global configuration mode. 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.
name	Asset tag name string.

Command Defaults

None

Command Modes

Global configuration (config) mode.

Examples

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

```
ServiceEngine(config)# asset tag entitymib
```

authsvr

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

authsvr {**enable** | **location-server** {**cache-timeout** *num* | **primary** *ip addr port num* | **secondary** *ip addr port num*} | **unknown-server allow**}

no authsvr {**enable** | **location-server** {**primary** *ip addr port num* | **secondary** *ip addr port num*} | **unknown-server allow**}

Syntax Description

enable	Enables the Authorization server.
location-server	Configures the geo location server IP address and port.
cache-timeout	Configures the location server cache timeout.
num	Location server cache timeout in seconds. The range is from 1 to 864000.
primary	Configures the primary geo location server IP address and port.
ip addr	IP address of the primary geo location server.
port num	Port number of the primary geo location server.
secondary	Configures the secondary geo location server IP address and port.
ip addr	IP address of the secondary geo location server.
port num	Port number of the secondary geo location server.
unknown-server	Configures the Authorization server unknown server or domain.
allow	Allows requests for an unknown server or domain.

Command Defaults

authsvr: enabled

cache-timeout: 691200 seconds or 8 days.

unknown-server: blocked

Command Modes

Global configuration (config) mode.

Usage Guidelines

Changing the primary or secondary Geo-Location server configuration requires a restart of the authsvr for the configuration change to take effect. To restart the authsvr, disable it by entering the **no authsvr enable** and then re-enable it by entering the **authsvr enable** command.

The **no authsvr unknown-server allow** command causes all blocked requests to increment the authsvr block statistic.

Examples

The following example shows how to enable the Authorization server:

```
ServiceEngine(config)# authsvr enable
Authserver is enabled
```

Related Commands

Command	Description
debug authsvr	Debugs the Autnentication Server.
debug authsvr error	Sets the debug level to error.
debug authsvr trace	Sets the debug level to trace.
show authsvr	Display the status of the Authorization server.
show statistics authsvr	Displays the Authentication Server statistics.

bandwidth (Global configuration)

To set an allowable bandwidth usage limit and its duration for Cisco Streaming Engine Windows Media Technology (WMT) streaming media, use the **bandwidth** command in Global configuration mode. 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.
bandwidth	Bandwidth size for the Movie Streamer, in kbps. The range is from 0 to 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.
day	Day of the week.
hour	Time to start (hh:mm). The range is from 00 to 23:00 to 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 2-45.

Command Defaults

None

Command Modes

Global configuration (config) mode.

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 prepositioned 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 the 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** commands enable you to specify a WMT incoming and an outgoing bandwidth as follows:

- Use the **bandwidth wmt outgoing** *kbits* command in Global configuration mode to specify the outgoing WMT bandwidth in kbps. This command sets the maximum bandwidth for the WMT content that can delivered to a client that is requesting WMT content. The range of values is between 0 and 2,147,483,647 kbps.

  If the specified outgoing bandwidth is above the limit specified by the WMT license, then a warning message is displayed. 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 may be changed to a higher value at a later time.

- Use the **bandwidth wmt incoming** *kbits* command in Global configuration mode to specify the incoming WMT bandwidth in kbps. This command sets the maximum bandwidth for the WMT content that can delivered to the 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 and 2,147,483,647 kbps. The incoming bandwidth applies to VoD content from the origin server for a cache miss.

Related Commands

Command	Description
bandwidth (interface configuration)	Sets the specified interface bandwidth to 10, 100, or 1000 Mbps.
interface	Configures a Gigabit Ethernet or port channel interface. Provides access to interface configuration mode.
show bandwidth	Displays the bandwidth allocated to a particular device.
show interface	Displays the hardware interface information.
show running-config	Displays the current operating configuration.
show startup-config	Displays the startup configuration.

bandwidth (interface configuration)

To configure an interface bandwidth, use the **bandwidth** command in interface configuration mode. 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.

Command Defaults

None

Command Modes

Interface configuration (config-if) mode.

Usage Guidelines

The bandwidth is specified in Mbps. The **1000** Mbps option is not available on all ports. On an SE model that has an optical Gigabit Ethernet interface, you cannot change the bandwidth of this interface. Therefore, Gigabit Ethernet interfaces run only 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 applies 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

Command	Description
interface	Configures a Gigabit Ethernet or port channel interface. Provides access to interface configuration mode.

banner

To configure the EXEC, login, and message-of-the-day (MOTD) banners, use the **banner** command in Global configuration mode. 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.
line	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.
message_text	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.
line	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.
message_text	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.
line	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.
message_text	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.

Command Defaults Banner support is disabled by default.

Command Modes Global configuration (config) mode.

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

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

Note All 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** command to enable banner support on the SE. Enter the **show banner** command in EXEC configuration mode 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** 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** 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** 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 the 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 sees 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 configuration mode CLI prompt is displayed:

```
ServiceEngine#
```

Related Commands

Command	Description
show banner	Enables banner support on the SE.

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** command in Global configuration mode. 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 kbps, for the Movie Streamer.
bitrate	Bit rate in kbps. The range is from 1 to 2147483647.
wmt	Configures the bit rate, in kbps, for large files sent using the WMT protocol.
incoming	Sets the incoming bit-rate settings.
bitrate	Incoming bit rate, in kbps. The range is from 0 to 2147483647.
outgoing	Sets the outgoing bit-rate settings.
bitrate	Outgoing bit rate, in kbps. The range is from 0 to 2147483647.

Command Defaults

movie-streamer *bitrate*: 1500 kbps

wmt incoming *bitrate*: 0 (no limit)

wmt outgoing *bitrate*: 0 (no limit)

Command Modes

Global configuration (config) mode.

Usage Guidelines

The WMT proxy 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** commands enable you to specify a WMT incoming and outgoing per session bit rate as follows:

- Use the **bitrate wmt incoming** *bitrate* command to specify the maximum incoming streaming bit rate per session that can be delivered to the WMT proxy server (the 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 and 2,147,483,647 kbps. The default value is 0 (no bit-rate limit).
- Use the **bitrate wmt outgoing** *bitrate* command to set the maximum outgoing streaming bit rate per session that can delivered to a client requesting WMT content. The specified bit rate is the maximum outgoing WMT per session bit rate). The range of values is between 0 and 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** 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 retrieves only 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

Command	Description
show wmt	Displays the WMT configuration.

blink

To identify physical devices by blinking their LED(s), use the **blink** command in EXEC configuration mode.

blink {**disk** *name* | **interface {GigabitEthernet** *slot/port_num* | **TenGigabitEthernet** *slot/port_num*}}

Syntax Description

disk	Flash disk LED for 3s.
name	disk name (format is disk00).
interface	Flash network interface port LED for 3s.
GigabitEthernet	Selects a Gigabit Ethernet interface.
slot/port_num	Slot and port number for the selected interface. The slot range is from 1 to 14; the port range is from 0 to 0. The slot number and port number are separated with a forward slash character (/).
TenGigabitEthernet	Selects a Ten Gigabit Ethernet interface.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The **blink disk** command submits IO to a disk, do not use this command in systems with live traffic.

Examples

The following example shows how to blink a disk:

```
ServiceRouter# blink disk disk00
Blinking disk00 LED for 3 seconds
```

The following example shows how to blink a GigabitEthernet interface:

```
ServiceRouter# blink interface gigabitEthernet 1/0
Blinking eth0 LED for 3 seconds
```

bootstrap-node

To configure a bootstrap node IP address, use the **bootstrap-node** Service Routing Protocol (SRP) configuration command. To remove a bootstrap node address, use the **no** or **default** form of the command.

bootstrap-node *ip-address*

[**no** | **default**] **bootstrap-node** *ip-address*

Syntax Description

ip-address	Valid IP address for the bootstrap node. IP addresses 0.0.0.0 and 255.255.255.255 are not valid addresses for a bootstrap node.

Command Defaults

No bootstrap node address is configured.

Command Modes

SRP configuration (config-srp) mode.

Usage Guidelines

This command is used to set bootstrap nodes for an SRP. A Proximity Engine specifies one or more bootstrap nodes to join a DHT network. In a DHT network, the domain ID of the bootstrap nodes and the Proximity Engine must the same.

The first Proximity Engine in the network, which acts as the bootstrap node for others, does not have to configure the bootstrap node address itself. This is the only exception to configuring bootstrap nodes. All other nodes need to configure a bootstrap node address before they can join any network.

The **no** and **default** forms of the command remove a given bootstrap node from the list of available bootstrap nodes of a Proximity Engine. The port number for bootstrap node is 9000. The **show srp process** command lists configured bootstrap nodes.

A Proximity Engine cannot be its own bootstrap node. A maximum 25 bootstrap nodes are allowed.

Examples

The following example shows how to configure a bootstrap node address with the **bootstrap-node** command:

```
ServiceRouter# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ServiceRouter(config)# router srp
ServiceRouter(config-srp)# bootstrap-node 192.168.6.91
ServiceRouter(config-srp)# end
ServiceRouter#
```

The following example shows how the **show srp process** command displays configured bootstrap nodes:

```
ServiceRouter# show srp process

Process:
  Domain: 0
  Node Id: 6b05858ab28345e62e9e614a48e1206445ec9ca0884fa0e827c1072f5fe8c5f5
Port: 9000
  Interfaces running SRP:
```

```
     *GigabitEthernet 1/0
Database Mirroring: Disabled
  # of storages requested for mirroring: 2
  # of storages used for mirroring     : 1
...

ServiceRouter#
```

Related Commands

Command	Description
domain	Sets the domain ID for the SRP.
router srp	Enters SRP configuration mode.
show srp process	Displays the basic configurations for SRP.

cache

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

cache content {**eviction-preferred-size** {**small** | **large**} | **eviction-protection** {**min-size-100MB** {**min-duration-1hr** | **min-duration-2hr** | **min-duration-3hr** | **min-duration-4hr**}| **min-size-1GB** {**min-duration-1hr** | **min-duration-2hr** | **min-duration-3hr** | **min-duration-4hr**} | **min-size-4GB** {**min-duration-1hr** | **min-duration-2hr** | **min-duration-3hr** | **min-duration-4hr**} | **min-size-500MB** {**min-duration-1hr** | **min-duration-2hr** | **min-duration-3hr** | **min-duration-4hr**}}| **max-cached-entries** *num*

Syntax Description

content	Configures the cached contents.
eviction-preferred-size	Configures cache content eviction preferred.
large	Selects cache content eviction preferred size (Retain smaller objects).
small	Selects cache content eviction preferred size (Retain larger objects).
eviction-protection	Configures the eviction protection.
min-size-100MB	Minimum cache entry size to protect.
min-duration-1hr	Minimum duration to protect the content from eviction.
min-duration-2hrs	Minimum duration to protect the content from eviction.
min-duration-3hrs	Minimum duration to protect the content from eviction.
min-duration-4hrs	Minimum duration to protect the content from eviction.
min-size-1GB	Minimum cache entry size to protect.
min-size-4GB	Minimum cache entry size to protect.
min-size-500MB	Minimum cache entry size to protect.
max-cached-entries	Cleans up the unwanted entries in the CDNFS.
num	Max cached entries. The range is from 1 to 20000000.

Command Defaults

The max-cached-entries default is 2000000 entries.

Command Modes

Global configuration (config) mode.

Usage Guidelines

The Content Manager manages the caching, storage, and deletion of content.

Current priority favors small objects. The **cache content eviction-preferred size** command allows users to configure a preference for small or large objects in the Content Manager. Once a preference is specified, it only applies on contents made after the configurative; contents prior to configuration remain unchanged.

Addition and Deletion Processes

Previously, the Internet Streamer CDS software did not restrict adding new content to CDNFS as long as there was enough disk space for the asset. The **cache content max-cached-entries** command restricted the number of assets, but it was not a hard limit. New content was always added and the CDS

would delete old content in an attempt to keep within the limits configured. The CDS could actually have more content than the configured limit, because the process to delete content is slower than the process to add content. The same situation applies to disk-usage based deletion, where deletion occurs when 90 percent of the CDNFS is used.

Content addition stops at 105 percent of the maximum object count or 95 percent of the CDNFS capacity (disk usage). For example, if the maximum number of objects has been configured as 20 million (which is the default value), the CDS starts deleting content if the object count reaches 20 million, but adding content is still allowed. Adding content stops when the maximum number of content objects reaches 21 million (105 percent of 20 million), which allows time for the content deletion process to reduce the number of objects in the CDS to the configured limit. Adding content resumes only after the number of objects is 20 million or less. The same logic applies to disk usage. The deletion process starts when disk usage reaches 93 percent, adding content stops when disk usage reaches 98 percent, and adding content resumes only after the disk usage percentage reaches 95 percent or less.

Note We recommend that any CDE model that has hard-disk drives (HDDs) (instead of solid-state drives [SDDs]), and is used to stream ABR content, be configured with a maximum of 5 million objects instead of the default of 20 million. This is because HDD-based hardware requires more seek time to access content. The software can handle 20 million objects, but the hard-drive access time impacts the ABR streaming performance. ABR content consists of a large number of small files, which results in a lot of overhead.

For long-tail content (Windows Media Streaming, Flash Media Streaming, Movie Streamer, and progressive download), the maximum number of content objects can be configured with the default of 20 million on the HDD-based hardware models. Two of the HDD-based hardware models are the CDE220-2G2 and CDE250-2M0.

If adding content has been stopped because either the content count reached 105 percent of the limit or the disk usage reached 98 percent of capacity, the un-writable flag is set in the share memory and when the protocol engine calls create, FastCAL library looks into the share memory and denies the creation request. The protocol engine performs a bypass or cut-through operation.

The **show cdnfs usage** command shows the current status of whether the content is able to be cached or not. Following is an example of the output:

```
ServiceEngine# show cdnfs usage
Total number of CDNFS entries  :    2522634
Total space                    :     4656.3 GB
Total bytes available          :     4626.0 GB
Total cache size               :        2.4 GB
Total cached entries           :    2522634
Cache-content mgr status       : Cachable
Units: 1KB = 1024B; 1MB = 1024KB; 1GB = 1024MB
```

If the maximum object count is reached, the following is displayed:

```
Cache-content mgr status:  Not cacheable on the following disk(s): [/disk00-06]
[/disk01-06] [/disk02-01]
105% of max obj count reached :        [/disk00-06] [/disk01-06] [/disk02-01]
```

If the disk usage reaches more than 98 percent, the following is displayed:

```
Cache-content mgr status:  Not cacheable on the following disk(s): [/disk01-06]
[/disk02-01]
98% of disk usage reached:       [/disk01-06] [/disk02-01]
```

Eviction Protection

The Content Manager provides configurable eviction protection for some content. The Content Manager eviction algorithm is triggered when the disk usage reaches 93 percent or when the cached object count reaches the configured maximum object count. The eviction algorithm assigns a priority number to each content object based on an algorithm similar to the greedy-dual-size-frequency (GDSF) algorithm. The priority number is based on the size and usage of the object. Small objects are given preference over large objects; that is, they are less likely to be deleted.

To protect incoming large objects from getting a low priority and being deleted, use the **cache content eviction-protection global configure** command. The **cache content eviction-protection** command allows you to set the minimum content size (100 MB, 500 MB, 1 GB, and 4 GB) and the minimum age (1-4 hours for 100 MB size, 1, 4, 8, or 24 hours for all other sizes) of the content object to be protected from deletion. For example, to set the eviction protection for content objects larger than 100 MB that were ingested in the last two hours, you would enter the following command:

```
ServiceEngine(config)# cache content eviction-protection min-size-100MB min-duration-2hrs
```

If the content object being cached is larger than the configured size, it is inserted into a protection table along with the current time stamp. If the difference between the object's time stamp and the current time is greater than the configured time duration, the object is removed from the protection table. If the eviction algorithm is triggered, before it selects an object for deletion, it first looks at the protection table, and if the object is found, it is skipped for that iteration. The **clear-cache-content** command also checks the protection table before deleting an object. The **clear-cache-all** command does not check the eviction protection table; cache content is just deleted. As for relative cache content, content in the protection table might still be deleted if the relative content that is not protected is deleted. The eviction protection is disabled by default.

If the Content Manager eviction algorithm is not able to find any content to delete, a syslog message is sent to notify the administrator to revisit the configuration. Changing the settings of the cache content eviction-protection command only affect the content that are currently in the protection table and any new content that is added. Any object that is removed from the protection table prior to the configuration change is not brought back into the protection table.

Reloading the SE or entering the **no cache content eviction-protection min-size-xx duration-xx** command removes all entries in the eviction protection table.

Note Changing the time on the SE affects the Content Manager eviction process. If the time is set forward, content is deleted sooner than expected. If the time is set back, content is protected longer.

The **show cache content** command displays the eviction protection status and the number of elements in the eviction protection table.

Examples

The following example shows how to configure the cache content:

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

The **show cdnfs usage** command shows the current status of whether the content is able to be cached or not. Following is an example of the output:

```
# show cdnfs usage
Total number of CDNFS entries  :    2522634
Total space                    :     4656.3 GB
Total bytes available          :     4626.0 GB
Total cache size               :        2.4 GB
Total cached entries           :    2522634
```

```
Cache-content mgr status       : Cachable
Units: 1KB = 1024B; 1MB = 1024KB; 1GB = 1024MB
```

If the maximum object count is reached, the following is displayed:

```
Cache-content mgr status       : caching paused[ max count 105% of configured reached ]
```

If the disk usage reaches more than 95 percent, the following is displayed:

```
Cache-content mgr status       : caching paused[ disk max 95% of disk usage reached ]
```

Note When the CDS is started or the cache Content Manager is restarted, it performs a scan of the entire CDNFS. During this period, the deletion starts at 94 percent (not 90 percent) and adding content stops at 95 percent.

Related Commands

Command	Description
show cache	Displays a list of cached contents.

capability

To modify the capability configuration, use the **capability** command in Global configuration mode. 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.
number	The profile ID. The range is from 1 to 65535.
add	(Optional) Adds the capability attributes.
attrib	Adds the capability attributes.
capability-url	Specifies the capability URL.
url	The capability URL string.
user-agent	Specifies the user-agent.
name	The user-agent name.
description	(Optional) Specifies the profile description.

Command Defaults

None

Command Modes

Global configuration (config) mode.

Related Commands

Command	Description
show capability	Displays information for the Cap-X profile ID.

cd

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

cd *directoryname*

Syntax Description

directoryname	Directory name.

Command Defaults

None

Command Modes

EXEC configuration mode.

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:

```
ServiceEngine(config)# cd local1
```

The following example shows how to use an absolute path:

```
ServiceEngine(config)# cd /local1
```

Related Commands

Command	Description
deltree	Deletes a directory and its subdirectories.
dir	Displays the files in a long list format.
lls	Displays the files in a long list format.
ls	Lists the files and subdirectories in a directory.
mkdir	Makes a directory.
pwd	Displays the present working directory.

cdn-select

To enable the CDN Selector for third-party service selection, use the **cdn-select** command in Global configuration mode. To disable the CDN Selector, use the **no** form of this command.

cdn-select enable

no cdn-select enable

Syntax Description

enable	Enables the CDN Selector.

Command Defaults

None

Command Modes

Global configuration (config) mode.

Usage Guidelines

The **cdn-select** command enables the CDN Selector, which provides a method to do third-party service selection based on parameters like content type and geographic location.

Examples

The following example shows how to enable the CDN Selector:

```
ServiceRouter(config)# cdn-select enable
ServiceRouter(config)#
```

The following example shows how to disable the CDN Selector:

```
ServiceRouter(config)# no cdn-select enable
ServiceRouter(config)#
```

Related Commands

Command	Description
geo-location-server	Redirects requests to different Content Delivery Networks based on the geographic location of the client.
show cdn-select	Displays the status of the CDN Selector.
show statistics cdn-select	Displays the statistics for the CDN Selector.

cdnfs

To browse the Internet Streamer CDS network file system (CDNFS), use the **cdnfs browse** command in EXEC configuration mode.

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	Summary information of the garbage entries. No cleanup.
start	Starts the CDNFS garbage collection.
force	Forces removing objections that are in transient states.
stop	Stops the CDNFS garbage collection.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The Internet Streamer CDS CDNFS stores the prepositioned Internet Streamer CDS network content to be delivered by all supported protocols.

Use the **cdnfs browse** command to browse the CDNFS directories and files. It does not display cached content for the Web Engine or Flash Media Streaming. It only caches content for Windows Media Streaming and Movie Streamer, and displays prefetched content. To display cached content, use the **show cache content** command.

```
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 contains information, it lists the websites as directories, and file attributes and content could be viewed using these subcommands.

The **cdnfs cleanup** command, which is used to cleanup unwanted entries in CDNFS, is deprecated in Release 2.6. in the following manner. When an SE is removed from a delivery service, the Content Manager removes all cache content for that delivery service. All prefetched content for that delivery service is removed by the Acquisition and Distribution process. However, if the Acquisition and Distribution process fails because of an SE being offline or for any other reason, then the **cdnfs cleanup** command is still required to remove the prefetched content.

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** command can be used to clean up all UNS content associated with deleted channels.

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

The **cdnfs database recover** command must be run when the cdnfs_db_corrupt alarm is raised. This alarm is raised when the Total Cached entries is more than Total CDNFS entries in the output for the **show cdnfs usage** command:

```
ServiceEngine# show cdnfs usage
Total number of CDNFS entries  :        202
Total space                    :     5037.9 GB
Total bytes available          :     5019.5 GB
Total cache size               :       21.0 GB
Total cached entries           :        218
Cache-content mgr status       : Cachable
 Units: 1KB = 1024B; 1MB = 1024KB; 1GB = 1024MB
```

This occurs generally when an internal bookkeeping file is corrupted. With the server in the offloading status, enter the **cdnfs database recover** command to remove this inconsistency, then reload the server.

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
```

The following example shows the output for the **cdnfs database recover** command:

```
ServiceEngine# cdnfs database recover
CDNFS database inconsistency issue found.
CDNFS database recovery operation would impact existing and new client sessions.
```

```
Recovering database would need device in offloaded state.
Do you want to recover the CDNFS database now (y/n)?
y
Recovering CDNFS database. It may take few minutes.
Please wait...
CDNFS database recovery is complete. Please reload the device now.
ServiceEngine# reload
Proceed with reload? [confirm] yes
Shutting down all services, will timeout in 15 minutes.
reload in progress...
```

Related Commands

Command	Description
show cdnfs	Displays the Internet Streamer CDS network file system information.
show statistics cdnfs	Displays the SE Internet Streamer CDS network file system statistics.

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** command in Global configuration mode. 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.
hostname	Hostname of the CDSM.
ip-address	IP address of the CDSM.
role	Configures the CDSM role to either primary or standby (available only from the CDSM CLI).
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 only from the CDSM CLI).
port	Configures the CDSM GUI port.
port-num	Port number. The range is from 1 to 65535.

Command Defaults

None

Command Modes

Global configuration (config) mode.

Usage Guidelines

You can use the **cdsm ui port** 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 only available on CDSM devices. 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* command when you register the device to the CDSM. If the 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 SIR'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 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** command in EXEC configuration mode 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 shows how to configure 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 shows how to configure a new GUI port to access the CDSM GUI:

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

The following example shows how to configure 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 shows how to configure the standby CDSM with the IP address of the primary CDSM by using the **cdsm ip** *ip-address* 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 cache

To clear the HTTP object cache use the **clear** command in EXEC configuration mode.

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

Syntax Description

all	(Optional) Clears all cached objects.
content	(Optional) Clears cached content.
1-15000	Free space, in Mbytes.
flash-media-streaming	Clears the Flash Media Streaming edge server cached content and DVR cached content.

Command Defaults

Cached content is 1000 Mbytes if not specified.

Command Modes

EXEC configuration mode.

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 **clear cache all** command requests the Content Manager to delete all cache contents. Only one **clear cache all** command can be executed at a time, and the Control-C option is not allowed with this command. During **the clear cache all** operation, the **show cache content** and **show cdnfs usage** outputs display a line about running the **clear cache all** command, and the progress is displayed in the output of these commands.

Caution The **clear cache all** command is irreversible, and all cached content is erased. Cisco does not recommend using this command on production systems.

When the **clear cache content** command is executed, by default, the command evicts 1000MB of content from all disks in the SE. For example, if the SE has 12 disks, then 1000MB/12 = ~83MB content is evicted from each disk. In this case, all content in the SE is 450MB content; therefore, each disk results in a minimum content of 450MB. This causes 450MB * 12 = 5400MB to be evicted. Each disk maintains its own eviction tree, so to avoid this issue, evict each disk separately.

Examples

The following example shows how to clear all cached contents:

```
ServiceEngine# clear cache all
This operation tries to free up all cached contents. Proceed? [yes|NO] yes
Clear cache all operation will stop CMGRSlowScan process running
Starting clear cache all operation, 100 contents will be deleted.
Clear cache all progress: done[100], total[100], progress[100.00%][####################]
Clear cache all finished, duration[3], tps[33.33].
```

Related Commands

Command	Description
cache content	Configures the cached contents.
show cache content	Displays a list of cached contents.
show cdnfs usage	Displays Content Delivery Network (CDN) current usage.

clear content

To clear the content of a Uniform Resource Locator (URL), use the **clear content** command in EXEC configuration mode.

clear content {**last-folder-url** *url* | **url** *url*}

Syntax Description

last-folder-url	Clears all content with a relative diskpath from the given URL without a filename.
url	The valid URL without the filename. Protocol is ignored.
url	Clears cached content with its original URL.
url	The URL for the content object to delete.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The **clear content url** command requests the Fast Content Abstraction Layer (FastCAL) API to delete the content of the specified URL and inform the Content Manager to remove it from its internal data structure.

Examples

The following example shows how to clear the content URL:

1. Verify the URL that is to be deleted from the SE.

```
ServiceEngine# show cache
Max-cached-entries is set as 10000000
Number of cal cached assets: 10
-----------------------------------------------
Priority    Size         URL
-----------------------------------------------
1.87390e+01 64000        http://7.1.200.200/file-1961503
1.87390e+01 64000        http://7.1.200.200/file-1961548
1.87390e+01 64000        http://7.1.200.200/file-1961450
1.87390e+01 64000        http://7.1.200.200/file-1961495
1.87390e+01 64000        http://7.1.200.200/file-1961540
1.87390e+01 64000        http://7.1.200.200/file-1961399
1.87390e+01 64000        http://7.1.200.200/file-1961349
1.87390e+01 64000        http://7.1.200.200/file-1961395
1.87390e+01 64000        http://7.1.200.200/file-1961302
1.87390e+01 64000        http://7.1.200.200/file-1961575
ServiceRouter#
```

2. Clear the URL content from that SE:

```
ServiceEngine# clear content url http://7.1.200.200/file-1961503
```

3. Verify the content is removed from SE:

```
ServiceEngine# show cache
Max-cached-entries is set as 10000000
Number of cal cached assets: 10
-----------------------------------------------
Priority    Size         URL
-----------------------------------------------
1.87390e+01 64000        http://7.1.200.200/file-1961548
1.87390e+01 64000        http://7.1.200.200/file-1961450
1.87390e+01 64000        http://7.1.200.200/file-1961495
1.87390e+01 64000        http://7.1.200.200/file-1961540
1.87390e+01 64000        http://7.1.200.200/file-1961399
1.87390e+01 64000        http://7.1.200.200/file-1961349
1.87390e+01 64000        http://7.1.200.200/file-1961395
1.87390e+01 64000        http://7.1.200.200/file-1961302
1.87390e+01 64000        http://7.1.200.200/file-1961575
1.87390e+01 64000        http://7.1.200.200/file-1961529
ServiceEngine#
```

This example shows how to delete all the contents matching the last-folder-url:

```
ServiceEngine# clear content last-folder-url  http://172.XX.XX.XXX/vod
This operation tries to free up all content which matches last-folder-url.
Proceed?[yes|NO] yes
Content to be deleted:
  url: [http://172.XX.XX.XXX/vod/rab1.flv]
  url: [http://172.XX.XX.XXX/vod/rab2.flv]
  url: [http://172.XX.XX.XXX/vod/119M.flv]
```

clear ip

To clear the IP configuration, use the **clear ip** command in EXEC configuration mode.

On the SE:

clear ip access-list counters [*standard_acl-num* | *extended_acl_num* | *acl-name*]

On the SR:

clear ip access-list counters [*standard_acl-num* | *extended_acl_num* | *acl-name*] | **bgp** {**ip address** | **all**} | **ospf** {**neighbor** {**all** | **GigabitEthernet** *slot/port num* | **PortChannel** *num*} | **rspf route** [*router-id*} | **traffic**}

Syntax Description

access-list	Clears the IP access list statistical information.
counters	Clears the IP access list counters.
standard_acl_num	(Optional) Counters for the specified access list, identified using a numeric identifier. The range is from 1 to 99.
extended_acl_num	(Optional) Counters for the specified access list, identified using a numeric identifier. The range is from 100 to 199
acl-name	(Optional) Counters for the specified access list, identified using an alphanumeric identifier up to 30 characters, beginning with a letter.
bgp	Clears the BGP[1] neighbors.
all	Specifies that all current BGP sessions are reset.
ip-address	Specifies that only the identified BGP neighbor is reset.
ospf	Clears the OSPF[2] tables.
neighbor	Neighbor statistics per interface.
all	Clears all neighbors.
GigabitEthernet	Selects a GigabitEthernet interface.
slot/port num	Slot and port number for the selected interface. The slot range is 1 to 14, and the port is 0. The slot number and port number are separated with a forward slash character (/).
PortChannel	Selects the Ethernet Channel of interfaces.
num	Specifies the Ethernet Channel interface number. The range is from 1 to 4.
rspf	OSPF rspf.
route	Internal OSPF rspf routes.
router-id	(Optional) Specifies the ID of a router for clear routing information.
traffic	OSPF traffic counters.

1. BGP = Border Gateway Protocol
2. OSPF = Open Shortest Path First

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Use the **clear ip bgp** command whenever any of the following changes occur:

- Additions or changes to the BGP-related access lists
- Changes to BGP-related weights
- Changes to BGP-related distribution lists
- Changes to BGP-related route maps

Examples

The **clear ip bgp all** command is used to clear all routes in the local routing table. In the following example, the Proximity Engine has only one neighbor, 192.168.86.3:

```
ServiceRouter# clear ip bgp all
ServiceRouter# show ip bgp summary

BGP router identifier 3.2.5.4, local AS number 1
BGP table version is 3626, IPv4 Unicast config peers 3, capable peers 2
2 network entries and 2 paths using 216 bytes of memory
BGP attribute entries [2/168], BGP AS path entries [3/14]
BGP community entries [2/8], BGP clusterlist entries [0/0]
BGP Location Communities:
Location Communities value: 1:1-2:2 target 1:1-2:2 weight 4

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
3.1.5.13        4    10   12787    8819        0    0    0 00:00:03 Closing
3.1.5.103       4     3    2036    2035     3626    0    0    1d09h 1
37.0.0.7        4     2    2036    2035     3626    0    0    1d09h 1

ServiceRouter#
```

The following example shows how to clear OSPF of all neighbors:

```
ServiceRouter# clear ip ospf neighbor all
ServiceRouter#
```

The following example shows how to clear OSPF of all neighbors in the GigabitEthernet 1/0 interface:

```
ServiceRouter# clear ip ospf neighbor GigabitEthernet 1/0
ServiceRouter#
```

The following example shows how to clear OSPF RSPF information for all routers:

```
ServiceRouter# clear ip ospf rspf route
ServiceRouter#
```

The following example shows how to clear OSPF RSPF information for the router with the ID 172. 20.168.41:

```
ServiceRouter# clear ip ospf rspf route 172.20.168.41
ServiceRouter#
```

Related Commands

Command	Description
show ip bgp summary	Displays the status of all BGP connections.

clear ipv6

To clear the IPv6 ACL counters, use the **clear ipv6** command in EXEC configuration mode.

clear ipv6 access-list counters [*standard_acl-num* | *extended_acl_num* | *acl_name*]

Syntax Description

access-list	Clears the IP access list statistical information.
counters	Clears the IP access list counters.
standard_acl_num	(Optional) Counters for the specified access list, identified using a numeric identifier. The range is from 1 to 99.
extended_acl_num	(Optional) Counters for the specified access list, identified using a numeric identifier. The range is from 100 to 199
acl-name	(Optional) Counters for the specified access list, identified using an alphanumeric identifier up to 30 characters, beginning with a letter.

Command Defaults

No

Command Modes

EXEC configuration mode.

Examples

The following example shows how to clear IPv6 ACL counters:

```
ServiceRouter# clear ipv6 access-list counters 99
ServiceRouter#
```

Related Commands

Command	Description
ipv6	Specifies the default gateway's IPv6 address.
show ipv6	Displays the IPv6 information.
traceroute6	Traces the route to a remote IPv6-enabled host.

clear isis

To clear IS-IS Routing for an IP, use the **clear isis** command in EXEC configuration mode.

clear isis {**adjacency** {**all** | **GigabitEthernet** *slot/port num* | **PortChannel** *num*} | **ip rspf route** [*LSP-ID*]}

Syntax Description

adjacency	Clears the IS-IS adjacency information.
all	Clears IS-IS adjacencies on all interfaces.
GigabitEthernet	Selects a GigabitEthernet interface.
slot/port num	Slot and port number for the selected interface. The slot range is 1 to 14; the port is 0. The slot number and port number are separated with a forward slash character (/).
PortChannel	Selects the Ethernet Channel of interfaces.
num	Specifies the Ethernet Channel interface number. The range is from 1 to 4.
ip	IS-IS IP information.
rspf	IS-IS Reverse SPF[1] routing information.
route	Specifies the IS-IS route.
LSP_ID	(Optional) Clears information for LSPs[2] ID in the form of xxxx.xxxx.xxxx.xxxx or name.

1. SPF = Shortest Path First
2. LSP = link-state packet

Command Defaults

If no LSP ID is specified in the **clear isis ip rspf route** command, IS-IS RSPF information is cleared for all LSP IDs.

Command Modes

EXEC configuration mode.

Usage Guidelines

The **clear isis ip rspf route** command is used to clear IS-IS RSPF routing information. IS-IS RSPF routing information is displayed only with the **show isis ip rspf route** command when a new proximity request has been received.

Examples

The following is sample output from the **show isis adjacency** command before and after running the **clear isis adjacency** command:

```
ServiceRouter# show isis adjacency

IS-IS adjacency database:
System ID       SNPA            Level  State  Hold Time  Interface
0200.c0a8.5401  0000.a1e8.e019  1      UP     00:00:21   GigabitEthernet 3/0
7301-7-core     001d.a1e9.c41b  1      UP     00:00:08   GigabitEthernet 3/0
7301-7-core     001d.a1e9.c41b  2      UP     00:00:08   GigabitEthernet 3/0
```

```
ServiceRouter#

ServiceRouter# clear isis adjacency all

ServiceRouter# show isis adjacency

IS-IS adjacency database:
System ID       SNPA            Level  State  Hold Time  Interface
7301-7-core     001d.a1e9.c41b  1      UP     00:00:09   GigabitEthernet 3/0
7301-7-core     001d.a1e9.c41b  2      UP     00:00:09   GigabitEthernet 3/0

ServiceRouter#
```

The following is a sample from the **show isis ip rspf route** command before and after running the **show isis ip rspf route** command:

```
ServiceRouter# show isis ip rspf route

LSP ID                 SPF Time  Cache Hit  Level      Age Max range
0200.c0a8.0a01.00-00   3d22h            0    1    3d22h 10

ServiceRouters# clear isis ip rspf route

ServiceRouter# show isis ip rspf route

LSP ID                 SPF Time  Cache Hit  Level      Age Max range
```

Related Commands

Command	Description
show isis adjacency	Displays IS-IS adjacencies.
show isis ip rspf route	Displays the Intermediate IS-IS RSPF route for IS-IS learned routes.

clear logging

To clear the syslog messages saved in the disk file, use the **clear logging** command in EXEC configuration mode.

clear logging

Syntax Description

This command has no keywords or arguments.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

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
```

Examples

The following example shows how to clear the syslogs:

```
ServiceRouter# clear logging
U11-CDE220-2#
```

clear service-router

To clear the proximity-based routing proximity cache , use the **clear service-router** command in EXEC configuration mode.

clear service-router proximity-based-routing proximity-cache

Syntax Description

proximity-based-routing	Clears proximity-based routing.
proximity-cache	Clears proximity cache.

Command Defaults

Clears the cache for all proximity ratings.

Command Modes

EXEC configuration mode.

Usage Guidelines

When an SR receives a redirect request from a client network 1 with proximity-based routing enabled, the SR queries the proximity server for the proximity rating of the SEs. The ratings returned from the proximity server are cached, and the default timeout for the cache is 1800 seconds . If there is any network or proximity rating change within this period, the SR does not know as it redirects based on the ratings cached for that network. The **clear service-router** command is used to force clear cache.

Examples

The following example shows how to clear the Service Router.

```
ServiceRouter# clear service-router proximity-based-routing proximity-cache
ServiceRouter#
```

Related Commands

Command	Description
show service-router	Shows the cache timeout period.

clear srp database offline

To clear the SRP database while it is offline, use the **clear srp database offline** command in privileged EXEC mode.

clear srp database offline

Syntax Description

This command has no keywords or arguments.

Command Defaults

None

Command Modes

Privileged EXEC configuration mode.

Usage Guidelines

The **clear srp database offline** command is used to clear the SRP database while it is offline.

Note You must turn off SRP before executing this command by entering the **no router srp** command.

Examples

The following example shows how to clear the SRP database offline:

```
ServiceRouter# clear srp database offline
Clearing database offline
ServiceRouter#
```

Related Commands

Command	Description
show srp database	Displays the descriptor-related information saved in the descriptor database.
show srp multicast database	Displays multicast database information.

clear srp descriptor

To delete either a single descriptor or all descriptors from the service routing layer, use the **clear srp descriptor** command in privileged EXEC mode.

clear srp descriptor *key*

Syntax Description

key	The DHT key in hexadecimal format for the descriptor to be deleted. A valid DHT key has 1 to 64 hexadecimal digits.

Command Defaults

None

Command Modes

Privileged EXEC configuration mode.

Usage Guidelines

The **clear srp descriptor** command is used to delete a single descriptor in the descriptor database. The delete operation deletes the descriptor at the descriptor root node (which may not necessarily be the local Proximity Engine). Therefore, the descriptor is deleted from the entire network.

Note Deleting a group descriptor also causes the deletion of the group from the network (not just the group's descriptor).

A valid DHT key must be specified in *key* to identify the descriptor that is deleted. Keys with less than 64 hexadecimal characters are appended with zeroes.

Deleting a nonexistent descriptor or a descriptor that does not appear in the descriptor database of the Proximity Engine results in an error message stating that the DHT key does not exist.

Examples

The following example shows how use the **clear srp descriptor** command to delete a descriptor with key 123. After the deletion, the **show srp database** command is used to verify that the descriptor has been deleted.

```
ServiceRouter# clear srp descriptor 123
ServiceRouter# show srp database 123

Getting database entry for
123

Entity key:
1230000000000000000000000000000000000000000000000000000000000000
Entity was DELETED on (47b4269b599afa86) Thu Feb 14 11:31:39 2008
```

Related Commands

Command	Description
show srp database	Displays the descriptor-related information saved in the descriptor database.
show srp multicast database	Displays multicast database information.

clear srp neighbor

To remove a neighbor Proximity Engine from the neighbor list of the local Proximity Engine, use the **clear srp neighbor** command in privileged EXEC mode.

clear srp neighbor *key*

Syntax Description

key	The DHT key in hexadecimal format for the node to be removed from the neighbor list. A valid DHT key has 1 to 64 hexadecimal digits.

Command Defaults

None

Command Modes

Privileged EXEC configuration mode.

Usage Guidelines

The **clear srp neighbor** command is used to delete a single neighbor in the service routing layer from the local Proximity Engine neighbor list. After a small interval, the neighbor list is refreshed and the deleted neighbor may be included in the neighbor list again if it is still a neighbor of the local Proximity Engine in the service routing layer.

A valid DHT key should be specified in *key* to identify the neighbor. Keys with less than 64 hexadecimal characters are appended with zeroes.

If you attempt to delete a neighbor that does not appear in the neighbor list of the local Proximity Engine, **clear srp neighbor** displays an error message stating that the neighbor could not be found.

Examples

The following example shows how to use Proximity Engine sn-sj85 with one neighbor sn-sj81 as seen in the following **show srp neighbor** command output. The neighbor sn-sj81 is also in the leafset of sn-sj85 as can be seen in the **show srp leafset** output. All commands are issued from Proximity Engine sn-sj85.

```
ServiceRouter# show srp neighbor

Codes: T - local node, L - leafset, P - primary, S - secondary, B - backup
       I - Intransitive, D - delay, H - hold time

Number of neighbors in the database: 1

PL  8886822171add71887d54107c266d814b605eaa0d5cc9b54b9160a137f4355d1
    via sn-sj81 [ 172.20.168.81 ] :9000, D=0.389864 ms,
   H=00:00:09


ServiceRouter# show srp leafset

Codes: T - local node, L - leafset, P - primary, S - secondary, B - backup
       I - Intransitive, W - wrapped

Leafset count: total 3, left 1, right 1

PL   8886822171add71887d54107c266d814b605eaa0d5cc9b54b9160a137f4355d1
```

```
    via sn-sj81 [ 172.20.168.81 ] :9000, 0.389864 ms, 00:00:08
T    9f752f56f347ca8fcc40a4e09b645f9b4c9b71c73401083f4c04920b30215b0a
    via sn-sj85 [ 172.20.168.85, 192.168.20.85, 192.168.86.85 ] :9000
WPL  8886822171add71887d54107c266d814b605eaa0d5cc9b54b9160a137f4355d1
    via sn-sj81 [ 172.20.168.81 ] :9000, 0.389864 ms, 00:00:08
```

The **clear srp neighbor** command is used to remove sn-sj81 from the neighbor list.

```
ServiceRouter# clear srp neighbor sn-sj81:9000

Clearing neighbor sn-sj81:9000

Neighbor is found and cleared
```

Finally, the **show srp neighbor** and **show srp leafset** commands are issued again and show the following:

- Output from **show srp neighbor s**hows that the neighbor sn-sj81 is in the intransitive state (I). The intransitive state means node sn-sj85 cannot reach node sn-sj81.

```
ServiceRouter# show srp neighbor

Codes: T - local node, L - leafset, P - primary, S - secondary, B - backup
       I - Intransitive, D - delay, H - hold time

Number of neighbors in the database: 1

I   8886822171add71887d54107c266d814b605eaa0d5cc9b54b9160a137f4355d1
    via sn-sj81 [ 172.20.168.81 ] :9000, D=0.000 ms,
   H=00:00:07
```

- Output from **show srp leafset s**hows that there are no leafset entries (PL or WPL) for the Proximity Engine sn-sj85.

```
ServiceRouter# show srp leafset

Codes: T - local node, L - leafset, P - primary, S - secondary, B - backup
       I - Intransitive, W - wrapped

Leafset count: total 1, left 0, right 0

T    9f752f56f347ca8fcc40a4e09b645f9b4c9b71c73401083f4c04920b30215b0a
    via sn-sj85 [ 172.20.168.85, 192.168.20.85, 192.168.86.85 ] :9000

ServiceRouter# #
```

The following example shows how to use the **clear srp resource** command to delete a resource having resource ID 456 from a descriptor with the key 123. The **show srp database** command is used to verify that the resource exists before the delete operation and that it has been deleted after the delete operation.

```
ServiceRouter# show srp database 123

Getting database entry for
123

Entity key:
123000000000000000000000000000000000000000000000000000000000000000
Entity rec type:          101     Entity total length: 175
Entity type:         38b73479     Entity flags:        0
--------------- Element 0        (main)-----------------
Element ID: main
```

```
  Element total len          49   ID len:      0
  Delete Time: 47b426ca5c706042
  Flags  0
  Last Update: Thu Feb 14 11:38:59 2008 (47b42853902a02b6)
  Expiration : Sat Mar 15 11:38:59 2008 (47dbb553902a0000)
  Element data len:           9
  Element data:
mycontent
--------------- Element 1        (comp)-----------------
Element ID: "456"(343536)
  Element total len          54   ID len:      3
  Last Update: Thu Feb 14 11:39:27 2008 (47b4286f0ad1055a)
  Expiration : Sat Mar 15 11:39:27 2008 (47dbb56f0ad10000)
  Element data len:          11
  Element data:
newResource

ServiceRouter# clear srp resource 123 456

ServiceRouter# show srp database 123

Getting database entry for
123

Entity key:
123000000000000000000000000000000000000000000000000000000000000000000000
Entity rec type:          101     Entity total length: 113
Entity type:         38b73479     Entity flags:        0
--------------- Element 0        (main)-----------------
Element ID: main
  Element total len          49   ID len:      0
  Delete Time: 47b426ca5c706042
  Flags  0
  Last Update: Thu Feb 14 11:38:59 2008 (47b42853902a02b6)
  Expiration : Sat Mar 15 11:38:59 2008 (47dbb553902a0000)
  Element data len:           9
  Element data:
mycontent

ServiceRouter#
```

Related Commands

Command	Description
show srp leafset	Displays SRP leafset information.
show srp neighbors	Displays SRP neighbor information.

clear srp resource

To delete a resource from a descriptor in the service routing layer, use the **clear srp resource** command in privileged EXEC mode.

clear srp resource *key*

Syntax Description

key	The DHT key in hexadecimal format for the descriptor from which the resource are deleted. A valid DHT key has 1 to 64 hexadecimal digits.

Command Defaults

None

Command Modes

Privileged EXEC configuration mode.

Usage Guidelines

The **clear srp resource** command is used to delete a resource from a descriptor in the service routing layer. Resources can be added to and deleted from any descriptor that exists in the descriptor database.

A valid DHT key must be specified in *key* to identify the descriptor from which a resource is deleted. Keys with less than 64 hexadecimal characters are appended with zeroes. If you attempt to delete a resource from a nonexistent descriptor, **clear srp resource** displays an error stating that the DHT key does not exist. Deleting a nonexistent resource has no impact, and no error warning is generated.

Examples

The following example shows how to use **clear srp resource** to delete a resource, newResource, having resource ID 456 from a descriptor with the key 123. The **show srp database** command is used to verify that the resource exists before the delete operation and that it has been deleted after the delete operation.

```
ServiceRouter# show srp database 123

Getting database entry for
123

Entity key:
123000000000000000000000000000000000000000000000000000000000000000
Entity rec type:          101     Entity total length: 175
Entity type:         38b73479     Entity flags:        0
--------------- Element 0        (main)-----------------
Element ID: main
  Element total len          49   ID len:      0
  Delete Time: 47b426ca5c706042
  Flags  0
  Last Update: Thu Feb 14 11:38:59 2008 (47b42853902a02b6)
  Expiration : Sat Mar 15 11:38:59 2008 (47dbb553902a0000)
  Element data len:           9
  Element data:
mycontent
--------------- Element 1        (comp)-----------------
Element ID: "456"(343536)
  Element total len          54   ID len:      3
  Last Update: Thu Feb 14 11:39:27 2008 (47b4286f0ad1055a)
  Expiration : Sat Mar 15 11:39:27 2008 (47dbb56f0ad10000)
```

```
  Element data len:          11
  Element data:
newResource

ServiceRouter# clear srp resource 123 456

ServiceRouter# show srp database 123

Getting database entry for
123

Entity key:
123000000000000000000000000000000000000000000000000000000000000000
Entity rec type:          101     Entity total length: 113
Entity type:         38b73479     Entity flags:        0
--------------- Element 0        (main)-----------------
Element ID: main
  Element total len          49   ID len:      0
  Delete Time: 47b426ca5c706042
  Flags  0
  Last Update: Thu Feb 14 11:38:59 2008 (47b42853902a02b6)
  Expiration : Sat Mar 15 11:38:59 2008 (47dbb553902a0000)
  Element data len:           9
  Element data:
mycontent

ServiceRouter#
```

Related Commands

Command	Description
clear srp descriptor	Deletes a single descriptor or all descriptors from the service routing layer
show srp database	Displays the descriptor-related information saved in the descriptor database.

clear srp route

To delete a single route entry from the DHT routing table of the local Proximity Engine, use the **clear srp route** command in privileged EXEC mode.

clear srp route *prefix/length*

Syntax Description

prefix	The prefix of the DHT key of the route entry to delete.
length	The length of the prefix (in multiples of 4).

Command Defaults

None

Command Modes

Privileged EXEC configuration mode.

Usage Guidelines

The **clear srp route** command deletes a single routing table entry from the local DHT routing table. Similar to other routing protocols, the DHT routing table entries consist of a prefix and length that index the DHT ID of the next-hop Proximity Engine. A valid DHT key prefix (1 to 64 hexadecimal characters) and valid prefix length (multiples of four) must be supplied to identify the neighbor to be deleted.

The **clear srp route** command provides a manual way to delete routing table entries. After a small interval, the DHT routing table is refreshed and the deleted next-hop Proximity Engine may be included in the DHT routing table again if it is still a viable neighbor.

The **clear srp route** command can be used to test the presence and persistence of neighbors. Deleting a routing entry that does not exist results in an error message.

Examples

In the following example, Proximity Engine sn-sj85 has four routing table entries. The example shows how to use the **clear srp route** command to clear the routing table entry that has 8/4 as its *prefix/length*. The **show srp route** command is used to verify the deletion of the route.

```
ServiceRouter# show srp route

Codes: T - local node, L - leafset, P - primary, S - secondary, B - backup
       I - Intransitive

PL  8/4 via 8886822171add71887d54107c266d814b605eaa0d5cc9b54b9160a137f4355d1
    sn-sj81 [ 172.20.168.81 ] :9000, 0.389525 ms, 00:00:08
PL  a/4 via ad3a659121442210a68b79348e9a42eaebfb229f388afb2628fa871f26bc750c
    sn-sj67 [ 172.20.168.67, 192.168.20.41, 192.168.20.44, 192.168.22.41, 192.168
.22.42 ] :9000, 1.825903 ms, 00:00:09
PL  b/4 via b5ca21563f5b938e46e2cb8f33a148ae00a1f6666f2a5eb735b7ed90c012c882
    sn-sj82 [ 172.20.168.82 ] :9000, 0.333920 ms, 00:00:08
PL  d/4 via d2fc632c53c9ff1de8683e265386b09502791aedd65f28025fe7f64ad8cab2d9
    sn-sj87 [ 172.20.168.87 ] :9000, 0.642357 ms, 00:00:09

ServiceRouter# clear srp route 8/4

Clearing entry 8/4

The entry is found and cleared
```

```
ServiceRouter# show srp route

Codes: T - local node, L - leafset, P - primary, S - secondary, B - backup
       I - Intransitive

PL  a/4 via ad3a659121442210a68b79348e9a42eaebfb229f388afb2628fa871f26bc750c
    sn-sj67 [ 172.20.168.67, 192.168.20.41, 192.168.20.44, 192.168.22.41, 192.168
.22.42 ] :9000, 1.846593 ms, 00:00:09
PL  b/4 via b5ca21563f5b938e46e2cb8f33a148ae00a1f6666f2a5eb735b7ed90c012c882
    sn-sj82 [ 172.20.168.82 ] :9000, 0.333920 ms, 00:00:09
PL  d/4 via d2fc632c53c9ff1de8683e265386b09502791aedd65f28025fe7f64ad8cab2d9
    sn-sj87 [ 172.20.168.87 ] :9000, 0.572056 ms, 00:00:09

ServiceRouter#
```

Related Commands

Command	Description
show srp route	Displays route information for a Proximity Engine to its neighbor nodes on the same DHT network.

clear statistics

To clear the statistics, use the **clear** s**tatistics** command in EXEC configuration mode.

On the SE:

clear statistics {**aaa** | **access-lists 300** | **all** | **authentication** | **authsvr** {**all** | **delivery-service-id** | **global**} | **distribution** {**all** | **mcast-data-receiver** | **mcast-data-sender** | **metadata-receiver** | **metadata-sender** | **unicast-data-receiver** | **unicast-data-sender**} | **flash-media-streaming** | **history** | **icap** | **icmp** | **ip** | **movie-streamer** | **radius** | **rule** {**action** *action-type* | **all** | **pattern** {**1-512** | **all**} | **rtsp**} | **running** | **snmp** | **tacacs** | **tcp** | **transaction-logs** | **udp** | **web-engine** [**force**] | **web-engine** [**force**] | **wmt**}

On the SR:

clear statistics {**aaa** | **all** | **authentication** | **history** | **http requests** | **icmp** | **ip** [**ospf** | **proximity** {**rib** | **server**}] | **isis** [**GigabitEthernet** *slot/port num* | **PortChannel** *num*] | **radius** | **running** | **service-registry** | **service-router** | **snmp** | **srp** | **tacacs** | **tcp** | **udp**}

Syntax Description

aaa	Clears AAA statistics.
access-lists	Clears the ACL statistics.
300	Clears the group name-based ACL.
all	Clears all statistics.
authentication	Clears the authentication statistics.
authsvr	Clears the Authorization Server statistics.
all	Clears global and delivery service-based statistics.
delivery-service-id	Clears Authentication Server statistics for the delivery service
global	Clears Authentication Server global statistics.
distribution	Clears the distribution statistics.
all	Clears the distribution statistics for every component.
mcast-receiver	Clears the distribution statistics for the mcast receiver. **Note** This command is only available on Cisco Internet Streamer CDS Release 3.1.1.
mcast-sender	Clears the distribution statistics for the mcast sender. **Note** This command is only available on Cisco Internet Streamer CDS Release 3.1.1.
metadata-receiver	Clears the distribution statistics for the metadata receiver. **Note** This command is only available on Cisco Internet Streamer CDS Release 3.1.1.
metadata-sender	Clears the distribution statistics for the metadata sender. **Note** This command is only available on Cisco Internet Streamer CDS Release 3.1.1.
unicast-data-receiver	Clears the distribution statistics for the unicast data receiver. **Note** This command is only available on Cisco Internet Streamer CDS Release 3.1.1.

unicast-data-sender	Clears the distribution statistics for the unicast data sender. This command is only available on Cisco Internet Streamer CDS Release 3.1.1.
flash-media-streaming	Clears the Flash Media Streaming statistics.
history	Clears the statistics history.
icap	Clears the ICAP[1] statistics.
icmp	Clears the ICMP statistics.
ip	Clears the IP statistics.
ospf	Clears the OSPF statistics.
proximity	Clears the proximity statistics.
rib	Clears the RIB proximity statistics.
server	Clears the Proximity Server statistics.
isis	Clears counters for an IS-IS instance.
GigabitEthernet	(Optional) Selects a GigabitEthernet interface.
slot/port num	Slot and port number for the selected interface. The slot range is 0 to 14; the port is 0. The slot number and port number are separated with a forward slash character (/).
PortChannel	(Optional) Selects the Ethernet Channel of interfaces.
num	Specifies the Ethernet Channel interface number. The range is from 1 to 4.
movie-streamer	Clears the Movie Streamer statistics.
radius	Clears the RADIUS statistics.
rule	Clears the rules statistics.
action	Clears the statistics of all the rules with the same action.
action-type	Specifies one of the following actions: **allow** **block** **generate-url-signature** **no-cache** **redirect** **rewrite** **use-icap-service** **validate-url-signature**
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.
srp	Resets to zero all statistics counters kept by the local DHT service

tacacs	Clears the TACACS+ statistics.
tcp	Clears the TCP statistics.
transaction-logs	Clears the transaction log export statistics.
udp	Clears the UDP statistics.
web-engine	Clears the Web Engine statistics.
force	Clears the Web Engine detail statistics.
web-engine	Clears Web Engine statistics.
force	(Optional) Clears Web Engine detail statistics.
wmt	Clears all WMT statistics.

1. ICAP = Internet Content Adaptation Protocol

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

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.

This command is used to reset to zero proximity statistics related to the Proximity Engine components that are used for the proximity function. Use the **show statistics ip proximity** command to display proximity statistics.

The DHT service keeps several counters, such as the number of requests and responses for DHT lookups. These counters can be displayed using the **show statistics srp** command.

The **clear statistics web-engine** and **clear statistics all** commands clear only normal statistics, not the Web Engine statistics details. To clear all Web Engine statistics, use the **clear statistics web-engine force** command.

The **clear stats authsvr delivery-service-id** command only clears the authsvr delivery-service specific statistics. It does not clear global statistics. If you want to clear the global statistics, you must use the **clear statistics authsvr al**l or **clear statistics authsvr global** commands.

Note The **clear statistics web-engine** and **clear statistics all** commands clear only normal statistics, not the Web Engine statistics details. To clear all Web Engine statistics, use the **clear statistics web-engine force** command. We do not recommend using the **clear statistics web-engine force** command, but if it is used, restart the Web Engine service by entering the **web-engine stop** and **web-engine start** commands.

Examples

The following example shows how to clear proximity statistics with the **clear statistics ip proximity** command:

```
ServiceRouter# clear statistics ip proximity server
ServiceRouter# show statistics ip proximity server
```

```
Proximity server: Requests received =  0
Proximity server: Responses sent =  0
Proximity server: Faults sent =  0
ServiceRouter#

ServiceRouter# show statistics ip proximity rib
Total number of proximity requests received from applications:  0
Total number of proximity replies sent to applications:         0
Proximity msg exchanges between urib and routing protocols:
          Sent Prox Req         Received Prox Resp
isis-p1               0                          0
ospf-p1               0                          0
isis-p1-te            0                          0
ospf-p1-te            0                          0
bgp-123               0                          0
mbgp-123              0                          0
Local proximity requests from applications: 0
Invalid proximity requests from applications: 0
PSA non-rankable proximity requests from applications: 0
Failed proximity requests to routing protocols: 0
Failed PSA lookups: 0
Failed PTA lookups: 0
ServiceRouter#
```

The following is sample output from the **show statistics isis** command before and after running **clear statistics isis** command:

```
ServiceRouter# show statistics isis

IS-IS statistics:
PDU        Received        Sent  RcvAuthErr OtherRcvErr
LAN-IIH          51          14           0           0
P2P-IIH           0           0           0           0
CSNP             67           0           0           0
PSNP              0           0           0           0
PDU        Received     Flooded  RcvAuthErr OtherRcvErr  ReTransmit
LSP              69           4           0           0           0
DIS elections:    10
SPF calculations: 82
LSPs sourced:     0
LSPs refreshed:   8
LSPs purged:      0

ServiceRouter#

ServiceRouter# clear statistics isis *

ServiceRouter# show statistics isis

IS-IS statistics:
PDU        Received        Sent  RcvAuthErr OtherRcvErr
LAN-IIH           1           0           0           0
P2P-IIH           0           0           0           0
CSNP              4           0           0           0
PSNP              0           0           0           0
PDU        Received     Flooded  RcvAuthErr OtherRcvErr  ReTransmit
LSP               1           0           0           0           0
DIS elections:    0
SPF calculations: 1
LSPs sourced:     0
LSPs refreshed:   0
LSPs purged:      0

ServiceRouter#
```

The following example shows the use of the **clear statistics srp** command. The **show statistics srp** command is used to verify that the SRP counters have been reset to zero:

```
ServiceRouter# show statistics srp

                              Sent     Received    Neighbors
Join request                     0           22            1
Join response                   22            0            0
LS exchange request            309          310            0
LS exchange response           310          309            0
Route exchange request          65            0            0
Route exchange response          0           64            0
Ping request                   410          412            1
Ping response                  412          410            0
Lookup request                  34          867            3
Lookup response                867           34            0
Ping traceroute request          0            0            0
Ping traceroute response         0            0            0

ServiceRouter# clear statistics srp

Clearing all statistics counters

ServiceRouter# show statistics srp

                              Sent     Received    Neighbors
Join request                     0            0            0
Join response                    0            0            0
LS exchange request              1            1            0
LS exchange response             1            1            0
Route exchange request           1            0            0
Route exchange response          0            1            0
Ping request                     2            2            0
Ping response                    2            2            0
Lookup request                   0            2            0
Lookup response                  2            0            0
Ping traceroute request          0            0            0
Ping traceroute response         0            0            0
ServiceRouter#
```

Related Commands

Command	Description
show statistics	Displays statistics information.

clear transaction-logs

To clear and archive the working transaction log files, use the **clear transaction-log** command in EXEC configuration mode.

clear transaction-logs

Syntax Description

This command has no keywords or arguments.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

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.

Examples

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

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

clear users

To clear the connections (login) of authenticated users, use the **clear users** command in EXEC configuration mode.

clear users administrative

Syntax Description

administrative	Clears the connections of administrative users who have been authenticated through a remote login service.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

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 how to clear the connections of the authenticated users:

```
ServiceRouter# clear users administrative
ServiceRouter#
```

clear wmt

To clear the WMT streams, use the **clear wmt** command in EXEC configuration mode.

clear wmt {**encoder-alarm-msg** *msg* | **stale-stat** | **stream-id** *num* [***stale-stat***]}

Syntax Description

encoder-alarm-msg	Detailed alarm message of the Encoder Alarm to be cleared.
msg	Detailed alarm message.
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.
1-999999	WMT stream ID to clear.
stale-stat	Stale statistic of the WMT stream to be cleared.

Command Defaults

None

Command Modes

EXEC configuration mode.

Examples

The following example shows how to clear a WMT stream for a stream ID of 22689:

```
ServiceEngine# clear wmt stream-id 22689
ServiceEngine#
```

Related Commands

Command	Description
show statistics wmt	Displays the WMT statistics.
show wmt	Displays WMT bandwidth and proxy mode configuration.

clock (EXEC)

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

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.
time	Current time in hh:mm:ss format (hh: 00 to 23; mm: 00 to 59; ss: 00 to 59).
day	Day of the month. The range is from 1 to 31.
month	Month of the year (January, February, March, April, May, June, July, August, September, October, November, December).
year	Year. The range is from 1993 to 2035.
update-calendar	Updates the calendar with the system clock.

Command Defaults

None

Command Modes

EXEC configuration mode.

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 have to set the system clock manually. Enter the local time when setting the clock. The SE calculates the Coordinated Universal Time (UTC) based on the time zone set by the **clock timezone** command.

Note We strongly recommend that you configure the SE for the NTP by using the **ntp** command. See the "ntp" section on page 2-270 for more details.

Note If you change the local time on the device, you must change the BIOS clock time as well; otherwise, the timestamps on the error logs are not synchronized. Changing the BIOS clock is required because the kernel does not handle time zones.

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 bootup 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 that 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 NTP clock source, you do not have 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** command.

Examples

The following example shows how to set the software clock on the SE:

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

Related Commands

Command	Description
clock timezone	Sets the clock timezone.
ntp	Configures the Network Time Protocol server.
show clock detail	Displays the UTC and local time.

clock (Global configuration)

To set the summer daylight saving time and time zone for display purposes, use the **clock** command in Global configuration mode. 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 hoursoffset 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 hoursoffset minutesoffset*}}

Syntax Description

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

hoursoffset	Hours offset (see Table B-1) from UTC. The range is from –23 to +23.
minutesoffset	Minutes offset (see Table B-1) from UTC. The range is from 0 to 59.

Command Defaults

None

Command Modes

Global configuration (config) mode.

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** command in EXEC configuration mode. The UTC and local time are displayed with the **show clock detail** command in EXEC configuration mode.

Use the **clock** *timezone offset* command to specify a time zone, where *timezone* is the desired time zone entry from Table 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, the system is automatically adjusted for daylight saving time.

Note If you change the local time on the device, you must change the BIOS clock time as well; otherwise, the timestamps on the error logs are not synchronized. Changing the BIOS clock is required because the kernel does not handle time zones.

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

Examples

The following example shows how to specify 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 shows how to configure 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 shows how to configure daylight saving time:

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

Related Commands

Command	Description
clock	To set the summer daylight saving time and time zone for display purposes.
show clock detail	Displays the UTC and local time.

cms (EXEC)

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

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.
filename	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.
filename	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.
word	Identity of the recovered device.

Command Defaults

None

Command Modes

EXEC configuration mode.

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 a CDS network, it must first be registered and then activated. The **cms enable** 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.

Note The **cms deregister** command cleans up the database automatically. You do not need to use the **cms database delete** command. If the deregistration fails, the best practice is to resolve any issues that caused the deregistration failure; for example, the Service Engine is the Content Acquirer of a delivery service and cannot be deleted or deactivated. Assign a different SE as the Content Acquirer in each delivery service where this SE is assigned as the Content Acquirer and try the **cms deregister** command again.

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, 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 or 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 are not sent to the primary CDSM.

If LCM is disabled, the settings configured through the CDSM GUI 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 is 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 overwrite the local device settings.

The **cms deregister force** command should be used only as the last option, because the CDSM does not know about the device being removed. When executing the **cms deregister force** command, take note of any messages stating that the deregistration failed and make sure to resolve them before reregistering the device with the same CDSM or registering the device to another CDSM. The **cms deregister force** command forces the deregistration to continue.

Examples

The following example shows how to back 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 shows how to validate 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 GUI:

```
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

Command	Description
cms enable	Enables the CMS.
show cms	Displays the CMS protocol, embedded database content, maintenance status, and other information.

cms (Global configuration)

To schedule maintenance and enable the Centralized Management System (CMS) on a given node, use the **cms** command in Global configuration mode. 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.
weekday	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.
time	Time of day to start the maintenance routine. The range is from 0 to 23:0 to 59 in hh:mm format.
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 for when making a connection.
5-1800	Timeout period, in seconds. The default for the CDSM is 30; the default for the SE and the SR is 180.
incoming-wait	Specifies the maximum time to wait for a client response.
10-600	Timeout period, in seconds. The default is 30.
transfer	Specifies the maximum time to allow a connection to remain open.
10-7200	Timeout period, in seconds. The default is 300.

Command 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 (config) mode.

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 runs only 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 stops only 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 two multicast senders.

Examples

The following example shows how to schedule 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...
```

```
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

Command	Description
cms database	Creates, backs up, deletes, restores, or validates the CMS-embedded database management tables or files.
show cms	Displays the CMS protocol, embedded database content, maintenance status, and other information.

configure

To enter Global configuration mode, use the **configure** command in EXEC configuration mode.

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 keywords or arguments.

Command Defaults

None

Command Modes

EXEC configuration mode.

Examples

The following example shows how to enable Global configuration mode:

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

Related Commands

Command	Description
end	Exits configuration and privileged EXEC configuration modes.
exit	Exits from interface, Global configuration, or privileged EXEC configuration modes.
show running-config	Displays the current operating configuration.
show startup-config	Displays the startup configuration.

contentmgr

To configure the Content Manager, use the **contentmgr** command in Global configuration mode. To remove the configuration, use the **no** form of this command.

contentmgr {delivery-service cache-content purge-on-delete *num* **| disk-bucket-fail-threshold** *num* **| hitcnt-decay-half-life** *num***}**

no contentmgr {delivery-service cache-content purge-on-delete *num* **| disk-bucket-fail-threshold** *num* **| hitcnt-decay-half-life** *num***}**

Syntax Description

delivery-service	Configures the Content Manager delivery service. **Note** This command was introduced in the 2.6.3 software release.
cache-content	Configures the Content Manager delivery service cache content.
purge-on-delete	Configures the Content Manager delivery service cache content purge on delete.
num	Purge after minutes (0 to 1440). **Note** 0 means not deleting.
disk-bucket-fail-threshold	Configures threshold percentage of disk failures per bucket, to raise alarm.
num	Threshold percentage (1 to 100).
hitcnt-decay-half-life	Configure half life decay period for cache hit count updates.
num	Half life decay for cache content hit count updates (1 to 30).

Command Defaults

purge-on-delete: 5 minutes

disk-bucket-fail-threshold: default is 30 percent.

hitcnt-decay-half-life: default is 14 days.

Command Modes

Global configuration (config) mode.

Usage Guidelines

As part of FastCAL, the Content Manager module replaces the Ucache process in Cisco Internet Streamer CDS 2.6 Release software. The Content Manager keeps track of all the files in CDNFS, and maintains all content popularity information and stores it in a snapshot file.

The **contentmgr disk-bucket-fail-threshold** command monitors the percentage of disks failed in a particular disk bucket. A minor alarm would be raised if the percentage disk failure crosses the configured threshold value.

A disk bucket is a logical unit in FastCAL module, where all the disks on an SE are distributed equally among each disk bucket. The number of disk buckets can be 1, 3, or 4 depending on the platform.

For example:

- A CDE220 with 12 hard-disks (disk00 to disk11):
  - This hardware has 3 disk-buckets.

- Each disk-bucket has 4 disks in it (sequentially allocated).
- The allocation of disks is as follows:

  disk-bucket00 | disk-bucket01 | disk-bucket02

  ----------|----------|----------

  disk00 | disk01 | disk02

  disk03 | disk04 | disk05

  disk06 | disk07 | disk08

  disk09 | disk10 | disk11
- The Number of Disk buckets for each platform type is as as follows:

  2S6 = 4

  2M1 = 3

  2M0 = 4

  2S3I = 3

  CDE220 = 3

  2G2 = 3

  CDE205 = 1

Use the **contentmgr hitcnt-decay-half-life** command to configure the time period after which cache hit count is decayed.

The Content Manager transaction logs help identify whether a content is being added, updated, deleted, or evicted. The format for Content Manager transaction logging is as follows:

```
ServiceEngine# tail -f /local/local1/logs/content_mgr/working.log
```

Examples

The following example shows how to configure the Content Manager delivery service cache content purge on delete after 10 minutes:

```
ServiceEngine# delivery-service cache-content purge-on-delete 10
ServiceEngine(config)#
```

The following example shows how to configure the cache hit count half life to 10 days:

```
ServiceEngine# contentmgr hitcnt-decay-half-life 10
ServiceEngine(config)#
```

The following example shows how to configure the percentage of disk failures to 20 percent:

```
ServiceEngine# contentmgr disk-bucket-fail-threshold 20
ServiceEngine(config)#
```

The following example shows the disk bucket alarm:

```
ServiceEngine# show alarms

Critical Alarms:
----------------
None

Major Alarms:
-------------
     Alarm ID             Module/Submodule     Instance
     -------------------- -------------------- -------------------------
```

```
   1 cms_clock_alarm      cms

Minor Alarms:
-------------
     Alarm ID             Module/Submodule     Instance
     -------------------- -------------------- -------------------------
   1 psu                  sysmon               Power Supply
   2 disk_bucket_thresh   sysmon/cmgr/bucket00 Disk Bucket 00
   3 disk_bucket_thresh   sysmon/cmgr/bucket01 Disk Bucket 01
   4 disk_failure         sysmon               disk05
   5 disk_failure         sysmon               disk09
   6 disk_failure         sysmon               disk12
```

Related Commands

Command	Description
content-mgr disk-info force-reset	Forces the Content Manager to reset the disk share memory information
show content-mgr	Displays all content management information.
show statistics content-mgr	Displays the Content Manager statistics.

content-mgr disk-info force-reset

To force the Content Manager to reset the disk share memory information, use the **copy** command in EXEC configuration mode.

content-mgr disk-info-force-reset

Syntax Description

This command has no keywords or arguments.

Command Defaults

None

Command Modes

EXEC configuration mode.

Examples

The following example shows how to force the Content Manager to reset the disk share memory information:

```
ServiceEngine# content-mgr disk-info force-reset
Disk info force reset completed.
```

Related Commands

Command	Description
contentmgr	Configures the Content Manager.
show content-mgr	Displays all content management information.
show statistics content-mgr	Displays the Content Manager statistics.

content-origin

To support multiple origin servers within a content origin, use the **content-origin** command in Global configuration mode. To remove configured content origin, use the no form of this command.

content-origin request-fqdn *domain* **config-url** *url* [**username** *username* **password** *password*]

no content-origin request-fqdn *domain* **config-url** *url* [**username** *username* **password** *password*]

Syntax Description

request-fqdn	Configures the request FQDN[1].
domain	Domain of the request FQDN. Domain size range should be between 1to 255 characters.
config-url	URL of the content origin configuration file.
url	URL name.
username	Configures a username to access configuration file.
username	Specifies a username.
password	Configures a password to access configuration file.
password	Specifies a password.

1. fully qualified domain name.

Command Defaults

None

Command Modes

Global configuration mode.

Usage Guidelines

Previously, only one origin server per content origin was allowed and the same origin server could not be shared across multiple content origins. Users had to create delivery services or content origins and different content origin domain names resolving to same IP addresses of the origin server. This created much overhead during deployment. The **content-origin** command supports multiple origin servers within a content origin and allows users to share single origin servers across multiple delivery service or content origins.

Examples

The following example shows how to create a

```
ServiceEngine# content-origin request-fqdn xxx.com config-url
http://171.XX.XX.XXX/cdsorigin.xml username admin password default
```

Related Commands

Command	Description
show content-origin	Displays information about the NAS mount.

copy

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

copy cdnfs disk *url sysfs-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**}

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

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.
url	URL of the CDNFS file to be copied to the sysfs.
sysfs-filename	Filename to be copied in the sysfs.
disk	Copies a local disk file.
ftp	Copies to a file on an FTP server.
hostname	Hostname of the FTP server.
ip-address	IP address of the FTP server.
remotefiledir	Directory on the FTP server to which the local file is copied.
remotefilename	Name of the local file after it has been copied to the FTP server.
localfilename	Name of the local file to be copied.
startup-config	Copies the configuration file from the disk to startup configuration (NVRAM).
filename	Name of the existing configuration file.
ftp	Copies a file from an FTP server.
disk	Copies a file to a local disk.
hostname	Hostname of the FTP server.
ip-address	IP address of the FTP server.
remotefiledir	Directory on the FTP server where the file to be copied is located.
remotefilename	Name of the file to be copied to the local disk.
localfilename	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.
hostname	Name of the FTP server.
ip-address	IP address of the FTP server.
remotefiledir	Remote file directory.
remotefilename	Remote filename.
http install	Copies the file from an HTTP server and installs the software release file on a local device.
hostname	Name of the HTTP server.
ip-address	IP address of the HTTP server.
remotefiledir	Remote file directory.
remotefilename	Remote filename.
port	(Optional) Specifies the port to connect to the HTTP server. The default is 80.
port-num	HTTP server port number. The range is from 1 to 65535.
proxy	Allows the request to be redirected to an HTTP proxy server.
hostname	Name of the HTTP server.
ip-address	IP address of the HTTP server.
proxy_portnum	HTTP proxy server port number. The range is from 1 to 65535.
username	Specifies the username to access the HTTP proxy server.
username	User login name.
running-config	Copies the current system configuration.
disk	Copies the current system configuration to a disk file.
filename	Name of the file to be created on disk.
startup-config	Copies the running configuration to the startup configuration (NVRAM).
disk	Copies the startup configuration to a disk file.
filename	Name of the startup configuration file to be copied to the local disk.
running-config	Copies the startup configuration to a running configuration.
system-status disk	Copies the system status to a disk file.
filename	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.
filename	Name of the file to be created on disk.
remotefilename	Remote filename of the system information file to be created on the TFTP server. Use the complete pathname.

Command Defaults

HTTP server port: 80

Default working directory for sysfs files: /local1

Command Modes

EXEC configuration mode.

Usage Guidelines

The **copy cdnfs** command in EXEC configuration mode copies data files from of the CDNFS to the sysfs for further processing. For example, you can use the **install** *imagefilename* command in EXEC configuration mode 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 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 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 copies technical support information to a a sysfs partition.

Related Commands

Command	Description
install	Installs a new version of the caching application.
reload	Halts a device and performs a cold restart.
show running-config	Displays the current operating configuration.
show startup-config	Displays the startup configuration.
write	Writes or erases the startup configurations to NVRAM or to a terminal session, or writes the MIB persistence configuration to disk.

cpfile

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

cpfile *oldfilename newfilename*

Syntax Description

oldfilename	Name of the file to be copied.
newfilename	Name of the copy to be created.

Command Defaults

None

Command Modes

EXEC configuration mode.

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

Command	Description
copy	Copies the configuration or image files to and from the CD-ROM, flash memory, disk, or remote hosts.
dir	Displays the files in a long-list format.
lls	Displays the files in a long-list format.
ls	Lists the files and subdirectories in a directory.
mkfile	Makes a file (for testing).
rename	Renames a file.
rmdir	Removes a directory.

debug

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

debug *option*

no debug *option*

Syntax Description

option	Specifies the debugger type; see the Usage Guidelines section for valid values.

Command Defaults

debug all: default logging level is ERROR.

Command Modes

EXEC configuration mode.

Usage Guidelines

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** 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, disable the debugging functions by using the **undebug** command (see the "undebug" section on page 2-746 section for more details), and reset the level of logging disk priority to any other setting that you want (for example, **notice** priority).

Table 2-2 shows valid values for the **debug** command options.

Table 2-2 debug Command Options

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

Table 2-2 debug Command Options

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 Autnentication 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 CNNFS.
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.
content-mgr	Debugs the Content Manager.
error	Sets the debug level to error.
trace	Sets the debug level to trace.

Table 2-2 debug Command Options

dataserver	Debugs the data server.
all	Debuts 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.

Table 2-2 debug Command Options

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).
mcast-data-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-data-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.
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.
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.

Table 2-2 debug Command Options

http	Debugs HTTP.
service-router	Debugs the HTTP Service Router.
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.
ip	Debugs Internet Protocol.
bgp	Debugs Border Gateway Protocol.
ospf	Debugs OSPF events.
proximity	Proximity debug commands.
all	All Proximity debugging information.
ippc	Proximity IPPC debugs.
rib	Debugs IP routing table events.
isis	Debugs IS-IS Routing for IP.
adjacency	Debugs IS-IS adjacency information.
all	Debugs all IS-IS debugging.
csnp	Debugs IS-IS Complete Sequence Number PDU (CSNP) information.
dis	Debugs IS-IS DIS election information.
esis	Debugs IS-IS ESIS information.
event	Debugs IS-IS event information.
hello	Debugs IS-IS hello information.
lsp	Debugs IS-IS timer LSP information.
mpls	Debugs IS-IS MPLS information.
psnp	Debugs IS-IS PSNP information.
spf	Debugs IS-IS SPF information.
timer	Debugs IS-IS timer information.
logging	Debugs logging.
all	Debugs all logging functions.

Table 2-2 debug Command Options

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.
rbcp	Debugs the RBCP (Router Blade Configuration Protocol) functions.
rpc	Displays the remote procedure call (RPC) logs.
detail	Displays the RPC logs of priority *detail* level or higher.
trace	Displays the RPC logs of priority *trace* level or higher.

Table 2-2 debug Command Options

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.
agent	SNMP agent debug.
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.

Table 2-2 debug Command Options

srp	Debugs the Service Routing Protocols.
all	Debugs all SRP.
api	Debugs the SRP API.
configuration	Debugs the SRP configuration.
database	Debugs the SRP database.
error	Debugs the SRP error.
function	Debugs the SRP function.
host	Debugs the SRP host.
internal	Debugs the SRP internal.
ippc	Debugs the SRP ippc (inter process command).
ippc-dump	Debugs the SRP ippc (pkt) dump.
key	Debugs the SRP key.
leafset	Debugs the SRP leafset.
lock	Debugs the SRP lock.
multicast	Debugs the SRP multicast.
neighbor	Debugs the SRP neighbor.
packet	Debugs the SRP packet.
private	Debugs the SRP private.
replica	Debugs the SRP replica.
route	Debugs the SRP route.
session	Debugs the SRP session.
srhp-packet	Debugs the SRP srhp packet.
startup	Debugs the SRP startup.
sync	Debugs the SRP sync.
standby	Debugs standby functions.
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.

Table 2-2 debug Command Options

svc	Debugs the Service Registration Daemon and Descriptor Interpreter.
all	Debugs all SVCREG and Descriptor Interpreter Library (DESCI).
desci	DESCI debug commands.
desc	Debugs DESCI desc.
err	DESCI internal error.
ippc	Debugs DESCI ippc (inter process comm).
xml	Debugs DESCI xml.
registry	Service Registry Daemon (SVCREG) debug commands.
err	SVCREG internal error.
if	Debugs SVCREG interface.
ippc	Debugs SVCREG ippc (inter process comm).
svc	Debugs SVCREG svc.
ven	Debugs SVCREG ven.
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.

Table 2-2 debug Command Options

wmt	Debugs the WMT component.
error	Debugs the WMT level 1 functionality. For more information, see the "Using WMT Error Logging" section on page 2-132.
client-ip *cl-ip-address*	(Optional) Debugs the request from a specific client IP address to level 1 (show error).
server-ip *sv-ip-address*	(Optional) Debugs the request to a specific server IP address to level 1 (show error).
trace	Debugs the WMT level 2 functionality.
client-ip *cl-ip-address*	(Optional) Debugs the request from a specific client IP address to level 2 (show error and trace).
server-ip *sv-ip-address*	(Optional) Debugs the request to a specific server IP address to level 2 (show error and trace).

Debugging Keywords

All modules have **debug error** as the default level if they support the **error** keyword; however, when you execute the **show debug** command, the error does not display.

Some modules have two debugging keywords (**error** and **trace**), but you cannot enable both at the same time. See the table above to identify commands with only the **error** and **trace** keywords.

Some modules have the **all** keyword through which you can enable both the **error** and **trace** keywords at the same time. This results in *debug set to everything*. See Table 2-2 to identify commands with the **all** keyword.

Note When debugging is set to trace level, it uses a lot of the CPU on the SE to handle error log writing. When writing the trace-level error logs reaches 100 percent of the CPU usage, 504 timeout error messages start to occur. Therefore, trace-level error logging should not be enabled in production systems.

Debugging the Authsvr

Table 2-3 shows the authsvr debugging commands and provides the corresponding log and error display information.

Table 2-3 Debug Authsvr Command Chart

Command	Debug Log Levels Printed	Show Debugging
undebug authsvr trace	error log	—
undebug authsvr error	error log	—
undebug all	error log	—
debug all	error log	Debug Authsvr error is on.
no debug all	error log	—

Table 2-3 Debug Authsvr Command Chart

Command	Debug Log Levels Printed	Show Debugging
debug authsvr error	error log	Debug Authsvr error is on.
debug authsvr trace	trace error log	Debug Authsvr trace is on.
no debug authsvr trace	error log	—
no debug authsvr error	error log	—

Debugging Cdnfs

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

Using WMT Error Logging

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** command in EXEC configuration mode. 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

Command	Description
logging	Configures system logging (syslog).
show debugging	Displays the state of each debugging option.
undebug	Disables the debugging functions (see also **debug**).

debug ip bgp

To display information relating to the BGP process, use the **debug ip bgp** command in privileged EXEC configuration mode. To disable the display of BGP information, use the **undebug** form of this command.

debug ip bgp {**A.B.C.D.** | **all** | **brib** | **events** | **internal** | **io** | **keepalives** | **list** | **packets** | **rib** | **updates**}

undebug ip bgp {**A.B.C.D.** | **all** | **brib** | **events** | **internal** | **io** | **keepalives** | **list** | **packets** | **rib** | **updates**}

Syntax Description

A.B.C.D.	Displays the BGP neighbor IP address.
all	Displays all BGP debugging information.
brib	Displays the BGP BRIB.
dampening	Displays the BGP dampening.
events	Displays BGP events.
internal	Displays BGP internal information.
io	Displays BGP IO information.
keepalives	Displays BGP keepalives.
list	Displays the BGP list.
packets	Displays the BGP packets.
rib	Displays the BGP RIB.
updates	Displays BGP updates.

Command Defaults

Debugging of the keepalives is turned on upon the start of the BGP daemon.

Command Modes

Privileged EXEC configuration mode.

Usage Guidelines

This command turns on BGP debugging information. When **debug ip bgp** is turned on, the performance of the Proximity Engine may be impacted slightly.

Examples

The following example shows sample output displayed before and after running the **debug ip bgp all** command:

```
ServiceRouter# show debugging ip bgp
Debugs Enabled: Keepalives
ServiceRouter# debug ip bgp all
BGP all information debug is on
ServiceRouter# show debugging ip bgp
Debugs Enabled: Events Internal RIB BRIB Updates Keepalives Packets IO List

ServiceRouter#
```

When the **undebug ip bgp all** command is run, the following output is displayed:

```
ServiceRouter# undebug ip bgp all
```

```
BGP all information debug is off
```

Related Commands

Command	Description
show debugging ip bgp	Displays the debugging flags that have been set for BGP.

debug ip ospf

To display information related to OSPF process, use the **debug ip ospf** command in privileged EXEC configuration mode. To disable the display of OSPF information, use the **undebug** form of this command.

debug ip ospf {**adjacency** [**detail** | **terse**] | **all** [**detail** | **terse**] | **database** [**detail** | **terse**] | **database-timers** | **events** [**detail** | **terse**] | **flooding** [**detail** | **terse**] | **hello** | **lsa-generation** [**detail** | **terse**] | **packets** | **retransmission** | **spf** [**detail** | **terse**] | **spf-trigger** [**detail**]}

undebug ip ospf {**adjacency** [**detail** | **terse**] | **all** [**detail** | **terse**] | **database** [**detail** | **terse**] | **database-timers** | **events** [**detail** | **terse**] | **flooding** [**detail** | **terse**] | **hello** | **lsa-generation** [**detail** | **terse**] | **packets** | **retransmission** | **spf** [**detail** | **terse**] | **spf-trigger** [**detail**]}

Syntax Description

adjacency	Specifies the adjacency events.
detail	Displays detailed neighbor events.
terse	Displays only major events.
all	All OSPF debugging.
database	OSPF LSDB[1] changes.
database-timers	OSPF LSDB timers.
events	OSPF related events.
flooding	LSAs[2] flooding.
hello	Hello packet and DR elections.
lsa-generation	Local OSPF LSA generation.
packets	OSPF packets.
retransmission	OSPF retransmission events.
spf	SPF calculation.
spf-trigger	Show SPF triggers

1. LSDB = link-state database
2. LSAs = link-state advertisement

Command Defaults

Display of information related to the OSPF process is disabled.

Command Modes

Privileged EXEC configuration mode.

Usage Guidelines

When **debug ip ospf** is turned on, the performance of the Proximity Engine may be impacted slightly.

Examples

Add the **detail** or **terse** keywords to each of the following commands to enable detailed or major events respectively.

The following example shows how to enable neighbor adjacency events:

```
ServiceRouter# debug ip ospf adjacency

ServiceRouter#
```

The following example shows how to enable all OSPF debugging:

```
ServiceRouter# debug ip ospf all

ServiceRouter#
```

The following example shows how to enable debugging for OSPF LSDB changes:

```
ServiceRouter# debug ip ospf database

ServiceRouter#
```

The following example shows how to enable debugging for OSPF LSDB timers:

```
ServiceRouter# debug ip ospf database-timers

ServiceRouter#
```

The following example shows how to enable debugging for OSPF-related events:

```
ServiceRouter# debug ip ospf events

ServiceRouter#
```

The following example shows how to enable debugging for LSA flooding events:

```
ServiceRouter# debug ip ospf flooding

ServiceRouter#
```

The following example shows how to enable debugging for hello packets and DR elections:

```
ServiceRouter# debug ip ospf hello

ServiceRouter#
```

The following example shows how to enable debugging for local OSPF LSA generation events:

```
ServiceRouter# debug ip ospf lsa-generation

ServiceRouter#
```

The following example shows how to enable debugging for of OSPF packets:

```
ServiceRouter# debug ip ospf packets

ServiceRouter#
```

The following example shows how to enable debugging for OSPF retransmission events:

```
ServiceRouter# debug ip ospf retransmission

ServiceRouter#
```

The following example shows how to enable debugging for SPF calculations:

```
ServiceRouter# debug ip ospf spf

ServiceRouter#
```

The following example shows how to enable debugging for SPF triggers:

```
ServiceRouter# debug ip ospf spf-trigger

ServiceRouter#
```

Related Commands

Command	Description
show debugging ip ospf	Displays the state of each debugging option for the OSPF process.

debug ip proximity

To debug the transport layer of proximity process in an SR, use the **debug ip proximity** command in privileged EXEC mode. To disable the display of RIB information, use the **no** form of this command.

debug ip proximity {**all** | **ippc** {**connection** | **execute** | **message** | **response** | **send**}}

no debug ip proximity {**all** | **ippc** {**connection** | **execute** | **message** | **response** | **send**}}

Syntax Description

all	Enables all proximity debugging.
ippc	Enables proximity transport logic.
connection	Enables transport connection debugging.
execute	Enables request execution debugging.
message	Enables message creation debugging.
response	Enables received message debugging.
send	Enables sent message debugging.

Command Defaults

None

Command Modes

Privileged EXEC configuration mode.

Usage Guidelines

The **debug ip proximity** command enables debugging of the transport layer of the proximity process in an SR to troubleshoot problems with proximity request and response.

Examples

The following example shows how to :

```
ServiceRouter# debug ip proximity all

ServiceRouter#
```

Related Commands

Command	Description
show debugging ip proximity	Displays the debug options that are enabled for the proximity process.

debug ip rib

To display RIB information, use the **debug ip rib** command in privileged EXEC mode. To disable the display of RIB information, use the **no** form of this command.

debug ip rib [**add-route** | **all** | **delete-route** | **detail** | **mod-route** | **proximity** | **rnh** | **summary**]

no debug ip rib [**add-route** | **all** | **delete-route** | **detail** | **mod-route** | **proximity** | **rnh** | **summary**]

Syntax Description

add-route	Adds route events.
all	Displays all IP routing table events.
delete-route	Deletes route events.
detail	Enables detailed debugging for IP routing.
mod-route	Modifies route events.
proximity	Turns on proximity debugging information.
rnh	Turns on recursive next hop events.
summary	Displays a one-line summary of URIB I/O events.

Command Defaults

None

Command Modes

Privileged EXEC configuration mode.

Usage Guidelines

This command is used to display debug information related to the routing information base (RIB).

Examples

The following example shows how to display the RIB information:

```
ServiceRouter# debug ip rib

ServiceRouter#
```

The following example shows how to add routes:

```
ServiceRouter# debug ip rib add-route

ServiceRouter#
```

The following example shows how to turn on all IP routing table events:

```
ServiceRouter# debug ip rib all

ServiceRouter#
```

The following example shows how to remove routes:

```
ServiceRouter# debug ip rib delete-route

ServiceRouter#
```

The following example shows how to enable detailed debugging for IP routing:

```
ServiceRouter# debug ip rib detail

ServiceRouter#
```

The following example shows how to modify IP routing events:

```
ServiceRouter# debug ip rib mod-route

ServiceRouter#
```

The following example shows how to turn on proximity debugging information:

```
ServiceRouter# debug ip rib proximity

URIB proximity routing information debug is on

ServiceRouter#
```

The following example shows how to enable recursive next hop events:

```
ServiceRouter# debug ip rib rnh

ServiceRouter#
```

The following example shows how to display a one-line summary or URIB I/O events:

```
ServiceRouter# debug ip rib summary

ServiceRouter#
```

Related Commands

Command	Description
show debugging ip rib	Displays the debug options that are enabled for the RIB process.

debug isis

To display information related to IS-IS process, use the **debug isis** command in privileged EXEC configuration mode. To disable the display of IS-IS information, use the **undebug** form of this command.

debug isis [**adjacency** | **all** | **csnp** | **dis** | **esis** | **event** | **hello** | **lsp** | **mpls** | **psnp** | **route-map** | **spf** | **timer**]

undebug isis [**adjacency** | **all** | **csnp** | **dis** | **esis** | **event** | **hello** | **lsp** | **mpls** | **psnp** | **route-map** | **spf** | **timer**]

Syntax Description

adjacency	Displays IS adjacency information.
all	Displays all IS-IS debugging information.
csnp	Displays IS-IS CSNP information.
dis	Displays IS-IS DIS election information.
esis	Displays IS-IS ESIS information.
event	Displays IS-IS event information.
hello	Displays IS-IS hello information.
lsp	Displays IS-IS LSP information.
mpls	Displays IS-IS MPLS information.
psnp	Displays IS-IS PSNP information.
route-map	Displays IS-IS route-map policy information.
spf	Displays IS-IS SPF information.
timer	Displays IS-IS timer information.

Command Defaults

Display of debugging information is disabled.

Command Modes

Privileged EXEC configuration mode.

Usage Guidelines

When **debug isis** is turned on, the performance of the Proximity Engine may be impacted slightly.

Examples

The following example shows how to turn on the debug information for the interaction between IS-IS and the RPM API library:

```
ServiceRouter# debug isis route-map
ServiceRouter#
```

Related Commands

Command	Description
show debugging isis	Displays the debug options that are enabled for the IS-IS process.

debug srp

To turn on SRP debugging information, use the **debug srp** command in Privileged EXEC configuration mode. To turn off the debugging information, use the **no** form of this command.

debug srp *option*

no debug srp *option*

Syntax Description

option	Specifies the category of SRP debugging information to turn on. See Table 2-4 for a list of *option* values.

Command Defaults

None

Command Modes

Privileged EXEC configuration mode.

Usage Guidelines

This command turns on SRP debugging information logging either in the trace file or log file.

The log file for SRP is /local/local1/errorlog/srp_log.current. The *option* argument to the **debug srp** command specifies a keyword indicating the category of SRP debugging information logging to turn on. Table 2-4 lists the values that can be specified in the *option* argument.

Each debugging information message includes a tag that indicates the debugging category. For example, the SRP API debug messages include the tag SRP_DEBUG_API. Table 2-4 lists the tags that are used for each category of debugging information.

To turn off SRP debugging information, use the **undebug srp** command in privileged EXEC configuration mode.

Table 2-4 debug SRP Options

Option	Tag	Description
all	not applicable	Turns on all categories of SRP debugging information.
api	SRP_DEBUG_API	Turns on SRP API debugging information.
configuration	SRP_DEBUG_CONFIG	Turns on SRP configuration debugging information.
database	SRP_DEBUG_DATABASE	Turns on SRP database debugging information.
error	SRP_DEBUG_ERROR	Turns on SRP error debugging information. Usually, thread creation errors, no memory, key not found, and so forth are reported by this log information.
function	SRP_DEBUG_FUNC	Turns on SRP function debugging information.
host	SRP_DEBUG_HOST	Turns on SRP host debugging information.
internal	SRP_DEBUG_INT_DUMP	Turns on SRP internal debugging information.
ippc	SRP_DEBUG_IPPC	Turns on SRP inter-process procedure (IPPC) call debugging information.
ippc-dump	SRP_DEBUG_IPPC_DUMP	Turns on SRP complete IPPC packet debugging information.

Table 2-4 debug SRP Options (continued)

Option	Tag	Description
key	SRP_DEBUG_KEY	Turns on SRP key-related debugging information.
leafset	SRP_DEBUG_LEAFSET	Turns on SRP leafset debugging information.
lock	SRP_DEBUG_LOCK	Turns on SRP lock and unlock debugging information.
multicast	SRP_DEBUG_MCAST	Turns on SRP multicast debugging information.
neighbor	SRP_DEBUG_NEIGHBOR	Turns on SRP neighbor debugging information.
packet	SRP_DEBUG_PACKET	Turns on SRP packet debugging information (for example, packet type, key, and so forth).
private	SRP_DEBUG_PRIVATE	Turns on SRP debugging information related to private variables and operations.
replica	SRP_DEBUG_REPLICA	Turns on SRP replica debugging information.
route	SRP_DEBUG_ROUTE	Turns on SRP route debugging information.
session	SRP_DEBUG_SESSION	Turns on SRP session debugging information.
srhp-packet	SRP_DEBUG_SRHP_PACKET	Turns on SRP service routing host packet (SRHP) debugging information.
startup	SRP_DEBUG_STARTUP	Turns on SRP startup debugging information.
sync	SRP_DEBUG_SYNC	Turns on SRP debugging information related to synchronization among peers.

Examples

The following example shows how to use the **debug srp** command to turn on SRP host and neighbor debugging information logging:

```
ServiceRouter# debug srp host
ServiceRouter# debug srp neighbor
```

Related Commands

Command	Description
show debugging srp	Displays the debug flags that are turned on for the SRP.
undebug srp	Turns off SRP debugging information.

delfile

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

delfile *filename*

Syntax Description

filename	Name of the file to delete.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Use this command to remove a file from a sysfs partition.

Examples

The following example shows how to delete a file:

```
ServiceEngine# delfile /local1/tempfile
```

Related Commands

Command	Description
cpfile	Copies a file.
deltree	Deletes a directory and its subdirectories.
mkdir	Creates a directory.
mkfile	Creates a file (for testing).
rmdir	Removes a directory.

deltree

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

deltree *directory*

Syntax Description

directory	Name of the directory tree to delete.

Command Defaults

None

Command Modes

EXEC configuration mode.

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

Command	Description
delfile	Deletes a file.
mkdir	Creates a directory.
mkfile	Creates a file (for testing).
rmdir	Removes a directory.

device

To configure the mode of operation on a device as a CDSM, SE or SR, use the **device** command in Global configuration mode. 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.

Command Defaults

The default device operation mode is SE.

Command Modes

Global configuration (config) mode.

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, 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** 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.

If you are changing the device mode of an SR or a CDSM back to an SE, 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

Command	Description
show device-mode	Displays the configured or current mode of a CDSM, SE, or SR device.

dir

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

dir [*directory*]

Syntax Description

directory	(Optional) Name of the directory to list.

Command Defaults

None

Command Modes

EXEC configuration mode.

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:

```
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
```

Related Commands

Command	Description
lls	Displays the files in a long list format.
ls	Lists the files and subdirectories in a directory.

direct-server-return

To enable a VIP for direct server return, use the **direct-server-return** command in Global configuration mode. 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.
ip_address	VIP for direct-server-return.

Command Defaults

None

Command Modes

Global configuration (config) mode.

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 2-5 shows the Direct Server Return flow.

Table 2-5 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

Note When issuing the **direct-server-return vip** command on an SE, the DSR VIP IP address cannot be the same as the Origin Server FQDN (OFQDN).

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

Command	Description
show direct-server-return	Displays the Direct Server Return information.

disable

To turn off privileged command in EXEC configuration mode, use the **disable** command in EXEC configuration mode.

disable

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The **disable** command places you in the user-level EXEC shell. To turn privileged EXEC configuration mode back on, use the **enable** command.

Examples

The following example shows how to enter the user-level EXEC configuration mode:

```
ServiceEngine# disable
ServiceEngine>
```

Related Commands

Command	Description
enable	Accesses the privileged EXEC commands.

disk (EXEC)

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

disk {**erase** *diskname* | **mark** *diskname* {**bad** | **good**} | **policy apply** | **recover-cdnfs-volumes** | **recover-system-volumes** | **repair** *diskname* **sector** *sector_address_in_decimal* | **unuse** *diskname*}

Syntax Description

erase	Erases drive (DANGEROUS).
diskname	Name of the disk to be erased (disk00, disk01, and so on).
mark	Marks a disk drive as good or bad.
diskname	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.
policy	Applies disk policy management.
apply	Invokes the disk policy manager for a disk.
recover-cdnfs-volumes	Erases all CDNFS volumes and reboots.
recover-system-volumes	Erases all SYSTEM and SYSFS volumes.
repair	Repairs the drive.
diskname	Name of the disk to be repaired (disk00, disk01, and so on).
sector	Repairs an uncorrectable sector.
sector_address_in_decimal	Name of the sector address in decimal.
unuse	Stops applications from using a disk drive.
diskname	Name of the disk to be stopped for application use (disk01, disk02, and so on).

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The disk space in the CDS software is allocated on a per-file system basis, rather than on a per-disk basis.

Note For details on the Cisco Internet Streamer CDS software disk storage and configuration requirements for SEs, see the *Cisco Internet Streamer CDS 3.2 Software Configuration Guide*.

The CDNFS amounts are reported by the actual usable amounts of storage for applications. Because of 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 disk details** command.

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

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

After upgrading, the disk space allocation remains the same as previously configured.

Remapping of Bad Sectors on Disk Drives

The **disk erase** command in EXEC configuration mode performs a low-level format of the SCSI or SATA disks. This command erases all the content on the disk.

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

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

Note SCSI and SATA drives can be reformatted.

Erasing Disk Drives

The **disk erase** command replaced the **disk reformat** command. This command erases all the content on the disk. The sequence to erase a disk with the **disk erase** and then use the **disk policy apply** commands. If a disk drive continues to report a failure after you have used the **disk erase** command, you must replace the disk drive.

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

Disk Hot Swapping

A new disk is recognized and the RAID is rebuilt when the device is rebooted. After inserting the new disk, enter the **disk policy apply** command to force the Internet Streamer CDS software to detect the new disk and rebuild the RAID.

Note RAID is not supported for generic hardware (UCS servers). These systems have a single un-RAIDed system disk. Any disk replacement requires that the system first be taken off-line.

The disk policy's design, when adding new disks, is to always favor safety. If when a new disk is added, the disk manager detects “degraded” or “bad” system volumes, the new disk is used to repair the system volumes. Thus, the disk manager always strives to have two disks allocated to the system volumes. If when a new disk is added, the system volumes are “normal” or “syncing,” the new disk is added to the cdnfs volume.

Note For the CDE220-2S3i,and the CDE220-2S3, because the system disks are internal drives, if the system disk is “bad,” the CDE should be replaced.

Repairing a Disk

The **disk repair** command re pairs the bad sector, including the proximal sectors. All data on the drive is lost, but the sectors are repaired and available for data storage again. This command provides equivalent functionality as the repair-disk utility. The disk repair command takes approximately three hours to complete per disk; after the repair disk command completes, reboot the SE to ensure all CDS software services are functioning correctly.

Caution The device should be offline before running the **disk repair** command. Because this command involves complex steps, we recommend you contact Cisco Technical Support before running this command.

The **disk repair** command not only repairs the bad sectors, but reformats the entire drive, so all data on the drive is lost. The difference between the **disk repair** command and the **disk erase** command is that the **disk erase** command only re-initializes the file system and does not repair bad sectors.

A minor alarm is set when an LSE is detected. After the sector is repaired with the disk repair command, the alarm is turned off.

```
Minor Alarms:
-------------
     Alarm ID             Module/Submodule     Instance
     -------------------- -------------------- -------------------------
   1 badsector            sysmon               disk11
     May 19 20:40:38.213 UTC, Equipment Alarm, #000003, 1000:445011
     "Device: /dev/sd1, 1 Currently unreadable (pending) sectors"
```

Stopping Applications from Using a Disk Drive

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

Note When executing the **disk unuse** command, any applications using the disk will be terminated. Off-line the device before executing this command.

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

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

Examples

The following example shows how to repair the sector 4660 on disk 02:

```
ServiceEngine# disk repair disk02 sector 4660
```

Note A system disk cannot be unused in a non-RAID system (generic/ucs).

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
To safely remove a RAID SYSTEM disk, the entire drive must be erased. This
operation has little effect on the RAID-ed SYSTEM volumes, as their data can
be resynced. However, because the drive also contains non-RAID CDNFS
data, it will result in loss of all CDNFS data for this drive!
Unuse disk01, erasing all CDNFS data? (Yes/No): yes
disk01 is now unused.
All partitions on disk01 have been erased.

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 view disk details:

```
ServiceEngine# show disk details
disk00: Normal (h02 c00 i00 l00 - mptsas) 476940MB(465.8GB)
disk00/01: SYSTEM 5120MB(5.0GB) mounted internally
disk00/02: SYSTEM 2560MB(2.5GB) mounted internally
disk00/04: SYSTEM 1536MB(1.5GB) mounted internally
disk00/05: SYSFS 32767MB(32.0GB) mounted at /local1
disk00/06: CDNFS 434948MB(424.8GB) mounted internally
disk01: Normal (h02 c00 i01 l00 - mptsas) 476940MB(465.8GB)
Unallocated: 476940MB(465.8GB)
disk02: Normal (h02 c00 i02 l00 - mptsas) 476940MB(465.8GB)
disk02/01: CDNFS 476932MB(465.8GB) mounted internally
```

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

```
ServiceEngine# show disk current
Local disks:
    SYSFS 32.0GB 0.7%
    CDNFS 4616.0GB 99.3%
```

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 %
```

The following example shows how to erase all CDNFS volumes and reboot the SE:

```
ServiceEngine# disk recover-cdnfs-volumes
This will erase all CDNFS volumes.
Any applications using CDNFS, including streaming applications, will be killed and the
system will be rebooted.
Please make sure you have offloaded the SE on the CDSM GUI so the SR is no longer sending
traffic to this SE.
Are you sure you want to proceed? [no] yes Are you really sure you want to proceed to
recover and reload? [yes/no] yes

Stopping all services (this may take several minutes) ...
diskman will now recover CDNFS volumes...
CDNFS recovery complete, rebooting now...
```

Related Commands

Command	Description
disk (Global configuration mode)	Configures how the disk errors should be handled.
show cdnfs	Displays the Internet Streamer CDS network file system information.
show disk	Displays the disk configurations.
show disk details	Displays more detailed SMART disk monitoring information.
show statistics	Displays statistics by module.

disk (Global configuration)

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

disk error-handling {**bad-sectors-mon-period** *minutes* | **reload** | **threshold** {**alarm-bad-sectors** *bad-sectors* | **alarm-remapped-sectors** *remapped-sectors* | **bad-sectors** bad-sectors | **errors** errors}}

no disk error-handling {bad-sectors-mon-period minutes | reload | threshold {alarm-bad-sectors bad-sectors | alarm-remapped-sectors remapped-sectors | bad-sectors bad-sectors | errors errors}}

Syntax Description

error-handling	Configures disk error handling.
bad-sectors-mon-period	Active bad sectors monitoring period (minutes).
minutes	Default value is 1440 minutes (24 hours); 0 disables sector monitoring. The range is from 0 to 525600.
reload	Whether to reload system if SYSFS disk(s) have problems.
threshold	Configure disk error handling thresholds.
alarm-bad-sectors	Configures the bad sector alarm threshold.
bad-sectors	Number of bad sectors allowed before the disk is marked as bad. The range is from 0 to 100. The default value is 15. The value 0 means that the disk should never be marked as bad.
alarm-remapped-sectors	Configure SMARTinfo remapped sectors alarm threshold (hard drives only).
remapped-sectors	Number of remapped sectors before alarm is triggered. Default value is 128 (hard drives only). The range is from 0 to 8192.
bad-sectors	Configure number of allowed (Active) bad sectors before disk is marked bad. **Note** Only applies to bad sectors detected since system boot.
bad-sectors	Number of bad sectors allowed before disk is marked bad. Default value is 30; 0 means the disk is never mark bad. The range is from 0 to 100.
errors	Configure number of allowed disk errors before marking disk bad. **Note** Only applies to disk or sector errors detected since system boot.
errors	The number of disk errors allowed before the disk is marked bad. Default value is 500; 0 means never mark disk bad. The range is from 0-100000.

Command Defaults

Bad sector minutes: 1440

Bad sectors alarm: 15

Remapped sectors: 128

Disk bad sectors: 30

Errors: 500

Command Modes

Global configuration (config) mode.

Usage Guidelines

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. Disk00 is not guaranteed to be the system drive or the 'key' CDNFS drive. For example, the system drives on a 2S6 are internal (disk24 and disk25), and the 'key' CDNSF disk is typically disk00, although it can move to other disks as a result of a missing or bad 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. On a generic UCS system the boot partition resides on the system disk (single disk, no RAID). In the event that this disk dies, the system is unbootable. 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. Monitor the critical disk drives on an SE and report any disk drive errors to Cisco TAC.

In a RAIDed system, if a single system disk fails, the system handles the failure seamlessly (apart from any would be CDNFS partitions). If the 'key' CDNFS disk, typically the lowest numbered disk containing CDNFS, fails the system enters an bad state and must be rebooted. In a non-RAID system, if the system disk fails, the system is no longer boots.

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

- Small Computer Systems Interface (SCSI) or Integrated Drive Electronics (IDE) device error is printed by a Linux kernel.
- Disk device access by an application (for example, an open(2), read(2), or write(2) system call) fails with an EIO error code.
- 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.

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 2-158.

You can remap bad (but unused) sectors on a SCSI drive and SATA drives using the **disk repair** command.

Disk Latent Sector Error Handling

Latent Sector Errors (LSE) are when a particular disk sector cannot be read from or written to, or when there is an uncorrectable ECC error. Any data previously stored in the sector is lost. There is also a high probability that sectors in close proximity to the known bad sector have as yet undetected errors, and therefore are included in the repair process.

The syslog file shows the following disk I/O error message and smartd error message when there are disk sector errors:

Apr 28 21:00:26 U11-CDE220-2 kernel: %SE-SYS-4-900000: end_request: I/O error, dev sdd, sector 4660

Apr 28 21:00:26 U11-CDE220-2 kernel: %SE-SYS-3-900000: Buffer I/O error on device sdd, logical block 582

Apr 28 21:04:54 U11-CDE220-2 smartd[7396]: %SE-UNKNOWN-6-899999: Device: /dev/sdd, SMART Prefailure Attribute: 1 Raw_Read_Error_Rate changed from 75 to 73

Apr 28 21:04:54 U11-CDE220-2 smartd[7396]: %SE-UNKNOWN-6-899999: Device: /dev/sdd, SMART Usage Attribute: 187 Reported_Uncorrect changed from 99 to 97

Apr 28 21:04:54 U11-CDE220-2 smartd[7396]: %SE-UNKNOWN-2-899999: Device: /dev/sdd, ATA error count increased from 1 to 3

Specifying the Disk Error-Handling Threshold

You can configure a disk error-handling threshold to determine how many disk errors or bad sectors can be detected before the disk drive is automatically marked as bad.

The **disk error-handling threshold bad-sectors** command determines how many bad sectors can be detected before the disk drive is automatically marked as bad. By default, this threshold is set to 15. To change the default threshold, use the **disk error-handling threshold bad-sectors** 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.

The **disk error-handling threshold errors** command determines how many disk errors can be detected before the disk drive is automatically marked as bad. By default, this threshold is set to 500. To change the default threshold, use the **disk error-handling threshold errors** command. Specify 0 if you never want the disk drive to be marked as bad.

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

Examples

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

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

Related Commands

Command	Description
disk (EXEC mode)	Allocates the disks among the CDNFS and sysfs file systems.
show disk	Displays the disk configurations.
show disk details	Displays currently effective configurations with more details.

distribution

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

distribution {**failover** {**delivery-service-id** *delivery_service_num* | **delivery-service-name** *delivery_service_name*} [**force**] | **fallback** {**delivery-service-id** *delivery_service_num* | **delivery-service-name** *delivery_service_name*} | **multicast** {**resend** {**all** [**on-demand-only**]| **delivery-service-id** *delivery_service_num* [**object** *url* | **on-demand-only**]| **delivery-service-name** *delivery_service_name* [**object** *url* | **on-demand-only**] | **send-nack-now** | **stop** {**all** | **delivery-service-id** *delivery_service_num* [**object** *url*] | **delivery-service-name** *delivery_service_name* [**object** *url*]} | **primary-ip-fallback** {**forwarder-id** *forwarder_num* | **forwarder-name** *forwarder_name*} | **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 Content Acquirer.
delivery-service-id	Specifies the delivery service ID to be used.
delivery_service_num	Delivery service number. The range is from 0 to 4294967295.
delivery-service-name	Specifies the delivery service name descriptor to be used.
name	Delivery service name.
force	(Optional) Forces a failover regardless of whether the root or forwarder SE is active.
fallback	Forces the temporary Content Acquirer to become a receiver SE.
multicast	Resends or stops multicast distribution.
resend	Resends multicast distribution delivery service.
all	Stops multicast distribution for all delivery services.
on-demand-only	(Optional) Triggers a resend only on demand of content NAK for the delivery service.
object	(Optional) Specifies the URL of object to be stopped.
url	Object URL.
send-nack-now	Generates a NACK for uncompleted objects and sends it to the multicast sender immediately.
stop	Stops multicast distribution delivery service.
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 2-161.
forwarder-id	Specifies the forwarder SE ID that is contacted by the receiver SE.
forwarder_num	Forwarder SE ID.
forwarder-name	Specifies the name of the forwarder SE that is contacted by the receiver SE.
name	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.
delivery_service_num	Delivery service number. The range is from 0 to 4294967295.

object	Forces the distribution of objects to be refreshed on every SE.
object_url	Specifies the object URL that needs to be refreshed on every SE.

Command Defaults None

Command Modes EXEC configuration mode.

Usage Guidelines

Note This command is only available on Cisco Internet Streamer CDS Release 3.1.1.

When the Content Acquirer fails, use the **distribution failover** command in EXEC configuration mode on an SE that is going to be the temporary Content Acquirer to trigger an immediate failover to the temporary Content Acquirer 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 Content Acquirer if its forwarder is an inactive Content Acquirer. If the Content Acquirer has not failed, a failover to the temporary Content Acquirer does not occur if you use the **distribution failover** command in EXEC configuration mode. Use the **distribution failover force** command to force a failover even if the Content Acquirer is active.

Use the **distribution fallback** command on an SE that is currently the temporary Content Acquirer 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 prepositioned (for example, expiration time), and so forth. The metadata is always distributed using unicast. The content can also 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. You can adjust the average interval between NACKs by configuring a NACK interval multiplier for an individual receiver SE. This value (an integer between 0.1 to 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 CDS supports NAT for unicast distribution (see the "NAT Firewall" section on page 2-162 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 NAT address of the forwarder 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

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.

Multicasting Content

Use the **distribution multicast** command to resend or stop metadata transfer. It is important to note that content metadata must be distributed to a receiver before the content itself can be replicated via either multicast or unicast. The meta data is sent to receiver only by unicast. Content metadata specifies what

content to distribute, how the content will be distributed, how the content has been updated, how the content is to be pre-positioned. A multicast receiver rejects a multicast sender's advertisement of a file if the proper content metadata has not arrived yet.

Multicast transmission happens on an SE if the following conditions are met:

- The SE is capable of sending multicast.
- The SE belongs to a multicast-enabled delivery service.
- The SE has an IP multicast address assigned to that delivery service.

Then, the multicast replicator on the SE multicasts out every file of that delivery service to the assigned addresses.

Related Commands

Command	Description
clear	Clears the HTTP object cache, the hardware interface, statistics, archive working transaction logs, and other settings.
show distribution	Displays the distribution information for a specified delivery service.
show statistics distribution	Displays the simplified statistics for content distribution components.

dnslookup

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

dnslookup *line*

Syntax Description

line	Domain name of host on the network.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The **dnslookup** command accepts IPv6 address. If an IPv6 address is specified in the dnslookup command, the server replies to a query including the IPv6 address and the IPv6 address displays in the output of the and **tcpdump** and **netstat** commands and all logs.

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
```

domain

To set the domain ID for the SRP, use the **domain** SRP configuration command. To remove a domain ID, use the **no** or **default** form of the command.

domain [*id*]

[**no** | **default**] **domain** [*id*]

Syntax Description

id	(Optional) A positive 32-bit integer for the domain.

Command Defaults

If the **no domain** command is used, the domain ID is 0.

Command Modes

SRP configuration (config-srp) mode.

Usage Guidelines

This command is used to set the domain ID for an SRP. All Proximity Engines running SRP routing with the same domain ID form a single network if the nodes are found through a bootstrap node. By changing a Proximity Engine's domain, the Proximity Engine leaves its current network.

The **no** and **default** forms of the command replace current domain ID with the default domain ID, which is 0.

Examples

The following example shows how to configure a domain ID with **domain**.

```
ServiceRouter# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ServiceRouter(config)# router srp
ServiceRouter(config-srp)# domain 100
ServiceRouter(config-srp)# end
ServiceRouter#
```

The following example illustrates how **show srp process** command displays the configured domain ID.

```
ServiceRouter# show srp process

Process:
  Domain: 100
  Node Id: 2a2db308fd3dc172940a7902a4db7c16c98c3a32e1b048005bce1e832b6d056f
  Host name: sn-sj88
  Port: 9000
  Interfaces running SRP:
     *GigabitEthernet 1/0, GigabitEthernet 2/0, GigabitEthernet 3/0
```

Related Commands

Command	Description
bootstrap-node	Configures a bootstrap node IP address.
router srp	Enters SRP configuration mode.
show srp process	Displays the basic configurations for SRP.

enable

To access privileged commands in EXEC configuration modes, use the **enable** command in EXEC configuration mode.

enable

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

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

Examples

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

```
ServiceEngine> enable
ServiceEngine#
```

Related Commands

Command	Description
disable	Turns off the privileged EXEC commands.
exit	Exits from interface, Global configuration, or privileged EXEC configuration modes.

enable password

To change the enable password, which is used if **aaa authentication enable enable** is configured, use the **enable password** command in Global configuration mode.

enable password

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

Global configuration mode.

Usage Guidelines

The enable password changes the enable password, which is used if **aaa authentication enable enable** is configured.

Examples

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

```
ServiceEngine> enable password
ServiceEngine#
```

Related Commands

Command	Description
aaa authentication enable enable	Enables authentication.

end

To exit Global configuration mode, use the **end** command in Global configuration mode.

end

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

Global configuration (config) mode.

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

Command	Description
exit	Exits from interface, Global configuration, or privileged EXEC configuration modes.

exec-timeout

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

exec-timeout *timeout*

no exec-timeout

Syntax Description

timeout	Timeout in minutes. The range is from 0–44640. The default is 15.

Command Defaults

The default is 15 minutes.

Command Modes

Global configuration (config) mode.

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 shows how to configure a timeout of 100 minutes:

```
ServiceEngine(config)# exec-timeout 100
```

The following example negates the configured timeout of 100 minutes and reverts to the default value of 15 minutes:

```
ServiceEngine(config)# no exec-timeout
```

Related Commands

Command	Description
sshd	Configures the SSH service parameters.
telnet enable	Enables the Telnet services.

exit

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

exit

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

EXEC, Global configuration (config), and interface configuration (config-if) modes.

Usage Guidelines

Use the **exit** command in any configuration mode to return to EXEC configuration 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 shows how to exit the Global configuration mode and return to the privileged-level EXEC configuration mode:

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

The following example shows how to exit the privileged-level EXEC configuration mode and return to the user-level EXEC configuration mode:

```
ServiceEngine# exit
ServiceEngine>
```

Related Commands

Command	Description
end	Exits configuration and privileged EXEC configuration modes.

expert-mode password

To set the customer configurable password, use the **expert-mode password** command in Global configuration mode.

expert-mode password [**encrypted**] *password*

Syntax Description

encrypted	(Optional) Encrypts the password.
password	The encrypted password.

Command Defaults

None

Command Modes

Global configuration (config) mode.

Usage Guidelines

This is a customer configurable password for allowing to enter engineering mode for troubleshooting purposes. The function prompts the user for the current admin password to verify that the user attempting to set the expert-mode password is authorized to do so. If the user is authenticated, the user is prompted twice to enter the new expert-mode password. The new expert-mode password is encrypted prior to being persisted.

Examples

The following example shows how to configure four external NAT IP addresses:

```
ServiceEngine(config)# expert-mode password encrypted xxxx
New Expert Mode Password: xxxx
Confirm New Expert Mode Password: xxxx
Password successfully changed
```

external-ip

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

external-ip *ip_addresses*

no external-ip *ip_addresses*

Syntax Description

ip_addresses	A maximum of eight external or NAT IP addresses can be configured.

Command Defaults

None

Command Modes

Global configuration (config) mode.

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* 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 shows how to configure 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
```

find-pattern

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

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.
filename	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.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

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

Examples

The following example shows how to search 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

Command	Description
cd	Changes the directory.
dir	Displays the list of files in a directory.
lls	Displays the files in a long list format.
ls	Lists the files and subdirectories in a directory.

flash-media-streaming

To enable and configure Flash Media Streaming, use the **flash-media-streaming** command in Global configuration mode. 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** | **ignore-query-string enable** | **max-bandwidth** *number* | **max-sessions** *number* | **monitoring enable**}}

no flash-media-streaming {**admin-api** [**ip** {**allow** *ip address*}] | **application-virtual-path vod map** *mapping_string* | **enable** | **ignore-query-string enable** | **max-bandwidth** *number* | **max-sessions** *number* | **monitoring enable**}}

On the SR:

flash-media-streaming {**application-virtual-path vod map** *mapping string* | **enable** | **monitoring enable**}

no flash-media-streaming {**application-virtual-path vod map** *mapping string* | **enable** | **monitoring enable**}

Syntax Description

admin-api	Allows accessing admin API from the IP.
ip	Allows an IP Address.
allow	Allows an IP Address.
ip_address	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.
mapping_string	Mapping string.
enable	Enables Flash Media Streaming.
ignore-query-string	Configures Flash Media Streaming to ignore query strings in requests.
enable	Enables ignoring query string in requests.
max-bandwidth	Configures max bandwidth for Flash Media Streaming.
number	Max bandwidth number Kbps. The range is from 1000 to 8000000).
max-sessions	Configures maximum sessions for Flash Media Streaming.
number	Maximum sessions number. The range is from 1 to 15000.
monitoring	Configures Flash Media Streaming monitoring.
enable	Enables monitoring.

Command Defaults

The ignore- query-string is disabled.

Command Modes Global configuration (config) mode.

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, an **application-virtual-path vod** command is available so customers can map to whichever folder they want on the origin server.

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 RTMPcalls 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.

Ignore Query String

Previously, if an RTMP request had a query string in the URL for VOD, the Web Engine could decide whether or not to cache the content based on the Web Engine configuration. However, if the query string in the RTMP URL included the end user and not the stream name, every request would have a different URL because every user has a different query string. This leads to the same content getting cached multiple times.

The **flash-media-streaming ignore-query-string enable** command tells Flash Media Streaming to remove the query string before forwarding the request to the Web Engine in the case of VOD, or before forwarding the request to the forwarder SE in the case of live streaming.

If URL signature verification is required, the sign verification is performed before the query string check is invoked. The URL signing and validation, which adds its own query string to the URL, continues to work independently of this enhancement.

When the **flash-media-streaming ignore-query-string enable** command is entered, for every request in which the query string has been ignored, a message is written to the FMS error log, and the Query String Bypassed counter is incremented in the output of the **show statistics flash-media-streaming** command. The FMS access log on the edge SE contains the original URL before the query string was removed.

The **flash-media-streaming ignore-query-string enable** command affects every VOD and live streaming request and is not applicable to proxy-style requests.

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 is 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 is 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 is mapped to rtmp://Temp4.se.cdsfms.com/bar/foo.flv.

Related Commands

Command	Description
show flash-media-streaming	Displays the Flash Media Streaming information.
show statistics flash-media-streaming	Displays the statistics for Flash Media Streaming.

flooding

To set the flooding threshold for SRP multicast, use the **flooding threshold** SRP configuration command. To restore the default flooding threshold, use the **no** or **default** form of the command.

flooding threshold *value*

[**no** | **default**] **flooding threshold** *value*

Syntax Description

threshold	Configures the flooding threshold.
value	A positive integer for the flooding threshold.

Command Defaults

If **no flooding** command is issued, the default threshold is 50.

Command Modes

SRP configuration (config-srp) mode.

Usage Guidelines

This command is used to set the flooding threshold for SRP multicasting.

SRP protocol uses flooding to send multicast messages for a multicast group if the number of subscribers of the group is equal or more than the value specified in **flooding**. An effective threshold value may improve protocol message overhead. The threshold value depends on the number of nodes in your DHT network. In general, the threshold value should be greater than half and smaller than 3/4 of the total number of DHT nodes in the network.

The **no** or **default** forms of the command replace the current flooding threshold value with the default flooding threshold value (50).

Examples

The following example shows how use the **flooding** command to set a flooding threshold value of 45.

```
ServiceRouter(config)# router srp
ServiceRouter(config-srp)# flooding threshold 45
ServiceRouter(config-srp)# end
ServiceRouter#
```

Related Commands

Command	Description
router srp	Enters SRP configuration mode.

geo-location-server

To redirect requests to different Content Delivery Networks based on the geographic location of the client, use the **geo-location-server** command in Global configuration mode. To cancel the request, use the **no** form of this command.

geo-location-server {**primary** *ip_address_port_num* | **secondary** *ip_address_port_num*}

no geo-location-server {**primary** *ip_address_port_num* | **secondary** *ip_address_port_num*}

Syntax Description

primary	Configures the primary geo location server IP address and port.
secondary	Configure secondary geo location server IP address and port.
ip_address	IP address of the geo location server.
port_num	Port number of the geo location server.

Command Defaults

None

Command Modes

Global configuration (config) mode.

Usage Guidelines

Use the **geo-location-server** command to redirect requests to different CDNs based on the geographic location of the client. You can configure requests from different countries to be redirected to different third party services.

Note A Quova server is mandatory to support this feature.

Examples

The following example shows how to configure a primary geo-location-server:

```
ServiceRouter# geo-location-server primary 171.71.51.140 7000
```

Related Commands

Command	Description
cdn-select	Enables the CDN Selector for third-party service selection.
show cdn-select	Displays the status of the CDN Selector.
show statistics cdn-select	Displays the statistics for the CDN Selector.

gulp

To capture lossless gigabit packets and write them to disk, use the **gulp** command in EXEC configuration mode.

gulp *line*

Syntax Description

line	(Optional) Specifies gulp options, enter **-h** to get help.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The **gulp** utility captures lossless gigabit packets and writes them to disk, as well as captures packets remotely. The **gulp** utility has the ability to read directly from the network.

To view the list of options, enter **gulp --h**.

```
ServiceEngine# gulp --help

Usage: /ruby/bin/gulp [--help | options]
    --help      prints this usage summary
    supported options include:
      -d        decapsulate Cisco ERSPAN GRE packets (sets -f value)
      -f "..."  specify a pcap filter - see manpage and -d
      -i eth#|- specify ethernet capture interface or '-' for stdin
      -s #      specify packet capture "snapshot" length limit
      -r #      specify ring buffer size in megabytes (1-1024)
      -c        just buffer stdin to stdout (works with arbitrary data)
      -x        request exclusive lock (to be the only instance running)
      -X        run even when locking would forbid it
      -v        print program version and exit
      -Vx...x   display packet loss and buffer use - see manpage
      -p #      specify full/empty polling interval in microseconds
      -q        suppress buffer full warnings
      -z #      specify write blocksize (power of 2, default 65536) for long-term capture
      -o dir    redirect pcap output to a collection of files in dir
      -C #      limit each pcap file in -o dir to # times the (-r #) size
      -W #      overwrite pcap files in -o dir rather than start #+1
      -B        check if select(2) would ever have blocked on write
      -Y        avoid writes which would block
```

Table 2-6 lists the gulp options and provides a description of each.

Table 2-6 gulp Options

Option	Description
-d	Decapsulates packets from a Cisco Encapsulated Remote SPAN Port (ERSPAN). Sets the pcap filter expression to "proto gre" and strips off Cisco GRE headers (50 bytes) from the packets captured. (If used with -f option note that arguments are processed left to right).
-f	Specify a pcap filter expression. This may be useful to select one from many GRE streams if using -d, or if not using -d, because filtering out packets in the kernel is more efficient than passing them first through the **gulp** utility and then filtering them out.
-i *eth#*	Specify the network interface to read from. The default is eth1 or the value of the environment variable $CAP_IFACE, if present. Specifying a hyphen (-) as the interface reads a pcap file from the standard input instead. (If you forget the -d option during a live capture, you can decapsulate offline this way.)
-r #	Specify a ring buffer size (in megabytes). Values from 1–1024 are permitted. The default is 100. If possible, the ring buffer is locked into RAM.
-c	Copy and buffer bytes from stdin to stdout—do not read packets from the network and do not assume anything about the format of the data. This may be useful to improve the real-time performance of another application.
-s #	Specify packet capture snapshot length. By default, complete packets are captured. For efficiency, captured packets can be truncated to a given length during the capture process, which reduces capture overhead and pcap file sizes. (If used with the -d option, it specifies the length after decapsulation.)
-x	Use file locking to request (by way of exclusive lock) that this is the only instance of the **gulp** utility running. If other instances are already running, they must be stopped before the **gulp** utility can start with this option.
-X	Override an exclusive lock (-x option) and run anyway. An instance of **gulp** started this way holds a shared lock if no exclusive locks were broken; otherwise, it holds no locks at all (causing a subsequent attempt to get an exclusive lock to succeed).
-v	Print program version and exit.
-V xxxxxxxx	If the string of Xs is wide enough (10 or more), it is overwritten twice per second with a brief capture status update consisting of one digit followed by two percentages. The digit is the number of decimal digits in the actual count of lost packets (0 indicates no drops). The two percentages are the current and maximum ring buffer utilization. The updated argument string can be seen with the ps -x option (or equivalent). If the string of Xs is too short to hold the information above, a more verbose status line is written, twice per second, to standard error instead. The first method is probably more useful to occasionally check on long captures and the second is more convenient while experimenting and setting up a capture.
-p #	Specify the thread polling interval (in microseconds). The reader and writer threads poll at this interval when the ring buffer is full or empty. Polling (even frequently) on modern hardware consumes immeasurably few resources. The default interval is 1000.
-q	Suppress warnings about the ring buffer being full. If input is not from a live capture, no data is lost when the ring buffer fills so the warning can be safely suppressed. If stdin is actually a file, warning suppression happens automatically.
-z #	Specify output write block size. Any power of two between 4096 and 65536. The default is 65536.

Table 2-6 gulp Options (continued)

Option	Description
-o *dir*	Redirects pcap output into a collection of files in the specified directory. Pcap files are named pcap###, where ### starts at 000 and increments. The directory must exist and be writable by the user running the **gulp** utility.
-C #	When using the -o option, start a new pcap file when the old one reaches about # times the size of the ring buffer. The default value is 10 and the default ring buffer size is 100MB; so by default, pcap files grow to about 1000 MB before a new one is started. Since some programs read an entire pcap file into memory when using it, splitting the output into chunks can be helpful.
-W #	Specifies a maximum number of pcap files to create before overwriting them. The default is to never overwrite them. This option allows capturing to occur indefinitely with finite disk space.
-B	This option enables the code to check before each write whether the write would block. When the **gulp** utility exits, it announces whether any writes would have been blocked.
-Y	This option writes which ones would be blocked, but are deferred until they are not blocked.

Examples

The following example shows how to get a basic capture on eth1 with a pcap filter:

```
ServiceEngine# gulp -i eth1 -f "..." > pcapfile
```

The ellipsis (...) refers to the Berkeley Packet Filter (pcap) expressions, such as “host foo.”

The following example shows how to get a capture of the 10 most recent files of a 200 MB ring buffer to 1000 MB files:

```
ServiceEngine# gulp -i eth1 -r 200 -C 10 -W 10 -o pcapdir
```

Related Commands

Command	Description
netmon	Displays the transmit and receive activity on an interface.
netstatr	Displays the rate of change of netstat statistics.
ss	Dumps socket statistics.
tcpmon	Searches all TCP connections.

help

To obtain online help for the command-line interface, use the **help** command in EXEC and Global configuration modes.

help

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

EXEC configuration and Global configuration (config) modes.

Usage Guidelines

You can get help at any point in a command by entering a question mark (**?**). If nothing matches, the help list is 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** command in EXEC configuration mode:

```
ServiceEngine# help
Help may be requested at any point in a command by entering a question mark '?'. If
nothing matches, the help list will be empty and you must backup until entering a '?'
shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a command argument (e.g. 'show ?')
and describes each possible argument.
2. Partial help is provided when an abbreviated argument is entered and you want to know
what arguments match the input (e.g. 'show stat?'.)
```

hostname

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

hostname *name*

no hostname

Syntax Description

name	New hostname for the device; the name is case sensitive. The name may be from 1 to 30 alphanumeric characters.

Command Defaults

The default hostname is the SE model number.

Command Modes

Global configuration (config) mode.

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 (-).
- Maximum length is 30 characters.
- Following characters are considered invalid 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

Command	Description
dnslookup	Resolves a host or domain name to an IP address.
ip	Configures the IP.
show hosts	Displays the IP domain name, name servers, IP addresses, and host table.

install

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

install *imagefile_name*

Syntax Description

imagefile_name	Name of the .bin file that you want to install.

Command Defaults

None

Command Modes

EXEC configuration mode.

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

Command	Description
copy ftp install	Installs an image file from an FTP server onto a local device.
copy http install	Installs an image file from an HTTP server onto a local device.
reload	Halts a device and performs a cold restart.

interface

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

interface {**GigabitEthernet** *slot/port_num* [**autosense** | **bandwidth** {**10** | **100** | **1000**} | **channel-group** *group_interface* | **description** *line* | **full-duplex** | **half-duplex** | **ip** {**access-group** {*access_list_num* {**in** | **out**} | *name*} | **address** {*ip_address_netmask* | **range** *low_num high_num netmask*} | **ipv6** {**access-group** {*access_list_num* {**in** | **out**}| *access_list_name* {**in** | **out**}} | **address** {*range low_num high_num netmask* {*prefix* | *subnet_mask*} | *ip_addr/mask*} | **mtu** *mtu_size* | **shutdown** | **standby** *num* [**priority** *num*] | **tx-queue-limit** *queue_length*] | **PortChannel** *num* [**autosense** | **bandwidth** {**10** | **100** | **1000**} | **description** line | **full-duplex** | **half-duplex** | **ip** *line* | **ipv6** *line* | **lacp** | **shutdown** | **standby** *num* [**priority** num] | **Standby** *group_number* [**description** *line* | **errors** *error_num* | **ip address** {*ip_address_netmask* | **range** *low_num high_num netmask*}| **ipv6 address** {**range** *low_num high_num netmask* {*prefix* | *subnet_mask*} | *ip_addr/mask*} | **shutdown**] | **TenGigabitEthernet** *slot/port_num* [**autosense** | **bandwidth** {**10** | **100** | **1000**} **channel-group** *group_interface* | **description** *line* | **full-duplex** | **half-duplex** | **ip** {**access-group** {*access_list_num* {**in** | **out**} | *name*} | **address** {*ip_address_netmask* | **range** *low_num high_num netmask*} | **ipv6** {*acccess-group* {*access_list_num* {**in** | **out**}| *access_list_name* {**in** | **out**}} | **address** {**range** *low_num high_num netmask* {*prefix* | *subnet_mask*} | *ip_addr/mask*} | **mtu** *mtu_size* | **shutdown** | **standby** *num* [**priority** *num*] | **tx-queue-limit** *queue_length*]

no interface {**GigabitEthernet** *slot/port_num* [**autosense** | **bandwidth** {**10** | **100** | **1000**} | **channel-group** *group_interface* | **description** *line* | **full-duplex** | **half-duplex** | **ip** {**access-group** {*access_list_num* {**in** | **out**} | *name*} | **address** {*ip_address_netmask* | **range** *low_num high_num netmask*} | **ipv6** {**access-group** {*access_list_num* {**in** | **out**}| *access_list_name* {**in** | **out**}} | **address** {*range low_num high_num netmask* {*prefix* | *subnet_mask*} | *ip_addr/mask*} | **mtu** *mtu_size* | **shutdown** | **standby** *num* [**priority** *num*] | **tx-queue-limit** *queue_length*] | **PortChannel** *num* [**autosense** | **bandwidth** {**10** | **100** | **1000**} | **description** line | **full-duplex** | **half-duplex** | **ip** *line* | **ipv6** *line* | **lacp** | **shutdown** | **standby** *num* [**priority** num] | **Standby** *group_number* [**description** *line* | **errors** *error_num* | **ip address** {*ip_address_netmask* | **range** *low_num high_num netmask*}| **ipv6 address** {**range** *low_num high_num netmask* {*prefix* | *subnet_mask*} | *ip_addr/mask*} | **shutdown**] | **TenGigabitEthernet** *slot/port_num* [**autosense** | **bandwidth** {**10** | **100** | **1000**} **channel-group** *group_interface* | **description** *line* | **full-duplex** | **half-duplex** | **ip** {**access-group** {*access_list_num* {**in** | **out**} | *name*} | **address** {*ip_address_netmask* | **range** *low_num high_num netmask*} | **ipv6** {*acccess-group* {*access_list_num* {**in** | **out**}| *access_list_name* {**in** | **out**}} | **address** {**range** *low_num high_num netmask* {*prefix* | *subnet_mask*} | *ip_addr/mask*} | **mtu** *mtu_size* | **shutdown** | **standby** *num* [**priority** *num*] | **tx-queue-limit** *queue_length*]

Syntax Description

GigabitEthernet	Selects a Gigabit Ethernet interface to configure.
slot/port_num	Slot and port number for the selected interface. The slot range is from 1 to 14; the port range is from 0 to 0. The slot number and port number are separated with a forward slash character (/).
autosense	(Optional) Specifies interface autosense.
bandwidth	(Optional) Configures the interface bandwidth.
10	Specifies the interface bandwidth as 10 Mbits per second.
100	Specifies the interface bandwidth as 100 Mbits per second.

1000	Specifies the interface bandwidth as 1000 Mbits per second.
channel-group	(Optional) Configures the EtherChannel group.
group_interface	EtherChannel group to which the interface belongs. The range is 1 to 4.
description	(Optional) Specifies interface specific description.
line	Text describing this interface
full-duplex	(Optional) Specifies full-duplex.
half-duplex	(Optional) Specifies half-duplex.
ip	(Optional) Interface Internet Protocol configuration commands.
access-group	Specifies access control for packets.
acccess_list_num	IP access list (standard or extended).
in	Specifies inbound packets.
out	Specifies outbound packets.
name	Specifies the access-list name.
address	Sets the IP address of the interface.
ip_address	IP address of the interface
netmask	Netmask of the interface.
range	IP address range.
low_num	IP address low range of the interface.
high_num	IP address low range of the interface.
netmask	Netmask of the interface.
ipv6	(Optional) Interface IPv6 configuration commands.
access-group	Specifies access control for packets.
ip_access_list	IP access list (standard or extended).
in	Inbound packets.
out	Outbound packets.
access-list-name	Specifies an access list name.
address	Specifies the IPv6 address of the interface.
range	Specifies the IPv6 address range.
low-num	Specifies the IPv6 address low range of the interface.
high-num	Specifies the IPv6 address high range of the interface.
prefix	Interface prefix. The range is from 1 to 128.
ip_addr/netmask	IPv6 address/netmask of the interface in format X:X:X:X::X/<0-128>.
mtu	Sets the interface Maximum Transmission Unit (MTU).
mtu_size	MTU size in bytes. The range is 576 to 9216.
shutdown	(Optional) Shuts down the specific portchannel interface.
standby	(Optional) Standby interface configuration commands.
interface_group_num	Group number for the selected interface. The range is from 1 to 4.
priority	Sets the priority of the interface. Default value is 100.
standby_group_priority	Set the priority of the interface for the standby group. The range is from 0 to 4294967295.
tx-queue-limit	Sets the interface maximum Transmission Queue Length.

queue_length	Sets the limit on the transmission queue length. The range is from 1000 to 80000.
PortChannel	Selects the Ethernet Channel of interfaces to be configured.
num	Sets the Ethernet Channel interface number. The range is from 1 to 4.
lacp	Specifies Link Aggregation Control Protocol.
Standby	Specifies a standby group number.
standby_group_num	Standby group number. The range is from 1 to 4.
description	(Optional) Standby interface description.
line	Text describing this interface.
errors	Sets the maximum number of errors allowed on this interface.
error_num	Maximum number of errors allowed on this interface for the standby group. The range is from 1 to 2147483647.
ip	Sets the IP address of the standby group.
address	Sets the IP address of the interface.
standby_group_ip_addr	IP address of the standby group.
standby_group_ netmask	Netmask of the standby group.
range	Sets the IP address range of the standby group.
low_range	IP address low range of an interface.
high_range	IP address high range of an interface.
interface_netmask	Netmask of the interface.
TenGigabitEthernet	Selects a ten Gigabit Ethernet interface to configure.

Command Defaults

Standby priority: 100.

Command Modes

Global configuration (config) mode.

Usage Guidelines

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

EtherChannel for Cisco Internet Streamer CDS 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 current link status of each interface.

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.

Configuring Multiple IP Addresses

The Multiple Logical IP Addresses feature supports up to 24 unique IP addresses within the same subnet for the same interface.

When you configure multiple IP addresses on an SE using either the range option or using individual commands, the **show running-config** output displays all the IP addresses individually. The netmask value is unique for each interface, so under a single interface you cannot have multiple IP addresses with different netmask values.

Configuring IPv6

When configuring an IPv6 address on the interface, if <*ipv6addr*> is specified, it must be in the form of hexadecimal using16-bit values between colons (X:X:X:X::X). Optionally, a double colon may be used when consecutive 16-bit values are denoted as zero.

To configure the IPv6 access list on an interface, first configure the Access List using the **access-list enable** command; **<in | out>** means apply for inbound or outbound packets.

```
interface {<GigabitEthernet | Portchannel | Standby | TenGigabitEthernet>} ipv6
access-group <access_ list_number | access_list_name> <in | out>
```

Examples

The following example shows how to create 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 how to remove 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** command in EXEC configuration mode:

```
ServiceEngine# show running-config
.
.
.
interface GigabitEthernet 0/0
description This is an interface to the WAN
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
```

The following example shows how to configure multiple IP addresses using a range command:

```
ServiceEngine(config)# interface PortChannel 2
ServiceEngine(config-if)# ip address range 2.2.2.3 2.2.2.6 255.255.255.0
```

The following example shows a sample output of the **show running-config** command in EXEC configuration mode after configuring multiple IP addresses:

```
ServiceEngine# show running-config
.
interface PortChannel 4
 ip address 2.2.2.3 255.255.255.0
 ip address 2.2.2.4 255.255.255.0
 ip address 2.2.2.5 255.255.255.0
 ip address 2.2.2.6 255.255.255.0
 exit
```

Related Commands

Command	Description
show interface	Displays the hardware interface information.
show running-config	Displays the current operating configuration.
show startup-config	Displays the startup configuration.

ip (Global configuration)

To change initial network device configuration settings, use the **ip** command in Global configuration mode. To delete or disable these settings, use the **no** form of this command.**ip** {**access-list** (see "ip access-list" section on page 201) | **default-gateway** *ip_address* [*gateway_ip_addr*] | **domain-name** *name1 name2 name3* | **name-server** *ip_addresses* | **path-mtu-discovery enable** | **route** *dest_IP_addr dest_netmask default_gateway* [**interface** *source_IP_addr*]}

no ip {**access-list** | **default-gateway** *ip_address* [*gateway_ip_addr*] | **domain-name** *name1 name2 name3* | **name-server** *ip_addresses* | **path-mtu-discovery enable** | **route** *dest_IP_addr dest_netmask default_gateway* [**interface** *source_IP_addr*]}

Syntax Description

access-list	Specifies the access list.
default-gateway	Specifies the default gateway (if not routing IP).
ip_address	IP address of the default gateway.
gateway_ip_addr	(Optional) Gateway IP address (maximum of 14).
domain-name	Specifies domain names.
name1 through *name3*	Domain name (up to three can be specified).
name-server	Specifies the address of the name server.
ip_addresses	IP addresses of the domain server (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.
dest_IP_addr	Destination route address.
dest_netmask	Netmask address.
default_gateway	Gateway address.
interface	Configures source policy routing to route outgoing traffic using the same interface where the request was received.
source_IP_addr	IP address of the interface configured for source policy routing.

Command Defaults

None

Command Modes

Global configuration (config) mode.

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 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 started by the sending device. If a server does not support IP Path MTU Discovery, the receiving device has 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.

Source Policy Routes

To configure source policy routing, use the **ip route** command with the interface option. By using source policy routing, the reply packet to a client leaves the SE on the same interface where the request came in. Source policy routing tables are automatically instantiated based on the interface subnets defined on the system. The policy routes are added automatically to the policy routing tables based on the nexthop gateway of the routes in the main routing table.

When configuring multiple IP address you must configure a default gateway in the same subnet. You can configure multiple gateways (up to 14) .

The CDE220-2S3i supports multiple IP addresses, which includes specifying the default gateway and IP routes. The IP routes, source policy routes, were added to ensure incoming traffic would go out the same interface it came in on. An IP route was added using the **interface** keyword and has the following syntax:

ip route <*dest_IP_addr*> <*dest_netmask*> <*default_gateway*> *interface* <*source_IP_addr*>

In the following example, all destination traffic (IP address of 0.0.0.0 and netmask of 0.0.0.0) sent from the source interface, 8.1.0.2, uses the default gateway, 8.1.0.1. This is a default policy route.

ip route 0.0.0.0 0.0.0.0 8.1.0.1 interface 8.1.0.2

A non-default policy route defines a specific destination (IP address and netmask). The following **ip route** command is an example of a non-default policy route:

ip route 10.1.1.0 255.255.255.0 <*gateway*> interface <*source_IP_addr*>

When upgrading to Cisco Internet Streamer CDS Release 2.5.9 software, any source policy routes configured using the Cisco Internet Streamer CDS Release 2.5.7 software interface keyword are rejected and are not displayed when the **show running-config** command is used. However, because you had to define the default gateway for all the interfaces as part of the multi-port support feature, the equivalent source policy route is automatically generated in the routing table. The following example shows the output for the **show ip route** command after upgrading to Cisco Internet Streamer CDS Release 2.5.9 software with the default source policy routes highlighted in bold and the non-default policy routes highlighted in italics:

```
ServiceEngine# show ip route

Destination      Gateway          Netmask
---------------- ---------------- ----------------
172.22.28.0      8.1.0.1          255.255.255.128
6.21.1.0         0.0.0.0          255.255.255.0
8.2.1.0          0.0.0.0          255.255.255.0
8.2.2.0          0.0.0.0          255.255.255.0
171.70.77.0      8.1.0.1          255.255.255.0
8.1.0.0          0.0.0.0          255.255.0.0
0.0.0.0          8.1.0.1          0.0.0.0
0.0.0.0          8.2.1.1          0.0.0.0
0.0.0.0          8.2.2.1          0.0.0.0

Source policy routing table for interface 8.1.0.0/16
172.22.28.0      8.1.0.1          255.255.255.128
171.70.77.0      8.1.0.1          255.255.255.0
8.1.0.0          0.0.0.0          255.255.0.0
0.0.0.0          8.1.0.1          0.0.0.0

Source policy routing table for interface 8.2.1.0/24
8.2.1.0          0.0.0.0          255.255.255.0
0.0.0.0          8.2.1.1          0.0.0.0

Source policy routing table for interface 8.2.2.0/24
8.2.2.0          0.0.0.0          255.255.255.0
0.0.0.0          8.2.2.1          0.0.0.0
```

If you have a default source policy route where the gateway is not defined as a default gateway, then you must add it after upgrading to Cisco Internet Streamer CDS Release 2.5.9 software. For example, if you had a source policy route with a gateway of 6.23.1.1 for a source interface of 6.23.1.12, and you did not specify the gateway as one of the default gateways, you would need to add it.

If you have a non-default source policy route, then you must add it as a regular static route (without the obsoleted interface keyword) after upgrading to Cisco Internet Streamer CDS Release 2.5.9 software. This route is then added to the main routing table as well as the policy routing table.

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.

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. 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.

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. 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).

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:

- 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.

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 are dropped according to the following guideline:

dP(AFny) >= dP(AFnz) >= dP(AFnx)

where dP (AFny) is the probability that packets of the AFny class are dropped and y denotes the dP within an AFn class.

In the following example, packets in the AF13 class are dropped before packets in the AF12 class, which in turn are dropped before packets in the AF11 class:

dP(AF13) >= dP (AF12) >= 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.

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.

Examples

The following example shows how to configure 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 shows how to configure 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 shows how to configure 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 shows how to configure 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
```

The following example shows how to configure source policy routing for the SE interface assigned with the IP address 192.168.1.5:

```
ServiceEngine(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.1 interface 192.168.1.5
```

Related Commands

Command	Description
ip (Interface configuration)	Configures the interface Internet Protocol.
show ip routes	Displays the IP routing table.

ip (Interface configuration)

To configure the interface Internet Protocol, use the **interface** command in interface configuration mode. To delete or disable these settings, use the **no** form of this command.

ip {**access-group** {*num* {**in** | **out**} {*name* {**in** | **out**} | **address** {*ip_addr netmask* | **range** {*ip_addr_low ip_addr_high netmask*}}

no ip {**access-group** {*num* {**in** | **out**} {*name* {**in** | **out**} | **address** {*ip_addr netmask* | **range** {*ip_addr_low ip_addr_high netmask*}}

Syntax Description

access-group	Specifies access control for incoming or outgoing packets.
num	Specifies an IP access list by number, in standard or extended form. The range is from 1-199.
in	Configures the IP access list that apply to inbound packets.
out	Configures the IP access list that apply to outbound packets.
name	Name of the access list.
in	Configures the access list name inbound packets.
out	Configures the access list name outbound packets.
address	Set the IP address of an interface.
ip-addr	IP address of the interface.
netmask	Netmask of the interface.
range	Specifies the IP address range.
ip_addr_low	IP address low range of an interface.
ip_addr_high	IP address high range of an interface.
netmask	Netmask of the interface.

Command Defaults

None

Command Modes

Interface configuration (config-if) mode.

Usage Guidelines

You can configure multiple IP addresses for Gigabit Ethernet, port channel and Standby interfaces in the SEs. With multiple IP support, the SEs can stream the content under a specific IP while having another stream with different source IP address under the same interface.

The **ip** command configures up to 24 unique IP addresses within the same subnet for the same Gigabit Ethernet, port channel and Standby interface. You can add and delete IP addresses for each interface without affecting other configured IP addresses.

Note All IP addresses configured in the same interface must be in the same subnet.

The **ip range** command adds and deletes an IP address range per interface without affecting other configured IP addresses, and it notifies the SR and CDSM on the added and deleted IP address. The IP address can only be deleted when it is already disassociated from the delivery service. If the delivery service's IP address has been updated, for example from 10.1.1.1 to 10.1.1.5, the service is not interrupted. The new stream uses the new IP address.

Examples

Configuring an IP Address Range

The following example shows how to configure an IP address in a range:

```
ServiceEngine(config)# interface PortChannel 1
ServiceEngine(config-if)# ip address 2.2.2.2 255.255.255.0
ServiceEngine(config-if)# ip address range 2.2.2.3 2.2.2.10 255.255.255.0
ServiceEngine(config-if)# ip address range 2.2.2.12 2.2.2.20 255.255.255.0
```

If the user configures an IP address range but one or more of the IP addresses in the range matched with an already configured IP address, the configuration is still accepted. For example, if interface PortChannel 1 has the following configuration:

```
interface PortChannel 1
ip address 2.2.2.2 255.255.255.0
ip address 2.2.2.3 255.255.255.0
ip address 2.2.2.5 255.255.255.0
ip address 2.2.2.12 255.255.255.0
```

The following configuration is accepted and the IP address in the range (not the same subnet) is rejected:

```
ServiceEngine# configure terminal
ServiceEngine(config)# interface PortChannel 1
ServiceEngine(config-if)# ip address range 2.2.2.3 2.2.2.4 255.255.255.0
ServiceEngine(config-if)# end
```

If the interface PortChannel 1 has the following configuration:

```
interface PortChannel 1
ip address 2.2.2.2 255.255.255.0
ip address 2.2.2.5 255.255.255.0
ip address 2.2.2.12 255.255.255.0
```

And you enter the following commands:

```
ServiceEngine# configure terminal
ServiceEngine(config)# interface PortChannel 1
ServiceEngine(config-if)# ip address range 2.2.3.9 2.2.3.15 255.255.255.0
ServiceEngine(config-if)# end
```

It is an invalid IP address range and an incompatible netmask.

Configuring an IP Address

The following example shows how to configure an individual IP address:

```
ServiceEngine(config)# interface PortChannel 1
ServiceEngine(config-if)# ip address 2.2.2.2 255.255.255.0
ServiceEngine(config-if)# ip address 2.2.2.3 255.255.255.0
ServiceEngine(config-if)# ip address 2.2.2.10 255.255.255.0
```

Removing an IP Address

The following example shows how to remove an IP address range configuration:

```
ServiceEngine(config)# interface PortChannel 1
```

```
ServiceEngine(config-if)# no ip address range 2.2.2.3 2.2.2.10 255.255.255.0
```

The following example shows how to remove an IP address configuration:

```
ServiceEngine(config)# interface PortChannel 1
ServiceEngine(config-if)# no ip address 2.2.2.3 255.255.255.
```

Related Commands

Command	Description
interface (Global configuration)	Configures a Gigabit Ethernet or port channel interface.
show interface	Displays the hardware interface information.
show running-config	Displays the current operating configuration.

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** command in Global configuration modes. 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.
acl_num	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.
acl_name	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.
num	(Optional) Position of condition to delete. The range is from 1 to 500.
deny	(Optional) Causes packets that match the specified conditions to be dropped.
num	IP Protocol Number.
ip address	Source IP address.
any	Any source host.
host	A single host address.
gre	Specifies GRE Tunneling by Cisco.
icmp	Specifies Internet Control Message Protocol.
ip	Specifies Any IP Protocol.
tcp	Specifies Transport Control Protocol.

udp	Specifies User Datagram Protocol.
insert	(Optional) Inserts the conditions following the specified line number into the access list.
num	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).
start_line_num	(Optional) Line number from which the list begins.
end_line_num	(Optional) Last line number in the list.
move	(Optional) Moves the specified entry in the access list to a new position in the list.
old_line_num	Line number of the entry to move.
new_line_num	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.

Command Defaults

An access list drops all packets unless you configure at least one **permit** entry.

Command Modes

Global configuration (config) mode.

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 2-9. For a list of supported UDP and TCP keywords, see Table 2-7 and Table 2-8.

Use access lists to control access to specific applications or interfaces on an SE. An ACL consists of one or more condition entries that specify the kind of packets that the SE drops or accepts 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:

- 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.
- SE is deployed anywhere within the enterprise. As with routers and switches, the administrator wants to limit Telnet and SSH access to the IT source subnets.
- 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 and SSH access to the SE.
- SE is deployed as a reverse proxy in an untrusted environment. The SE administrator wants 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. Use a standard access list for providing access to the SNMP server or to the TFTP gateway or 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 2-7 lists the UDP keywords that you can use with extended access lists.

Table 2-7 UDP Keywords and Port Numbers

CLI Keyword	Description	UDP Port Number
bootpc	BOOTP[1] client service	68
bootps	BOOTP server service	67
domain	DNS[2] 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

1. BOOTP = bootstrap protocol
2. DNS = Domain Name System

Table 2-8 lists the TCP keywords that you can use with extended access lists.

Table 2-8 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

Table 2-8 TCP Keywords and Port Numbers (continued)

CLI Keyword	Description	TCP Port Number
ftp-data	FTP data connections (used infrequently)	20
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 2-9 lists the keywords that you can use to match specific ICMP message types and codes.

Table 2-9 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 DoD[1] 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 one (ICMP) and the type field in the ICMP header set to three (Host Unreachable). This is the most common response. Large numbers of this datagram type on the network are indicative of network difficulties or 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 2-9 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 DF[2] 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 one (ICMP) and the type field in the ICMP header set to five (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 one (ICMP) and the type field in the ICMP header set to four (Source Quench). This datagram may be used in network management to provide congestion control. A source quench packet is issued when a router is beginning to lose packets because of 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 2-9 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.

1. DoD = department of defense
2. DF = do not fragment

Examples

The following example shows how to create an access list to allow all web traffic and to allow only 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

Command	Description
clear ip access-list counters	Clears the IP access list statistical information.
show ip access-list	Displays the access lists that are defined and applied to specific interfaces or applications.

ip ospf priority

To set the router priority, which helps determine the designated router for this network; use the ip ospf priority command in interface configuration mode. To return to the default value, use the **no** form of this command.

ip ospf priority *number_value*

no ip ospf priority *number_value*

Syntax Description

number_value	A number value that specifies the priority of the router (the range is 0 to 255).

Command Defaults

Priority of 1

Command Modes

Interface configuration (config-if) mode.

Usage Guidelines

When two routers attached to a network both attempt to become the designated router, the one with the higher router priority takes precedence. If there is a tie, the router with the higher router ID takes precedence. A router with a router priority set to zero is ineligible to become the designated router or backup designated router. Router priority is configured only for interfaces to multi-access networks (that is, not to point-to-point networks).

Examples

The following example shows how to set the router priority value to 4:

```
ServiceRouter(config)# router ospf
ServiceRouter(config-ospf)# interface GigabitEthernet 2/0
ServiceRouter(config-ospf-if)# ip ospf priority 4
ServiceRouter(config-ospf-if)
```

Related Commands

Command	Description
router ospf	Enables the Open Shortest Path First (OSPF) routing process.

ip rib route

To configure unicast static routes for the Proximity Engine, use the **ip rib route** command in Global configuration mode. To , use the **no** form of the command.

ip rib route *destination prefix netmask* {*gateway ip_addr* | **GigabitEthernet** *num* [*gateway ip_addr*]}

no ip rib route *destination prefix netmask* {*gateway ip_addr* | **GigabitEthernet** *num* [*gateway ip_addr*]}

Syntax Description

destination prefix	Destination network prefix.
netmask	Network mask.
gateway ip_addr	Gateway IP address.
GigabitEthernet	Selects a GigabitEthernet interface to configure.
num	GigabitEthernet slot/port number.

Command Defaults

None

Command Modes

Global configuration mode.

Usage Guidelines

Unicast static routes can be configured for the Proximity Engine. Static routes provide the Proximity Engine the ability to resolve learned BGP route next hops without IGP routing information.

The **show ip rib route static** command displays the static routes. The **show ip static route** command displays the static route configured and stored in the RIB table.

The **ip rib route** command allows static route configuration where the next-hop resolution depends on other static route configuration, The maximum number of static routes that can be configured is 200. The maximum number of equal cost multiple path (ECMP) static routes is 16.

When the next hop cannot be resolved, the static route configuration is not rejected, but the static route is not installed in Routing Information Base (RIB). When the next hop is resolved, the static route is installed automatically.

Examples

The following examples shows how to configure a static route:

```
ServiceRouter(config)# ip rib route 10.1.1.1 255.255.255.0 20.1.1.1
ServiceRouter#
```

The following example shows how to configure a static route with disabled nexthop:

```
ServiceRouter(config)# ip rib route 10.1.1.1 255.255.255.0 gigabitEthernet 2/0
ServiceRouter(config)# ip rib route 20.1.1.1 255.255.255.0 192.168.82.54
ServiceRouter(config)#
```

The following examples shows how to configure a static route on a GigabitEthernet interface:

```
ServiceRouter(config)# ip rib route 10.1.1.1 255.255.255.0 gigabitethernet1/0
```

```
ServiceRouter#
```

The following examples shows how to configure a static route on a GigabitEthernet interface with a gateway IP address:

```
ServiceRouter(config)# ip rib route 10.1.1.1 255.255.255.0 gigabitethernet1/0 20.1.1.1
ServiceRouter#
```

Related Commands

Command	Description
show ip rib route	Displays IP RIB route information.
show ip static route	Displays IP Static route information.

ip router isis

To specify the interfaces to be used for routing IS-IS, use the **ip router isis** command in interface sub-configuration mode under IS-IS configuration mode. To detach the IS-IS process from an interface, use the **no** form of the command.

ip router isis

no ip router isis

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

Interface configuration mode under IS-IS (config-isis-if) configuration mode.

Usage Guidelines

This command is used to specify the interfaces to actively route IS-IS. Before an IS-IS routing process can be attached to an interface, you must assign a network entity title (NET) using the **net** command and enter the interface sub-configuration mode.

Examples

The following example shows how to configure an IS-IS process to be attached and form adjacency on Ethernet interface 1:

```
ServiceRouter(config)# router isis
ServiceRouter(config-isis)# net 49.0001.aaaa.aaaa.aaaa.00
ServiceRouter(config-isis)# interface GigabitEthernet 1/0
ServiceRouter(config-isis-if)# ip router isis
ServiceRouter(config-isis-if)#
```

Related Commands

Command	Description
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

ipv6

To specify the default gateway's IPv6 address, use the **ipv6** command in Global configuration mode. To disable the IPv6 address, use the **no** form of this command.

ipv6 {**access-list** {**extended** {extended_*acess_list_num* [**delete** *num* | **deny** {*protocol_num* {**any** | **host** | *ipv6_addr*} | **gre** {**any** | **host** | *ipv6_addr*} | **icmpv6** {**any** | **host** | *ipv6_addr*} | **ip** {**any** | **host** | *ipv6_addr*} | **tcp** {**any** | **host** | *ipv6_addr*} | **udp** {**any** | **host** | *ipv6_addr*} | **insert** *position_num* {**deny** {*protocol_num* {**any** | **host** | *ipv6_addr*} | **gre** {**any** | **host** | *ipv6_addr*} | **icmpv6** {**any** | **host** | *ipv6_addr*} | **ip** {**any** | **host** | *ipv6_addr*} | **tcp** {**any** | **host** | *ipv6_addr*} | **udp** {**any** | **host** | *ipv6_addr*}} | **permit** {**any** | **host** | *ipv6_addr*}} | **list** [*position_start position_end*] | **move** {*move_from move_to*} | **permit** {*protocol_num* {**any** | **host** | *ipv6_addr*} | **gre** {**any** | **host** | *ipv6_addr*} | **icmpv6** {**any** | **host** | *ipv6_addr*} | **ip** {**any** | **host** | *ipv6_addr*} | **tcp** {**any** | **host** | *ipv6_addr*} | **udp** {**any** | **host** | *ipv6_addr*}}] | *access_list name* [**delete** *num* | **deny** {*protocol_num* {**any** | **host** | *ipv6_addr*} | **gre** {**any** | **host** | *ipv6_addr*} | **icmpv6** {**any** | **host** | *ipv6_addr*} | **ip** {**any** | **host** | *ipv6_addr*} | **tcp** {**any** | **host** | *ipv6_addr*} | **udp** {**any** | **host** | *ipv6_addr*}} | **insert** *position_num* {**deny** {*protocol_num* {**any** | **host** | *ipv6_addr*} | **gre** {**any** | **host** | *ipv6_addr*} | **icmpv6** {**any** | **host** | *ipv6_addr*} | **ip** {**any** | **host** | *ipv6_addr*} | **tcp** {**any** | **host** | *ipv6_addr*} | **udp** {**any** | **host** | *ipv6_addr*}} | **permit**} | **list** [*position_start position_end*] | **move** {*move_from move_to*} | **permit** {*protocol_num* {**any** | **host** | *ipv6_addr*} | **gre** {**any** | **host** | *ipv6_addr*} | **icmpv6** {**any** | **host** | *ipv6_addr*} | **ip** {**any** | **host** | *ipv6_addr*} | **tcp** {**any** | **host** | *ipv6_addr*} | **udp** {**any** | **host** | *ipv6_addr*}}]} | **standard** {*standard_acess_list_num* [**delete** *num* | **deny** {**any** | **host** | *ipv6_addr*} | **insert** *position_num* {**deny** {**any** | **host** | *ipv6_addr*} | **permit** {**any** | **host** | *ipv6_addr*}} | **list** [*position_start position_end*] | **move** {*move_from move_to*} | **permit** {**any** | **host** | *ipv6_addr*} | **default-gateway** *ip_address* | **route** *dest_ip_adder gateway_ip_addr*}

no ipv6 {**access-list** {**extended** {extended_*acess_list_num* [**delete** *num* | **deny** {*protocol_num* {**any** | **host** | *ipv6_addr*} | **gre** {**any** | **host** | *ipv6_addr*} | **icmpv6** {**any** | **host** | *ipv6_addr*} | **ip** {**any** | **host** | *ipv6_addr*} | **tcp** {**any** | **host** | *ipv6_addr*} | **udp** {**any** | **host** | *ipv6_addr*} | **insert** *position_num* {**deny** {*protocol_num* {**any** | **host** | *ipv6_addr*} | **gre** {**any** | **host** | *ipv6_addr*} | **icmpv6** {**any** | **host** | *ipv6_addr*} | **ip** {**any** | **host** | *ipv6_addr*} | **tcp** {**any** | **host** | *ipv6_addr*} | **udp** {**any** | **host** | *ipv6_addr*}} | **permit** {**any** | **host** | *ipv6_addr*}} | **list** [*position_start position_end*] | **move** {*move_from move_to*} | **permit** {*protocol_num* {**any** | **host** | *ipv6_addr*} | **gre** {**any** | **host** | *ipv6_addr*} | **icmpv6** {**any** | **host** | *ipv6_addr*} | **ip** {**any** | **host** | *ipv6_addr*} | **tcp** {**any** | **host** | *ipv6_addr*} | **udp** {**any** | **host** | *ipv6_addr*}}] | *access_list name* [**delete** *num* | **deny** {*protocol_num* {**any** | **host** | *ipv6_addr*} | **gre** {**any** | **host** | *ipv6_addr*} | **icmpv6** {**any** | **host** | *ipv6_addr*} | **ip** {**any** | **host** | *ipv6_addr*} | **tcp** {**any** | **host** | *ipv6_addr*} | **udp** {**any** | **host** | *ipv6_addr*}} | **insert** *position_num* {**deny** {*protocol_num* {**any** | **host** | *ipv6_addr*} | **gre** {**any** | **host** | *ipv6_addr*} | **icmpv6** {**any** | **host** | *ipv6_addr*} | **ip** {**any** | **host** | *ipv6_addr*} | **tcp** {**any** | **host** | *ipv6_addr*} | **udp** {**any** | **host** | *ipv6_addr*}} | **permit**} | **list** [*position_start position_end*] | **move** {*move_from move_to*} | **permit** {*protocol_num* {**any** | **host** | *ipv6_addr*} | **gre** {**any** | **host** | *ipv6_addr*} | **icmpv6** {**any** | **host** | *ipv6_addr*} | **ip** {**any** | **host** | *ipv6_addr*} | **tcp** {**any** | **host** | *ipv6_addr*} | **udp** {**any** | **host** | *ipv6_addr*}}]} | **standard** {*standard_acess_list_num* [**delete** *num* | **deny** {**any** | **host** | *ipv6_addr*} | **insert** *position_num* {**deny** {**any** | **host** | *ipv6_addr*} | **permit** {**any** | **host** | *ipv6_addr*}} | **list** [*position_start position_end*] | **move** {*move_from move_to*} | **permit** {**any** | **host** | *ipv6_addr*} | **default-gateway** *ip_address* | **route** *dest_ip_adder gateway_ip_addr*}

Syntax Description

default-gateway	Specifies the default gateway's IPv6 address.
ip_address	IPv6 address of the default gateway.

access-list	Named access-list.
route	Specifies IPv6 net route.
extended	Specifies extended IPv6 Access List.
extended_access_list_num	Extended IPv6 access-list number. The range is from 100 to199.
extended_access_list_name	Extended IPv6 Access-list name (maximum 30 characters).
delete	(Optional) Deletes a condition.
num	Position of condition to delete. The range is from 1 to 500.
deny	(Optional) Specifies packets to reject.
protocol_num	An IP Protocol Number. The range is from 1 to 255.
any	Any source or destination host.
host	A single host address.
ipv6_addr	Source or Destination IPv6 address, in format X:X:X:X::X/(0-128).
gre	Cisco's GRE Tunneling.
icmpv6	Internet Control Message Protocol.
ip	Any IP Protocol.
tcp	Transport Control Protocol.
udp	User Datagram Protocol.
insert	(Optional) Inserts a condition.
position_num	Position to insert new condition. The range is from 1 to 500.
eq	Matches only packets on a given port number.
gt	Matches only packet with a greater port number.
host	A single host address.
lt	Matches only packets with a lower port number.
neq	Matches only packets not on a given port.
range	Matches only packets in the range of port numbers.
list	(Optional) Lists conditions.
position_start	(Optional) Position of condition to start listing. The range is from 1 to 500.
position_end	(Optional) Position of condition to end listing. The range is from 1 to 500.
move	(Optional) Moves a condition.
move_from	(Optional) Position to move condition from. The range is from 1 to 500.
move_to	(Optional) Position to move condition to. The range is from 1 to 500.
permit	(Optional) Specifies packets to accept.
standard	Specifies Standard IPv6 Access List.
standard_access_list_num	Standard IPv6 access-list number. The range is from 100 to 199.
standard_access_list_name	Standard IPv6 Access-list name (maximum 30 characters).
default-gateway	Defines the default gateway's IPv6 address.
ip_address	Default gateway IPv6 address (maximum of 14), in format X:X:X.
route	Specifies the IPv6 net route.
dest_ip_adder	Destination IPv6 address, in format X:X:X:X::X/<0-128.
gateway_ip_addr	Gateway IPv6 address, in format X:X:X:X::X.

Command Defaults None

Command Modes Global configuration (config) mode.

Usage Guidelines Explosive growth in network device diversity and mobile communications, along with global adoption of networking technologies have resulted in IPv4 addresses getting exhausted. IPv4 address space has a theoretical limit of 4.3 billion addresses. IPv6 quadruples the number of network address bits from 32 bits (in IPv4) to 128 bits. This provides more than enough globally unique IP addresses for every networked device in use.

CDS-IS IPv6 ACL, a permit or deny policy for IPv6 traffic you want to filter is based on source and destination IPv6 address, plus other IPv6 protocol factors such as TCP/UDP, ICMPv6 and GRE, or specify the port number. This command mirrors IPv4:

```
[no] ipv6 access-list {<standard|extended>} {<name|number>}
{<permit|deny|delete|move|insert|list>} {protocol no|protocol
name}[any|host|ipv6addr/prefix] {any|host|ipv6addr/prefix}
```

IPv6 access lists are identified by user selected names. Access lists are defined by a list of “permit” and “deny” statements.

```
[no] ip name-server {<hostname|ipv6addr|ipv4addr>}
[no] ntp server {<hostname|ipv6addr|ipv4addr>}
```

These above configurations should support both IPv6 and IPv4 addresses.

DNS Configuration

The IPv6 address name server must be configured by using the **ipv6 name-server ip-address** command.

Note The Service Router acts as the authoritative DNS server, and supports IPv6 DNS extensions.

If an IPv6 address is configured on the SR for DNS, the communication between the SR and the DNS server is over the IPv6 transport. The IPv4 address of the Service Router must be configured in the DNS server, so that the Service Router can respond to both A and AAAA queries. In this case, the communication between the DNS Server and the SR is over IPv4 transport.

Service Router

Communication between the SE and SR is through the IPv4 stack, including the keep-alive message. If IPv6 is enabled, then the keep-alive message includes the IPv6 address of the SE in the keep-alive message payload. This enables the SR to resolve the SE's IPv6 address correctly.

The SR operates as a DNS Server for the requests that belong to the delivery service to which the SR is associated. The SR is provisioned to respond to A or AAAA queries for the configured Service Routing Domain Name (RFQDN). The query can be on either an IPv4 or IPv6 transport.

The SR accepts the HTTP, RTSP, and RTMP requests and sends back the response by way of the IPv6 transport. The SR also supports the IP-based redirection, and includes the IPv6 address of the SE in the redirect URL. If the redirect URL has the SE host name, the client sends a DNS query to the SR, and the SR responds with the SE’s IPv4 address for the A query and the SE’s IPv6 address for the AAAA query.

The Coverage Zone file supports IPv6 and IPv4 addresses. The network and subnetwork addresses in the Coverage Zone file support CIDR format (IP address with a prefix).

Note The Geo-Location servers do no support IPv6 client configuration; therefore, location-based routing only supports IPv4 addresses.

Examples

The following example shows how to configure an IPv6-related address:

```
ServiceRouter(config)# ipv6 default-gateway fec0::100/64
```

When configuring a static IPv6 prefix route, specify the host ipv6 address and prefix. <*next-hop*> is the IPv6 address of the next-hop to reach the destination prefix. The following example shows how to configure a static IPv6 prefix route:

```
ServiceRouter(config)# ipv6 route <ipv6addr/prefix> <next-hop>
```

Related Commands

Command	Description
clear ipv6	Clears IPv6 ACL counters.
show ipv6	Displays the IPv6 information.
traceroute6	Traces the route to a remote IPv6-enabled host.

isis

To configure IS-IS routing for IP, use the **isis** command in interface configuration mode under route IS-IS configuration mode. To turn off this function, use the **no** form of this command.

isis {**authentication key-chain** *name* {**level-1** | **level-2**} | **authentication-check** {**level-1** | **level-2**} | **authentication-type** {**cleartext** | **md5**} | **circuit-type** [**level-1** | **level-1-2** | **level-2**] | **priority** *priority_value* {**level-1** | **level-2**}}

no isis {**authentication key-chain** *name* {**level-1** | **level-2**} | **authentication-check** {**level-1** | **level-2**} | **authentication-type** {**cleartext** | **md5**} | **circuit-type** [**level-1** | **level-1-2** | **level-2**] | **priority** *priority_value* {**level-1** | **level-2**}}

Syntax Description

authentication	Sets hello authentication key chain.
key-chain	Sets hello authentication key chain.
name	Authentication key chain name.
level-1	Specifies authentication key chain for level-1 IIHs.
level-2	Specifies authentication key chain for level-2 IIHs.
authentication-check	Checks authentication.
authentication-type	Sets hello authentication type.
cleartext	Specifies cleartext.
md5	Specifies HMAC-MD5.
circuit-type	Configures circuit type for interface.
level-1	(Optional) Configures a router for Level 1 adjacency only.
level-1-2	(Optional) Configures a router for Level 1 and Level 2 adjacency.
level-2	(Optional) Configures a router for Level 2 adjacency only.
priority	Sets the priority for DIS election.
priority_value	Priority setting for interfaces. The range is from 0 to 127.

Command Defaults

A Level 1 and Level 2 adjacency is established.

Priority is set to 64 for interfaces.

Authentication-check is on.

Command Modes

Interface configuration mode under IS-IS (config-isis-if) configuration.

Usage Guidelines

Use the **isis authentication key-chain** command to specify the key chain to be used for the interface and the corresponding level. The key chain range cannot exceed 63 characters.

Use the **isis authentication-check** command to enables or disables the checking of received packets for the interface on the corresponding level. When authentication-check is disabled, IS-IS adds authentication to the outgoing packets, but it does not check authentication on incoming packets. This feature allows smooth transition of enabling authentication without disrupting the network operation.

Use the **isis authentication-type** command to specify the md5 or cleartext authentication type for the interface and the corresponding level.

Use the **isis circuit-type** command to specify adjacency levels on a specified interface.

Use the **isis priority** configuration command to configure the priority of a specific interface.

Examples

The following example shows how to specify the key chain to be used for 'GigabitEthernet 3/0', level-1 for the IS-IS process running on that interface:

```
ServiceRouter(config)# router isis
ServiceRouter(config-isis)# interface GigabitEthernet 3/0
ServiceRouter(config-isis-if)# isis authentication key-chain my-key level-1
ServiceRouter(config-isis-if)#
```

The following example shows how to configure the authentication check of interface 'GigabitEthernet 3/0', level-1 for the IS-IS process running on that interface:

```
ServiceRouter(config)# router isis
ServiceRouter(config-isis)# interface GigabitEthernet 3/0
ServiceRouter(config-isis-if)# isis authentication-check level-1
ServiceRouter(config-isis-ifSVCREG internal error
  if    SVCREG interface debugs
  ippc  SVCREG ippc (inter process comm) debugs
  svc   SVCREG svc debugs
  ven   SVCREG ven debugs
)#
```

The following example shows how to configure the authentication type of interface 'GigabitEthernet 3/0' to be md5 level-1 for the IS-IS process running on that interface:

```
ServiceRouter(config)# router isis
ServiceRouter(config-isis)# interface GigabitEthernet 3/0
ServiceRouter(config-isis-if)# isis authentication-type md5 level-1
ServiceRouter(config-isis-if)#
```

The following example shows how to configure the circuit type of interface 'GigabitEthernet 3/0' to be level-1-2 for the IS-IS process running on that interface:

```
ServiceRouter(config)# router isis
ServiceRouter(config-isis)# interface GigabitEthernet 3/0
ServiceRouter(config-isis-if)# isis circuit-type level-1-2
ServiceRouter(config-isis-if)# end
ServiceRouter#
```

The following example shows how to set the priority of interface 'GigabitEthernet 3/0' to 100 for the IS-IS process running on that interface:

```
ServiceRouter(config)# router isis
ServiceRouter(config-isis)# interface GigabitEthernet 3/0
ServiceRouter(config-isis-if)# isis priority 100
ServiceRouter(config-isis-if)# end
ServiceRouter#
```

Related Commands

Command	Description
router isis	Enables the IS-IS routing protocol and specifies the IS-IS process.

is-type

To configure a Proximity Engine to act as a Level 1 (intra-area) router, as both a Level 1 router and a Level 2 (interarea) router, or as an inter-area router only, use the **is-type** IS-IS configuration command. To reset the default value, use the **no** form of this command.

is-type [**level-1**| **level-1-2** | **level-2**]

no is-type [**level-1**| **level-1-2** | **level-2**]

Syntax Description

level-1	(Optional) Router performs only Level 1 (intra-area) routing. This router learns only about destinations inside its area. Level 2 (inter-area) routing is performed by the closest Level 1-2 router.
level-1-2	(Optional) Router performs both Level 1 and Level 2 routing. This router runs two instances of the routing process. It has one link-state packet database (LSDB) for destinations inside the area (Level 1 routing) and runs a shortest path first (SPF) calculation to discover the area topology. It also has another LSDB with link state packets (LSPs) of all other backbone (Level 2) routers, and runs another SPF calculation to discover the topology of the backbone, and the existence of all other areas.
level-2	(Optional) Routing process acts as a Level 2 (inter-area) router only. This router is part of the backbone, and does not communicate with Level 1-only routers in its own area.

Command Defaults

The IS-IS routing process configured is a Level 1-2 (intra-area and inter-area) router.

Command Modes

IS-IS configuration (config-isis) mode.

Usage Guidelines

By default, the first instance of the IS-IS routing process that you configure using the **router isis** command is a Level 1-2 router.

If the network has only one area, there is no need to run both Level 1 and Level 2 routing algorithms. If IS-IS is used for Connectionless Network Service (CLNS) routing (and there is only one area), Level 1 only must be used everywhere. If IS-IS is used for IP routing only (and there is only one area), you can run Level 2 only everywhere. Areas you add after the Level 1-2 area exists are, by default, Level 1 areas.

If the router instance has been configured for Level 1-2 (the default for the first instance of the IS-IS routing process in a Cisco device), you can remove Level 2 (inter-area) routing for the area by using the **is-type** command. You can also use the **is-type** command to configure Level 2 routing for an area, but it must be the only instance of the IS-IS routing process configured for Level 2 on the Cisco device.

Examples

The following example shows how to specify an area router:

```
ServiceRouter(config)# router isis
ServiceRouter(config-isis)# is-type level-2
ServiceRouter(config-isis)#
```

Related Commands

Command	Description
router isis	Enables the IS-IS routing protocol and specifies the IS-IS process.

kernel

To configure the kernel, use the **kernel** command in Global configuration mode. To disable the kernel configuration, use the **no** form of this command.

kernel {kdb | optimization network}

no kernel {kdb | optimization network}

Syntax Description

kdb	Specifies the kernel debugger (kdb).
optimization	Enables kernel performance optimization.
network	Optimizes network performance.

Command Defaults

Kdb is disabled by default.

Command Modes

Global configuration (config) mode.

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.

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
```

key

To create a key ID and enter into key configuration submode, use the **key** command in Global configuration mode. To exit key chain configuration submode, use the **no** form of this command.

key *keyid*

no key *keyid*

Syntax Description

keyid	Key identifier. The range is from 0 to 65535.

Command Defaults

None

Command Modes

Global configuration (config) mode.

Usage Guidelines

Multiple key ID's may be configured under the same key chain. The key chain string cannot exceed 63 characters.

When IS-IS is configured to use a particular key chain for the authentication and the corresponding key chain is not configured in the system, it causes IS-IS to always reject incoming packets that require the key chain.

When a key chain has multiple keys, IS-IS should advertise the first key in the chain. For validation of received packets, it should iterate through all the keys until there is a match.

They **key** command is within the **key chain** command context, not simply the key chain itself.

Examples

The following example shows how to create a key ID and enter the key configuration submode:

```
ServiceRouter(config)# key chain my-key
ServiceRouter(config-keychain)#
```

Related Commands

Command	Description
key chain	Creates a key chain and enter into key chain configuration submode.
key-string	Creates a key string to be used for authentication.
show key chain	Displays the key chains in the system.

key-string

To create a key string to be used for authentication, use the **key chain** command in Key ID configuration submode. To remove the key-string, use the **no** form of this command.

key-string *keyid*

no key-string *keyid*

Syntax Description

keyid	The unencrypted (cleartext) user password.

Command Defaults

None

Command Modes

Key ID configuration submode.

Usage Guidelines

The **key-string** command creates a key string to be used for authentication.

A key string is always valid upon creation.

The Proximity Engine does not support key-string expiration.

You can only create one key-string per key ID.

Key-chain string cannot exceed 63 characters.

Examples

The following example shows how to specify terminal line settings:

```
ServiceRouter(config-keychain-key)# key-string topos123
ServiceRouter(config-keychain-key)#
```

Related Commands

Command	Description
key	Creates a key ID and enters into key configuration submode.
key chain	Creates a key chain and enter into key chain configuration submode.
show key chain	Displays the key chains in the system.

key chain

To create a key chain and enter into key chain configuration submode, use the **key chain** command in Global configuration mode. To exit key chain configuration submode, use the **no** form of this command.

key chain *name*

no key chain *name*

Syntax Description

name	Name of the key chain.

Command Defaults

None

Command Modes

Global configuration (config) mode.

Usage Guidelines

Multiple key ID's may be configured under the same key chain. Key chain string cannot exceed 63 characters.

When IS-IS is configured to use a particular key chain for the authentication and the corresponding key chain is not configured in the system, it results IS-IS to always reject incoming packets that requires the key chain.

When a key chain has multiple keys, IS-IS should advertise the first key in the chain. For validation of received packets, it should iterate through all the keys until there is a match.

Examples

The following example shows how to create a key and enter into key ID configuration submode:

```
ServiceRouter(config)# key chain my-key
ServiceRouter(config-keychain)#
```

The following example shows a complete sample configuration for IS-IS MD5 authentication:

```
ServiceRouter(config)# key chain lsp-key
ServiceRouter(config-keychain)# key 1
ServiceRouter(config-keychain-key)# key-string lsp
ServiceRouter(config-keychain-key)# exit
ServiceRouter(config-keychain)# exit
ServiceRouter(config)# key chain int-key
ServiceRouter(config-keychain)# key 1
ServiceRouter(config-keychain-key)# key-string topos123
ServiceRouter(config-keychain-key)# exit
ServiceRouter(config-keychain)# exit
ServiceRouter(config)# router isis
ServiceRouter(config-isis)# net 10.1111.1111.1111.00
ServiceRouter(config-isis)# is-type level-1
ServiceRouter(config-isis)# authentication-type md5 level-1
ServiceRouter(config-isis)# authentication key-chain lsp-key level-1
ServiceRouter(config-isis)# interface giagabitethernet 1/0
ServiceRouter(config-isis-if)# isis authentication-type md5 level-1
ServiceRouter(config-isis-if)# isis authentication key-chain int-key level-1
```

Related Commands

Command	Description
key	Creates a key chain and enter s into key chain configuration submode.
key-string	Creates a key string to be used for authentication.
show key chain	Displays the key chains in the system.

lacp

To turn on Link Aggregation Control Protocol (LACP), use the **lacp** command in Interface configuration mode. To turn off lacp, use the **no** form of this command.

lacp

no lacp

Syntax Description

This command has no keywords or arguments.

Command Defaults

None

Command Modes

Interface configuration (config-if) mode.

Usage Guidelines

The port channel must be configured on both the switch and the host side before enabling LACP. Speed and duplex must be the same for both the switch and host. To configure LACP on the switch side, every interface must be configured.

For load balancing, the round robin method alone is not supported with LACP.

Examples

The following example shows how to turn on LACP:

```
ServiceEngine(config)# interface portChannel 1
ServiceEngine(config-if)# lacp
```

The following example shows how to turn off LACP:

```
ServiceEngine(config)# interface portChannel 1
ServiceEngine(config)# no lacp
```

The following example shows how to configure the load balancing on a global basis:

```
ServiceEngine(config)# port-channel load-balance
```

This command can also include various load balancing methods:

- dst-ip—Destination IP Address (default)
- dst-mac—Destination Mac Address
- dst-mixed-ip-port—Destination IP Address and Layer 4 port, supported in 6500 and 7600
- dst-port—Destination Layer 4 port
- round-robin—Round Robin
- src-dst-ip—Source and Destination IP Address
- src-dst-ma—Source Destination Mac Address
- src-dst-mixed-ip-port—Source and Destination IP Address and Layer 4 port, supported in 6500 and 7600

- src-dst-port—Source and Destination Layer 4 port
- src-mixed-ip-port—Source IP Address and Layer 4 port, supported in 6500 and 7600
- src-port—Source Layer 4 port

Related Commands

Command	Description
show interface portchannel 1 lacp	Displays the LACP port channel status.
show lacp	Displays LACP information.

line

To specify terminal line settings, use the **line** command in Global configuration mode. 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.

Command Defaults

This feature is disabled by default.

Command Modes

Global configuration (config) mode.

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 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** user command in user EXEC configuration mode.

lls [*directory*]

Syntax Description

directory	(Optional) Name of the directory for which you want a long list of files.

Command Defaults

None

Command Modes

User EXEC configuration mode.

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

Command	Description
dir	Displays a detailed list of files contained within the working directory, including names, sizes, and time created.
ls	Lists the files or subdirectory names within a directory.

location community

To configure the community values that are associated with a Proximity Engine, use the **location community** command in BGP configuration (config-bgp) mode. To remove community values that are associated with a Proximity Engine, use the **no** form of this command.

location community *community_string* [**target** *community_string* | **weight** *num*]

no location community *community_string* [**target** *community_string* | **weight** *num*]

Syntax Description

community_string	Community value string associated with the Proximity Engine.
target	(Optional) Specifies the BGP target community.
weight	(Optional) Specifies the location community weight.
num	Location community weight (the range is 1-7).

Command Defaults

By default, no community values are associated with the Proximity Engine.

Command Modes

BGP configuration (config-bgp) mode.

Usage Guidelines

Use the **location community** command to configure community string values. The configuration includes all community values that represent location. When community values are configured, the Proximity Engine creates and maintains a sorted table of communities within BGP.

The maximum number of location communities allowed for each SE is 128.

The *community_string* can be in one of the following forms:

- Community number, such as 100:3535 or 200:4566
- Interval of community numbers, such as 100:3000 to 100:4000 or 100:5000 to 100:6000

Use the **show ip bgp summary** and s**how ip bgp community** commands to display the community values that are configured for a Proximity Engine.

In order for the proximity function to work, one of the following is required:

- Enabled link-state protocol, such as OSPF or IS-IS for IGP proximity.
- Enabled policy routing protocol, such as BGP for best-path proximity, and one of the IGP (OSPF or IS-IS) is required for next hop resolution.

Note All BGP routes must resolve to IGP next hops or directly connected routes.

Previously location-specific communities must be manually configured using the **location community** command. The **location community weight** command includes the weight that must be assigned to the location community. Also in this release, the order the community strings are displayed in the running-config was changed. In the old releases, community strings were displayed in the order of lengths of the strings, but now they are displayed in alphabetical order.

Location community ranges overlaps are not allowed. Specific location communities are always allowed. Thus if location community 5:1-5:10 is already configured, then 5:2-5:3 is not allowed, 5:2-5:7 is also not allowed. 5:5 is allowed:

```
ServiceRouter(config-bgp)# location community 5:1-5:10 weight 2
ServiceRouter(config-bgp)# location community 5:2-5:3
%BGP: Invalid or overlapping location community.
ServiceRouter(config-bgp)# location community 5:2-5:7
%BGP: Invalid or overlapping location community.
ServiceRouter(config-bgp) #location community 5:5
ServiceRouter(config-bgp)#
```

For the proximity calculation, the most specific match's weight is taken. If there is no such match, then the weight of the range is taken. In the example above, a PTA with location-community 5:5, has weight 1 if both PSA and PTA location-community match, and a PTA with location community 5:1 has weight 2, if PSA And PTA location-community also match.

Examples

The following example shows how use the **location community** command to configure community values for a Proximity Engine.

```
ServiceRouter# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ServiceRouter(config)# router bgp 23
ServiceRouter(config-bgp)# location community 100:3535
ServiceRouter(config-bgp)# location community 100:50-100:100
```

The following example shows how to configure the location community weight of 2:

```
ServiceRouter(config)# router bgp 23
ServiceRouter(config-bgp)# location community 5:1-5:10 weight 2
```

The following example associates a source/PSA with a location-community community 1:1 with a target/PTA with a location community 2:2 and the weight of this association is 2. Also, the source and/or target community might be a range:

```
ServiceRouter(config)# router bgp 23
ServiceRouter(config-bgp)# location community 1:1 target 2:2 weight 2
```

The following example associates the source community 1:1 with all target communities in the range 2:0-2:10 with preference weight 2:

```
ServiceRouter(config)# router bgp 23
ServiceRouter(config-bgp)# location community 1:1 target 2:0-2:10 weight 2
```

The following example associates all source communities in the range 1:0-1:10 with target community 2:2 with preference weight 2:

```
ServiceRouter(config)# router bgp 23
ServiceRouter(config-bgp)# location community 1:0-1:10 target 2:2 weight 2
```

The following example associates all source communities in the range 1:0-1:10 with all target communities in the range 2:0-2:10 with preference weight 2. It can also be seen that a PSA with community 1:1 and a PTA with community 2:2 would satisfy all four commands above since 1:1 falls in the range 1:0-1:10 and 2:2 falls in the range 2:0-2:10. In such scenario, where multiple commands satisfy the matching criteria, the weight is based on the preference level of the commands. The preference level of the four commands above is descending in the following order:

1. Specific source community(1:1)-specific target community(2:2)
2. Specific source community(1:1)-range target community(2:0-2:10)

3. Range source community(1:0-1:10)-specific target community(2:2)
4. Range source community(1:0-1:10)-range target community(2:0-2:10)

```
ServiceRouter(config)# router bgp 23
ServiceRouter(config-bgp)# location community 1:0-1:10 target 2:0-2:10 weight 2
```

Related Commands

Command	Description
proximity algorithm bgp location-community	Specifies that the community-based proximity algorithm be used.

log-adjacency-changes

To configure the router to send a syslog message when an IS-IS neighbor goes up or down, use the **log-adjacency-changes** router configuration command. To turn off this function, use the **no** form of this command.

log-adjacency-changes

no log-adjacency-changes

Syntax Description

This command has no arguments or keywords.

Command Defaults

Sending syslog messages when an IS-IS neighbor goes up or down is enabled.

Command Modes

BGP (config-bgp), IS-IS (config-isis) and OSPF configuration (config-ospf) modes.

Usage Guidelines

This command allows you to know about IS-IS neighbors going up or down without turning on the **debug IS-IS adjacency** command. The **log-adjacency-changes** command provides a higher level view of changes in the peer relationship with less output. This command is enabled by default but messages are sent only when up or down (full or down) events are reported.

Examples

The following example shows how to configure the router to send a syslog message when an IS-IS neighbor's state changes:

```
ServiceRouter(config)# router isis
ServiceRouter(config-isis)# log-adjacency-changes
ServiceRouter(config-isis)#
```

Related Commands

Command	Description
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

logging

To configure system logging, use the **logging** command in Global configuration mode. 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** *loglevel*} | **disk** {**enable | filename** *filename* **| priority** *loglevel* | **recycle** *size*} | **facility** *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.
loglevel	
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.
filename	Specifies the name of the syslog file.
recycle	Overwrites the *syslog.txt* when it surpasses the recycle size.
size	Size of the syslog file in bytes (100000000 to 500000000).
facility	Sets the facility parameter for syslog messages.
facility	
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.
hostname	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.
ip_address	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.
port_num	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.
loglevel	
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.
message_rate	Rate limit (in messages per second) for sending messages to the host. (0 to 10000). Setting the rate limit to 0 disables rate limiting.

Command 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

Command Modes

Global configuration (config) mode.

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 is 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** command. Logging can be configured to send various levels of messages to the console using the **logging console priority** command.

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

Users can log to only a single remote syslog host Use one of the following two commands 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.
- *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 the configured syslog hosts. If the rate limit is exceeded, a message of the day (MOTD) is 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

Command	Description
clear logging	Removes all current entries from the syslog.txt file, but does not make an archive of the file.
debug	Monitors and records caching application functions.
show logging	Displays the system message log confirmation.

log-neighbor-changes

To enable logging of BGP neighbor resets, use the **log-neighbor-changes** BGP configuration command. To disable the logging of BGP neighbor changes, use the **no** form of this command.

log-neighbor-changes

no log-neighbor-changes

Syntax Description

This command has no arguments or keywords.

Command Defaults

If the **log-neighbor-changes** command is not issued, neighbor status change messages are not tracked. One exception is a reset, which is always available as output of the **show ip bgp neighbors** command.

Command Modes

BGP configuration (config-bgp) mode.

Usage Guidelines

The **log-neighbor-changes** command enables logging of BGP neighbor status changes (up or down) and resets for troubleshooting network connectivity problems and measuring network stability. Unexpected neighbor resets might indicate high error rates or high packet loss in the network and should be investigated.

Using the **log-neighbor-changes** command to enable status change message logging does not cause a substantial performance impact, unlike, for example, enabling per BGP update debugging.

In order for the proximity function to work, one of the following is required:

- Enabled link-state protocol, such as OSPF or IS-IS for IGP proximity.
- Enabled policy routing protocol, such as BGP for best-path proximity, and one of the IGP (OSPF or IS-IS) is required for next hop resolution.

Note All BGP routes must resolve to IGP next hops or directly connected routes.

Log neighbor changes help keep track of the adjacency changes. Once you enable the **log-neighbor-changes** command, you can monitor BGP logs to see changes and troubleshoot issues by using the **type-tail errorlog/bgp_log.current** command.

Examples

The following example logs neighbor changes for BGP:

```
ServiceRouter(config)# router bgp 23
ServiceRouter(config-bgp)# log-neighbor-changes
ServiceRouter(config-bgp)#
```

ls

To view a list of files or subdirectory names within a directory, use the **ls** command in EXEC configuration mode.

ls [*directory*]

Syntax Description

directory	(Optional) Name of the directory for which you want a list of files.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

To list the filenames and subdirectories within a particular directory, use the **ls** *directory* 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 shows how to display a list of files within the current working directory:

```
ServiceEngine# ls
/local1
```

The following example shows how to display a list of files within the /local1 directory:

```
ServiceEngine# ls /local1
core_dir
crash
errorlog
logs
lost+found
service_logs
smartfilter
syslog.txt
```

Related Commands

Command	Description
dir	Displays a detailed list of files contained within the working directory, including names, sizes, and time created.
lls	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.
pwd	Displays the present working directory of the SE.

lsp-mtu

To set the maximum transmission unit (MTU) size of IS-IS LSPs, use the **lsp-mtu** IS-IS configuration command. To set the MTU to it's default value, use the **no** form of this command.

lsp-mtu *size*

no lsp-mtu *size*

Syntax Description

size	Maximum number of bytes allowed in LSPs (the range is 128 to 4352).

Command Defaults

The default size is 1497 bytes.

Command Modes

IS-IS configuration (config-isis) mode.

Usage Guidelines

The LSP MTU size describes the amount of information that can be recorded in a single LSP. The **lsp-mtu** command is used to configure the maximum number of bytes allowed in an LSP. If this command is not configured, IS-IS uses the default size of 1500 bytes while sending LSPs for Gigabit Ethernet. Use the **no lsp-mtu** command to configure the maximum number of bytes allowed in an LSP at the default value of 1497 bytes.

Examples

The following example shows how to configure the MTU size to be 1400 bytes.

```
ServiceRouter(config)# router isis
ServiceRouter(config-isis)# lsp-mtu 1400
ServiceRouter(config-isis)# end
ServiceRouter#
```

Related Commands

Command	Description
router isis	Enables the IS-IS routing protocol and specifies the IS-IS process.

mkdir

To create a directory, use the **mkdir** command in EXEC configuration mode.

mkdir *directory*

Syntax Description

directory	Name of the directory to create.

Command Defaults

None

Command Modes

EXEC configuration mode.

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:

```
ServiceEngine# mkdir /local1/mydir
```

Related Commands

Command	Description
dir	Displays a detailed list of files contained within the working directory, including names, sizes, and time created.
lls	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.
ls	Lists the files or subdirectory names within a directory.
pwd	Displays the present working directory of the SE.
rmdir	Removes a directory from the SE file system.

mkfile

To create a new file, use the **mkfile** command in EXEC configuration mode.

mkfile *filename*

Syntax Description

filename	Name of the file that you want to create.

Command Defaults

None

Command Modes

EXEC configuration mode.

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

Command	Description
lls	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.
ls	Lists the files or subdirectory names within a directory.
mkdir	Creates a new directory or subdirectory in the SE file system.

model

To change the CDE250 platform model number after a remanufacturing or rescue process, use the **model** command in EXEC configuration mode.

model {**cde250-2S10** | **cde250-2S6** | **cde250-2S8** | **cde250-2S9**}

Syntax Description

cde250-2S10	Configures this platform as CDE250-2S10.
cde250-2S6	Configures this platform as CDE250-2S6.
cde250-2S8	Configures this platform as CDE250-2S8.
cde250-2S9	Configures this platform as CDE250-2S9.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Use the **model** command to change the CDE250 model type. Table 2-10 shows the internal and external drives for the CDE250 models.

Table 2-10 CDE250 Model Drives

CDE250 Variation	Internal Drives	External Drives
2S6	Intel 100GB LV SSD	Intel 300GB PVR SSD x 24
2S8	Intel 100GB LV SSD	Intel 300GB PVR SSD x 24
2S9	Intel 100GB LV SSD	Intel 300GB PVR SSD x 12
2S10	Intel 100GB LV SSD	Intel 300GB PVR SSD x 24

Examples

The following example shows how to change the CDE250 to model 2S9:

```
ServiceEngine# model CDE250-2S6

This platform is already a CDE250-2S6.

ServiceEngine#
```

movie-streamer

To enable and configure the Movie Streamer server, use the **movie-streamer** command in Global configuration mode. To disable the Movie Streamer, use the **no** form of this command.

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*}

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.
num	Client idle timeout, in seconds. The range is from 0 to 300.
rtp-timeout	Sets the RTP timeout.
origin-server	Configures the advanced origin server.
idle-interval	Sets the origin server idle interval.
num	Server idle interval, in seconds. The range is from 1 to 10.
broadcast	Configures the Movie Streamer live broadcast.
port-list	Specifies a port list.
num	Broadcast list number. The range is from 1 to 1024.
port_num	Broadcast port number.
cache	Configures the Movie Streamer cache.
age-multiplier	Sets the Movie Streamer cache heuristic modifier.
num	Expiration time as a percentage of their age. The range is from 0 to 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.
num	Maximum time to live. The range is from 1 to 1825.
hours	Specifies the maximum time to live units, in hours.
num	Maximum time to live. The range is from 1 to 43800.
minutes	Specifies the maximum time to live units, in minutes.
num	Maximum time to live. The range is from 1 to 2628000.
seconds	Specifies the maximum time to live units, in seconds.

num	Maximum time to live. The range is from 1 to 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.
num	The maximum concurrent sessions. The range is from 1 to 16000.
proxy	Configures the Movie Streamer proxy.
outgoing	Configures the outgoing proxy.
rtsp	Configures the outgoing RTSP proxy.
host	Specifies the outgoing proxy server.
ip_address	IP address of outgoing proxy server.
port_num	Port number of outgoing proxy server. The range is from 1 to 65535.
transport-src-address	Specifies the source IP address to be set in transport header (useful if behind NAT).
ip_address	Source IP address in transport header.

Command Defaults

days: 1
hours: 72
minutes: 4320
seconds: 259200

Command Modes

Global configuration (config) mode.

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 to 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
```

The following example shows how to set the original server interval to 5 second:

```
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 their age's 50%:

```
ServiceEngine(config)# movie-streamer cache age-multiplier 50
```

The following example shows how to set the cache content max ttl to 100 days:

```
ServiceEngine(config)# movie-streamer cache max-ttl days 100
```

The following example shows how to set the max concurrent sessions to 7000:

```
ServiceEngine(config)# movie-streamer max-concurrent-sessions 7000
```

The following example shows how to set the out going proxy:

```
ServiceEngine(config)# movie-streamer proxy outgoing rtsp host 10.74.61.98 554
```

The following example shows how to set the source the IP of the transport header while behind NAT:

```
ServiceEngine(config)# movie-streamer transport-src-address 10.74.61.99
```

Related Commands

Command	Description
show movie-streamer	Displays the Movie Streamer configuration.
show statistics movie-streamer	Displays statistics for the 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 *mtu_size*

no mtu *mtu_size*

Syntax Description

mtu_size	MTU packet size in bytes (576 to 1500).

Command Defaults

The default MTU packet size for an Ethernet interface is 1500 bytes.

Command Modes

Interface configuration (config-if) mode.

Usage Guidelines

The MTU is the largest size of IP datagram that can be transferred using a specific data link connection. Use the **mtu** command to set the maximum packet size in bytes.

Examples

The following example shows how to set the MTU packet size as 1500 bytes:

```
ServiceEngine(config-if)# mtu 1500
```

The following example shows how to reset the MTU packet size:

```
ServiceEngine(config-if)# no mtu 1500
```

Related Commands

Command	Description
show interface	Displays the hardware interface information.
show running-config	Displays the current running configuration information on the terminal.
show startup-config	Displays the startup configuration.

multicast (Global Configuration)

To configure multicast options, use the **multicast** command in Global configuration mode. To disable individual options, use the **no** form of this command.

multicast {**client** {**receiver enable** | **sender enable**} | **fixed-carousel enable** | **max-concurrent-jobs** *number_jobs* | **priority-weight** *num* | **sender-delay** *delay*}

no multicast {**client** {**receiver enable** | **sender enable**} | **fixed-carousel enable** | **max-concurrent-jobs** *number_jobs* | **priority-weight** *num* | **sender-delay** *delay*}

Syntax Description

client	Selects multicast sender or receiver.
receiver	Configures multicast receiver.
enable	Enables the multicast client for receiver.
sender	Configures multicast sender.
enable	Enables the multicast client for the sender.
fixed-carousel enable	Enable fixed carousel sending, regardless of receiver feedback. The intelligent carousel will be disabled, which does carousel based on receiver feedback. This configuration is applicable only to primary sender and will be removed if this SE is moved to backup sender.
max-concurrent-jobs	Specifies the maximum number of jobs that can be scheduled concurrently for multicast distribution.
number_jobs	Maximum number of jobs (1–50). The default is 5.
priority-weight	(Optional) Specifies the percentage of multicast bandwidth that is used for priority-based scheduling.
num	Bandwidth percentage to be used for priority-based scheduling. The range is from 0 to 100.
sender-delay	Sets the multicast sender delay time.
delay	Delay time in seconds (480–7200).

Defaults

Sender Delay: 960 seconds.

Maximum Concurrent Jobs: 5

Priority Weight: 50%

Command Modes

Global configuration mode.

Usage Guidelines

Note This command is only available on Cisco Internet Streamer CDS Release 3.1.1.

In the CDS, content is replicated through a channel distribution architecture. Content in channels can be transmitted by unicast pull, or if multicasting is enabled, by multicast push. Multicasting allows efficient distribution of content to multiple SEs and is useful when many end users are interested in the same content. The Internet Streamer CDS software supports Pragmatic General Multicast (PGM)-based multicast replication using either satellite or multicast-enabled terrestrial infrastructures.

Multicast delivery enables the distribution of streaming media by allowing different receiving devices on the IP multicast to receive a single stream of media content from the SE simultaneously. This method 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 content from the same channel, can subscribe. The delivering device sends content to the multicast address set up at the SE, from which it becomes available to all subscribed receiving devices.

To take advantage of multicasting, all devices, including SEs, routers, and clients, must be multicast enabled. For this reason, multicasting is mostly used in local networks where routers can be configured for multicasting. Multicast delivery over the Internet can only be accomplished when all the devices that participate in the multicast have been enabled for multicasting.

For multicast content replication, SEs are grouped into multicast clouds. A multicast cloud consists of one sender SE, an optional backup sender SE, and at least one receiver SE in a hub and spoke topology. All the SEs in one multicast cloud share a unique advertisement address that allows them to communicate multicast session information. The multicast cloud is then associated with one or more multicast-enabled channels.

In pull-based unicast content distribution, a unicast receiver pulls file data out of the proper forwarder (or root SE) when a client requests the content. In multicast content distribution, the sender SE in a multicast cloud proactively pushes content into the cloud according to a preconfigured schedule.

The receiver SEs listen on the advertisement IP address for information on the content to be replicated from the sender and decide whether to accept an advertisement and whether to receive the content.

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 the content will be retrieved, how recently the content has been updated, how the content is to be pre-positioned (for example, the expiration time), and so forth. The metadata is always distributed using unicast. The content, however, can be replicated using either multicast or unicast. A multicast receiver rejects the multicast sender's advertisement of a file if the proper content metadata has not arrived. During the content distribution process, both the content and its associated information describing the content, called the metadata, are distributed. A multicast receiver does not accept any multicast content unless it has already received the associated metadata for that particular content.

Use the **multicast fixed-carousel enable** command to enable fixed-carousel sending. Carousel sending, which refers to the multicast retransmission of content, allows receivers who join a multicast group after a distribution has ended or who miss some content to receive the content without requiring a unicast transmission. By default, the SE uses intelligent carousel sending, which means that the retransmission is guided by feedback from the content receivers. Late-joining receivers or receivers that missed some content send a negative acknowledgement (NACK) to the sender for any files that were not received.

Fixed-carousel sending causes the content to be sent without depending on any receiver feedback. When this feature is enabled, the SE continuously retransmits the content after waiting for the time specified by the **sender-delay** option. You can use the **fixed-carousel** option when sending the content to receivers, which do not send NACKs to the sender. This configuration is allowed only for the primary sender and is not supported for an SE configured as a backup sender. Use the **no multicast fixed-carousel enable** command to disable fixed-carousel sending and to restore the default configuration.

Use the **multicast max-concurrent-jobs** command option to set the maximum number of objects that can be scheduled concurrently for multicast distribution. When networks are reliable or the size of files being multicast is small, we recommend that you set the maximum number of concurrent objects to 50. However, when networks are unreliable or the size of files being multicast is large, a smaller number of concurrent objects (for example, five) is recommended. The default maximum number of jobs is five.

The **priority-weight** option allows you to change the percentage of multicast bandwidth that is used for priority-based scheduling. By default, 50 percent of the bandwidth is allocated for a priority-based queue and 50 percent is allocated for a time-based, first in, first out (FIFO) queue. The time-based queue allows the system to process lower-priority traffic in a timely way even when it frequently receives large, high-priority requests.

Multicast Sender Delay

The multicast sender delay interval is the amount of time before each multicast transmission begins. A period of delay before the actual multicast transmission begins is required to allow the content metadata time to propagate to the receiver SE. The metadata contains the content file and configuration information that is necessary for the successful transmission of content files. The sender delay parameter is used to configure an extra delay before a multicast transmission can begin.

When configuring the sender delay interval, you must take into account that the content metadata must first propagate to the receiver before the multicast transmission can begin. During a multicast session, a receiver SE sends out periodic requests for files that it has not received. The sender retransmits files only as requested by the receiver SE. A multicast receiver will reject a multicast sender's advertisement of a file if the associated content metadata has not arrived. The sender delay option allows you to configure enough time for the metadata to propagate to the receiver, and avoid having the receiver reject the multicast sender's advertisement of a file.

To configure the sender delay interval, use the multicast sender-delay global configuration command on a sender SE. The **sender-delay** option controls the length of time that the multicast sender must wait for its associated metadata to propagate to the multicast receivers. The default delay time value is 960 seconds, the minimum is 480 seconds, and the maximum is 7200 seconds. You can configure the duration of the delay based on your expectation or best guess of the amount of time required for the metadata to be propagated. The system takes this user-configured sender delay value and delays the multicast transmission for a period defined by the sender delay.

Note The sender delay interval cannot be configured using the CDSM GUI. You must configure the sender delay interval using the CLI of the sender SE.

Examples

The following example shows how to enable the multicast client for the receiver on an SE:

```
ServiceEngine(config)# multicast client receiver enable
```

Related Commands

Command	Description
multicast (EXEC configuration	Generates multicast packets and test connectivity through multicast routers.
show multicast	Shows whether multicast sender and receiver are enabled or disable.

multicast (EXEC Configuration)

To generate multicast packets and test connectivity through multicast routers, use the **multicast** command in EXEC configuration mode.

multicast connectivity-test {**cloud-id** *cloud_id* [**duration** *duration_num* [**message-length** | **mullticast-address** *multicast_addr* | **output-style** {**detail** | **error**} | **port** *port_num*] | **packet-count** *packet_num*] | **cloud-name** *name* [**duration** *duration* [**message-length** | **multicast-address** *multicast_addr* | **output-style** {**detail** | **error**} | **port** *port_num*] | **packet-count** *packet_num*] | **receive** *multicast_ip_addr* **interface** *interface_ip_addr* | s**end** *multicast_ip_addr ttl* **interface** *interface_ip_addr* | **streamer** *receiver_ip_addr* {*receiver_ip_addr* | **multicast-address** *multicast_addr* [**duration** *duration* [**FEC-size** *size* | **max-transfer-rate** *rate* | **message-length** | **output-style** {**detail** | **error**} | **port** *port_num*] | **packet-count** *packet_num* | **time-to-live** *ttl*]}}

Syntax Description

connectivity-test	Verifies multicast connectivity between a sender and multiple receivers.
cloud-id	Sends Pragmatic General Multicast (PGM) packets to the multicast cloud.
cloud_id	Cloud ID. The range is from 0 to 4294967295.
duration	(Optional) Configures the length of time over which PGM packets are to be sent to receiver SEs. This is the default option for **multicast-address**.
duration	Number of seconds that PGM packets are sent to receiver SEs. The range is from 30 to 3600; suggested number is 180.
message-length	(Optional) Message length to send.
multicast-address	(Optional) Configures the multicast IP address to be used for sending PGM packets. When you use the **cloud-id** or **cloud-name** option, you can choose not to specify the multicast address. When the multicast address is not specified, the advertising IP address specified in the multicast cloud configuration is used as the multicast address.
multicast_addr	Multicast Address to use for generating PGM Packets.
output-style	(Optional) Define the output display style.
detail	Prints the Detailed Report.
error	Prints the Error Report.
port	(Optional) Destination port to send packets.
port_num	Destination port to send packets. Range is 1025 to 65535; suggested amount is 7000.
packet-count	(Optional) Configures the number of PGM packets to be sent to receiver SEs.
packet_num	Number of PGM packets to send each receiver SE. The range is from 50 to 4096; suggested number is 100.
cloud-name	Sends PGM packets to the multicast cloud.
cloud-name	Name of the cloud.
receive	Receives PGM packets from the multicast address.
multicast_ip_addr	Multicast IP address to listen for PGM Packets.
interface	Interface to be used for Multicast.
interfrace_ip_addr	Interface IP address.

send	Sends PGM packets to the multicast address.
ttl	Time to Live for the multicast packet. Range is from 1 to 255; suggested is 255.
streamer	Sends PGM packets to receiver SEs.
receiver_ip_addr	IP Address of the Receiver SE (max up to 20 Receivers) to check the multicast connectivity.
FEC-size	(Optional) Configures the appending of forward error correction (FEC) redundancy bytes.
size	Number of FEC redundancy bytes to be appended (8–128). The values must be powers of 2 (for example, 8, 16, 32, or 64). The default is 8.
max-transfer-rate	(Optional) Configures the maximum bandwidth that can be used for this multicast transmission.
rate	Maximum Transfer Rate to generate PGM Packets. The range is from 56 to 1000000; suggested is 128Kb.
time-to-live	(Optional) Configures the maximum number of hops permitted for PGM packets before they expire on the network. For each hop, the original specified TTL is decremented by 1. When the TTL reaches 0, PGM packets expire and are no longer forwarded through the network.

Command Defaults

Duration: 180 seconds

Packet Count: 100

FEC Size: 8

Maximum Transfer Rate: 128 kbps

Port: 7000

Time-to-live: 255

Message Length: 1024

Output Style: Detail Report

Command Modes

EXEC configuration mode.

Usage Guidelines

Note This command is only available on Cisco Internet Streamer CDS Release 3.1.1.

You can use the **multicast connectivity-test** command to test multicast connectivity within the CDS network. The **multicast connectivity-test** command options run pgmrategen (the PGM packet generation application) and pgmratemon (the PGM packet receiver application) in the background to test multicast connectivity. These applications use the PGM protocol, which allows a receiver to report lost data and to request retransmission from the sender. With PGM, the sender multicasts sequenced data packets, and the receivers reply with unicast negative acknowledgments (NACKs) when data packets are missing from the expected sequence. Network elements forward the NACKs to the multicast sender and confirm each hop by multicasting a NACK confirmation on the interface on which the NACK was received.

Multicast Forward Error Correction

Forward error correction (FEC) is a type of data encoding that protects transmissions against errors, without requiring retransmission. The FEC number denotes the number of packets that will be encoded into one FEC transmission group. A higher FEC number means that the transmission group size is larger. The multicast may be more error-resistant, but there will also be more computational overhead on the multicast sender and receivers. No bandwidth overhead is related to FEC.

The FEC default value is 8. If the multicast sender device is a high-end SE model, you can set this number higher to improve multicast reliability when your network connectivity has a high uniform loss rate. However, we do not recommend that you set this number beyond 64, because it may place too much of a load on all the receiver SEs.

You can also set proactive FEC using the PGM configuration file (a text file accessible from the SE CLI in the /local1/multicast-expert-config/ directory). Proactive FEC is the number of extra packets that the multicast sender proactively sends out for every FEC number of data packets. The proactive FEC default value is 0. You can set the proactive FEC number higher for better multicast reliability. For example, you can set 2 proactive packets for every 16 FEC packets at the expense of 12.5 percent traffic overhead (2 divided by 16).

Proactive FEC is an additional reliability measure above and beyond that of normal FEC. Although normal FEC does not incur bandwidth overhead, proactive FEC does use bandwidth overhead. Proactive FEC primarily protects the multicast from uniform losses. For example, if the network has a uniform loss rate of 15 percent, then a proactive FEC of 2 extra packets for every 16 FEC packets (a 12.5 percent bandwidth overhead) cuts the effective loss rate down to 2.5 percent. Most network losses are not completely uniform. Still, during bursts, proactive FEC undercuts the effective burst loss rate. For example, if the burst loss rate is 20 percent while the average loss rate is 2 percent, with proactive FEC at 12.5 percent, the receiver SEs experience a burst loss rate of 7.5 percent and an average loss rate near 0 percent.

Testing Multicast Connectivity in CDS Networks

The **multicast connectivity-test** command options allow you to test multicast connectivity in the CDS networks. You can specify a maximum of 20 multicast receiver SEs using this option. Use the **cloud-id** or **cloud-name** options to test multicast connectivity to receiver SEs grouped into multicast clouds in the CDS network. There is no limit to the number of SEs you can have in a multicast cloud.

The **cloud-id** or **cloud-name** options initiate the following sequence of events:

1. When you specify the IP addresses of the receiver SEs, multicast cloud ID, or multicast cloud name, you initiate the multicast connectivity test.
2. The multicast sender initiates RPC calls to the receiver SEs, which prompt them to listen for the PGM multicast data on the default port or the port specified in the **multicast connectivity-test** command.
3. The SE displays the following:
   - A list of receiver SEs that failed to respond to the RPC calls
   - Warning messages if multicast is not enabled on any receiver SE
4. The multicast sender starts sending PGM packets to the specified multicast address. The receiver SE keeps updating the session statistics for each packet received.

   If you interrupt the test by pressing **Ctrl-C**, the multicast sender sends a notification to all receiver SEs to stop listening and displays the information obtained so far.
5. After the multicast session is completed or the transmission has timed out, the receiver SE sends the statistics to the multicast sender using an RPC call.

Note If the multicast receiver SE times out, it sends a "no packet received" error message to the multicast sender if it has not received any PGM packets for 60 seconds. Similarly, the multicast sender waits for 60 seconds for a response from the receiver SE before timing out.

6. The multicast sender displays the statistics obtained for the session.
7. The multicast sender repeats the test with the receiver SEs and generates a consolidated report.

Using the cloud-id or cloud-name Option

You can use the **cloud-id** or **cloud-name** options to test multicast connectivity in large networks where a number of SEs are grouped under multicast clouds.

Note You cannot specify values for the optional parameters **FEC-size** and **max-transfer-rate** when the **cloud-id** or **cloud-name** options are used. The values for these two parameters are taken from the multicast cloud configuration.

Use the **multicast connectivity-test cloud-name** command to test the multicast connectivity to the receiver SEs in the multicast cloud mcloud1.

The multicast address is not specified in this example. The Internet Streamer CDS software uses the advertisement IP address specified in the multicast cloud configuration as the multicast address. Because no values were specified for the options, the Internet Streamer CDS software uses the default values for all the optional parameters.

multicast connectivity-test send Command

To test the multicast connectivity to the receiver SEs listening to a specific multicast address, use the **multicast connectivity-test send** command. This command runs the pgmrategen application, which continuously sends PGM packets to the specified multicast IP address. After you enter this command, the system displays the percentage of packets that have been multicast and stops sending packets when the packets sent reaches 100 percent. Press **Ctrl-C** to interrupt the PGM application and return to the EXEC prompt.

To determine the number of network elements through which the packet can pass before reaching the receiver, specify the Time To Live (TTL), which can vary between 1 and 255.

multicast connectivity-test receive Command

To receive PGM packets, use the **multicast connectivity-test receive** command. Entering this command runs the pgmratemon application, which listens for the PGM multicast data transmitted from a PGM sender on the specified multicast IP address. When a packet is received, the pgrmratemon application lists the packet size and bandwidth.

To test the multicast connectivity between two SEs, use the same multicast IP address for both send and receive. The pgmratemon application terminates by itself after a default period of 3 minutes and returns to the EXEC prompt. You can press **Ctrl-C** to terminate the pgmratemon application and return to the EXEC prompt.

Examples

The following example shows the output of the **multicast connectivity-test** command for a multicast IP address of 239.1.1.1 and receiver SE IP addresses 10.43.27.2 and 10.43.27.4:

```
ServiceEngine# multicast connectivity-test 10.43.27.2 10.43.27.4 multicast-address
239.1.1.1
```

```
Connecting to Receiver : 10.43.27.2
Starting PGM Receiver on the SE 10.43.27.2
Connecting to Receiver : 10.43.27.4
Starting PGM Receiver on the SE 10.43.27.4
Packet Generation thread has started. It will start sending packets after PGMReceivers
have been started
Time Elapsed : 180 seconds
PGM Sender has finished sending packets. Awaiting Receiver response
Will wait for 60 seconds...

Configuration
-------------
Multicast Address : 239.1.1.1
Port : 7000
Max Rate to send PGM Packets : 128 kbps
Time to live for multicast packets : 255
Forwarder Error Correction Size : 8

Detailed Report
----------------

Receiver IP : 10.43.27.2
Duration : 180 seconds
No of Packets received : 1134
Packet Length : 1024 Bytes
Minimum BW : 5.714 KBps
Maximum BW : 7 KBps
Average BW : 6.291 KBps
NAK Count : 0

Receiver IP : 10.43.27.4
Duration : 180 seconds
No of Packets received : 1134
Packet Length : 1024 Bytes
Minimum BW : 5.691 KBps
Maximum BW : 7 KBps
Average BW : 6.298 KBps
NAK Count : 0

Summary Report
--------------
Total number of receivers : 2
No: of receivers which received Packets : 2
No: of receivers which did not receive Packets : 0
No: of RPC calls failures : 0
No: of Other Errors obtained from Receivers : 0
```

The following example shows all the optional parameters and default values:

```
ServiceEngine# multicast connectivity-test 10.77.155.171 10.77.155.175 10.77.155.179
multicast-address 239.10.1.11 duration 180 FEC-size 8 max-transfer-rate 128
message-length 1024 output-style detail port 7000 time-to-live 255
```

The following example shows the **multicast connectivity-test cloud-name command** with all the optional parameters and default values:

```
ServiceEngine# multicast connectivity-test cloud-name mcloud1 duration 180 message-length
1024 output-style detail port 7000
```

The following example shows the output of the **multicast connectivity-test cloud-name** command for the multicast cloud Mcloud1. Because the multicast address was not specified, the Internet Streamer CDS software uses the advertisement IP address 239.1.1.1, specified in the multicast cloud configuration, as the multicast IP address. PGM packets are sent to the two receiver SEs (IP addresses 10.43.27.2 and 10.43.27.4) that make up the multicast cloud Mcloud1.

```
ServiceEngine# multicast connectivity-test cloud-name Mcloud1
Connecting to Receiver : 10.43.27.2
Starting PGM Receiver on the SE 10.43.27.2
Connecting to Receiver : 10.43.27.4
Starting PGM Receiver on the SE 10.43.27.4
Packet Generation thread has started. It will start sending packets after PGMReceivers
have been started
Time Elapsed : 180 seconds
PGM Sender has finished sending packets. Awaiting Receiver response
Will wait for 60 seconds...

Configuration
-------------
Multicast Address : 239.1.1.1
Port : 7000
Max Rate to send PGM Packets : 10000 kbps
Time to live for multicast packets : 255
Forwarder Error Correction Size : 16

Detailed Report
----------------

Receiver IP : 10.43.27.4
Duration : 180 seconds
No of Packets received : 1139
Packet Length : 1024 Bytes
Minimum BW : 4.903 KBps
Maximum BW : 7 KBps
Average BW : 6.296 KBps
NAK Count : 0

Receiver IP : 10.43.27.2
Duration : 180 seconds
No of Packets received : 1139
Packet Length : 1024 Bytes
Minimum BW : 5.641 KBps
Maximum BW : 7 KBps
Average BW : 6.319 KBps
NAK Count : 0

Summary Report
--------------
Total number of receivers : 2
No: of receivers which received Packets : 2
No: of receivers which did not receive Packets : 0
No: of RPC calls failures : 0
No: of Other Errors obtained from Receivers : 0
```

The following example shows the output of the **multicast connectivity-test send** command for a multicast IP address of 239.1.1.1 and TTL of 255:

```
ServiceEngine# multicast connectivity-test send 239.1.1.1 255
Starting pgmrategen ....
pgmrategen is already running.  Exiting previous instance
Sending 1024 messages of 1024 bytes (1024 Kbytes)
PGM rate is 1024 Kbps
Progress: 99%
```

```
Total time 159.924 seconds, 6.40302 KBps, 52.4536 Kbps
```

The following example shows the output of the **multicast connectivity-test receive** command:

```
ServiceEngine# multicast connectivity-test receive 239.1.1.1
Starting pgmratemon ....
This SE is not configured as Multicast receiver in any cloud
Configuring this SE as Satellite mode receiver

Press ^C to abort or wait for 3 mins to exit....

Multicasting PGM multicast data to SmartPGM receivers on multicast address 239.1

Sending 1024 messages of 1024 bytes (1024 Kbytes)
PGM rate is 1024 Kbps
Progress: 99%
Total time 8.39756 seconds, 121.94 KBps, 998.934 Kbps

Exiting....
Stopping pgmratemon
ServiceEngine#
```

Related Commands

Command	Description
multicast (Global configuration)	Configure multicast options.
show multicast	Displays whether or not the multicast sender and receiver are enabled.

neighbor

To configure BGP neighbors, use the **neighbor** BGP configuration command. To return to the default, use the **no** form of this command.

neighbor *ip_address* {**ebgp-multihop** *TTL* | **password** *word* | **remote-as** *as_number* | **timers** *keepalive_timer hold_timer*}

no *ip_address* {**ebgp-multihop** *TTL* | **password** *word* | **remote-as** *as_number* | **timers** *keepalive_timer hold_timer*}

Syntax Description

ip_address	IP address of the neighbor.
ebgp-multihop	Sets the Time-to-Live (TTL) value for the EBGP multihop scenarios.
TTL	Time-to-Live value. The range is from 1 to 255.
password	Specifies the BGP neighbor password.
word	BGP MD5 password.
remote-as	Specifies the Remote Autonomous Systems (AS) number.
as_number	Autonomous system to which the neighbor belongs.
timers	Configures keepalive and hold timers.
keepalive_timer	Keepalive timer interval, in seconds. The range is from 0 to 3600.
hold_timer	Hold timer interval, in seconds. The range is from 0 to 3600.

Command Defaults

- There are no BGP or multi protocol BGP neighbor peers.
- Default TTL value is 1 for all neighbors.
- Keepalive timer interval is set to 60 seconds, and the hold timer interval is set to 180 seconds.

Command Modes

BGP configuration (config-bgp) mode.

Usage Guidelines

Use the **neighbor ebgp-multihop** BGP configuration command to set the TTL value for the EBGP multihop scenarios.

Specifying a neighbor with an autonomous system number that matches the autonomous system number specified in the **router bgp** Global configuration command identifies the neighbor as internal to the local autonomous system. Otherwise, the neighbor is considered as external.

Use the **neighbor remote-as** command to add a neighbor to the BGP, or multi protocol BGP table, before setting the TTL value for the neighbor.

By default, neighbors that are defined using the **neighbor remote-as** command in router configuration mode exchange only unicast address prefixes.

Use the **neighbor remote-as** command before setting the TTL value.

In order for the proximity function to work, one of the following is required:

- Enabled link-state protocol, such as OSPF or IS-IS for IGP proximity.
- Enabled policy routing protocol, such as BGP for best-path proximity, and one of the IGP (OSPF or IS-IS) is required for next hop resolution.

Note All BGP routes must resolve to IGP next hops or directly connected routes.

Examples

The following example shows that a router at the address 192.168.86.3 is a neighbor in autonomous system number 23, and has a ebgp-multihop TTL value of 3:

```
ServiceRouter(config)# router bgp 23
ServiceRouter(config-bgp)# neighbor 192.168.86.3 remote-as 23
ServiceRouter(config-bgp)# neighbor 192.168.86.3 ebgp-multihop 3
ServiceRouter(config-bgp)#
```

The following example shows how to specify that a router at the address 192.168.86.3 is a neighbor in autonomous system number 23:

```
ServiceRouter(config)# router bgp 23
ServiceRouter(config-bgp)# neighbor 192.168.86.3 remote-as 23
ServiceRouter(config-bgp)#
```

The following example shows that a router at the address 192.168.86.3 is a neighbor in autonomous system number 23, and its keepalive timer interval and hold timer interval are set to be 100 seconds and 200 seconds, respectively.

```
ServiceRouter(config)# router bgp 23
ServiceRouter(config-bgp)# neighbor 192.168.86.3 remote-as 23
ServiceRouter(config-bgp)# neighbor 192.168.86.3 timers 100 200
ServiceRouter(config-bgp)#
```

To confirm that timers are updated correctly, use the **show ip bgp neighbors** command. The following example output shows that the keepalive interval has been changed to 100 seconds and the hold timer has been changed to 200 seconds:

```
ServiceRouter> show ip bgp neighbors

BGP neighbor is 192.168.86.3, remote AS 23, ibgp link, Peer index 1
  BGP version 4, remote router ID 192.168.86.3
  BGP state = Established, up for 1d05h
  Peer is directly attached, interface GigabitEthernet 2/0
  Last read 0.868226, hold time = 200, keepalive interval is 100 seconds
  Last written 00:00:09, keepalive timer expiry due 00:01:30
  Received 78444 messages, 0 notifications, 0 bytes in queue
  Sent 1788 messages, 0 notifications, 0 bytes in queue
  Connections established 1; dropped 0
  Last reset by us never, due to process restart
  Last reset by peer never, due to process restart
  Neighbor capabilities:
  Dynamic capability: advertised (mp, refresh, gr)
  Dynamic capability (old): advertised
  Route refresh capability (new): advertised received
  Route refresh capability (old): advertised received
  Address family IPv4 Unicast: advertised received
  For address family: IPv4 Unicast
  BGP table version 1, neighbor version 810749
  8518 accepted paths consume 613296 bytes of memory
```

```
  0 sent paths
  Local host: 192.168.86.47, Local port: 58920
  Foreign host: 192.168.86.3, Foreign port: 179
  fd = 35

ServiceRouter>
```

Related Commands

Command	Description
router bgp	Configures a BGP routing process.

net

To configure an IS-IS network entity title (NET) for a Connectionless Network Service (CLNS) routing process, use the **net** IS-IS configuration command. To remove a NET, use the **no** form of this command.

net *network_entity_title*

no net *network_entity_title*

Syntax Description

network_entity_title	NET that specifies the area address and the system ID for a CLNS routing process. Either an address or a name may be specified.

Command Defaults

No *NET* is configured and the CLNS process does not start without a NET.

Command Modes

IS-IS configuration (config-isis) mode.

Usage Guidelines

Under most circumstances, one and only one NET must be configured.

A NET is a network service access point (NSAP) where the last byte is always zero. On a Proximity Engine running IS-IS, a NET can be 8 to 20 bytes. The last byte is always the n-selector and must be zero.

The six bytes directly in front of the n-selector are the system ID. The system ID length is a fixed size and cannot be changed. The system ID must be unique throughout each area (Level 1) and throughout the backbone (Level 2).

All bytes in front of the system ID are the area ID.

Even when IS-IS is used to perform IP routing only (that is, no CLNS routing enabled), a NET must still be configured to define the router system ID and area ID.

- Area ID must match the area ID of the IS-IS router that the Proximity Engine is pairing with.
- System ID is unique for each Proximity Engine.

Examples

The following example shows how to use the **net** command to configure a router with system ID 0001.0c11.1111.00 and area ID 47.0004.004d.0001:

```
ServiceRouter(config)# router isis
ServiceRouter(config-isis)# net 47.0004.004d.0001.0001.0c11.1111.00
ServiceRouter(config-isis)#
```

Related Commands

Command	Description
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

netmon

To display the transmit and receive activity on an interface, use the **netmon** command in EXEC configuration mode.

netmon *line*

Syntax Description

line	netmon options, -h to get help.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The netmon utility displays the transmit and receive activity on each interface in megabits per second (Mbps), bytes per second (Bps), and packets per second (pps).

Examples

The following example shows how to display the netmon list of options:

```
ServiceEngine# netmon -h
Usage: netmon [<loop-time-in-seconds>] [<iterations>]
       (runs forever if iterations not specified)
```

Related Commands

Command	Description
gulp	Captures lossless gigabit packets and writes them to disk.
netstatr	Displays the rate of change of netstat statistics.
ss	Dumps socket statistics.
tcpmon	Searches all TCP connections.

netstatr

To display the rate of change of netstat statistics, use the **netstatr** command in EXEC configuration mode.

netstatr *line*

Syntax Description

line	netmon options, -h to get help.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The **netstatr** utility displays the rate of change, per second, of netstat statistics for a given period of time. The average rate per second is displayed, regardless of the sample period. To view the list of options, enter **netstatr -h**.

Examples

The following example shows how to display the netstart list of options:

```
ServiceEngine# netstatr -h
Usage: netstatr [-v] [<loop-time-in-seconds>] [<iterations>]
       -v verbose mode
       (default is 3 sec loop time, run forever)
```

Related Commands

Command	Description
gulp	Captures lossless gigabit packets and writes them to disk.
netmon	Displays the transmit and receive activity on an interface.
ss	Dumps socket statistics.
tcpmon	Searches all TCP connections.

network area

To define the interfaces on which OSPF runs and the area ID for those interfaces, use the **network area** router configuration command. To disable OSPF routing for interfaces defined with the address wildcard-mask pair, use the no form of this command.

network *ip_address wildcard_mask* **area** *area_id*

no network *ip_address wildcard_mask* **area** *area_id*

Syntax Description

ip_address	IP address in the form of *xxx.xxx.xxx.xxx*
wildcard_mask	IP-address-type mask that includes “don’t care” bits.
area_id	Area that is to be associated with the OSPF address range. It can be specified as either a decimal value or as an IP address. If you intend to associate areas with IP subnets, you can specify a subnet address as the value of the *area_id.*

Note Any individual interface can only be attached to a single area. If the address ranges specified for different areas overlap, the software adopts the first area in the network command list and ignore the subsequent overlapping portions. In general, it is recommend that you configure address ranges that do not overlap to avoid inadvertent conflicts.

Command Defaults

OSPF routing for interfaces is disabled by default.

Command Modes

OSPF configuration (config-ospf) mode.

Usage Guidelines

The *ip_address* and *wildcard_mask* arguments together allow you to define one or multiple interfaces to be associated with a specific OSPF area using a single command. Using the *wildcard_mask* argument allows you to define one or multiple interfaces to be associated with a specific OSPF area using a single command. If you intend to associate areas with IP subnets, you can specify a subnet address as the value of the *area_id* argument.

For OSPF to operate on the interface, the primary address of the interface must be covered by the **network area** command. If the **network area** command covers only the secondary address, it does not enable OSPF over that interface.

The Proximity Engine sequentially evaluates the *ip_address wildcard_mask* pair for each interface as follows:

1. The *wildcard_mask* is logically ORed with the interface IP address.

2. The *wildcard_mask* is logically ORed with the *ip_address* argument in the **network** command.

3. The software compares the two resulting values. If they match, OSPF is enabled on the associated interface and this interface is attached to the OSPF area specified.

There is no limit to the number of **network area** commands that can be used on the router.

Note Any individual interface can only be attached to a single area. If the address ranges specified for different areas overlap, the software adopts the first area in the network command list and ignores the subsequent overlapping portions. In general, we recommend that you configure address ranges that do not overlap to avoid inadvertent conflicts.

When a more specific OSPF network range is removed, interfaces belonging to that network range are retained and remain active if, and only if, a less specific network range exists.

For example, consider the following configuration:

```
router ospf
   network 205.188.129.16 0.0.0.3 area 20
   network 205.188.129.40 0.0.0.3 area 20
   network 205.188.129.44 0.0.0.3 area 20
   network 205.188.129.96 0.0.0.3 area 20
   network 205.188.129.96 0.0.127.255 area 20
```

Enter the following:

```
no network 205.188.129.40 0.0.0.3 area 20
```

Interfaces falling into the network range 205.188.129.40/0.0.0.3 still remains active because the superset, 205.188.128.0/0.0.127.255, exists for area 20. A more specific network statement causes interfaces belonging to that range to be removed from a different area only if a less specific network statement (superset) exists.

Consider a configuration such as the following:

```
router ospf 1
  network 205.188.128.0 0.0.127.255 area 20
```

If the following network statement is entered:

```
network 205.188.129.96 0.0.0.3 area 40
```

the interfaces belonging to range 205.188.129.96/0.0.0.3 are removed from area 20 and moved to area 40. Network statements with identical ranges but different area IDs are considered as area changes. For example, the following network statements cause interfaces belonging to network range 205.188.129.40/0.0.0.3 to move from area 20 to area 40:

```
network 205.188.129.40 0.0.0.3 area 20
network 205.188.129.40 0.0.0.3 area 40
```

Examples

The following example shows how to initialize OSPF routing process. Area 0 enables OSPF.

```
ServiceRouter(config)# router ospf
ServiceRouter(config-ospf)# network 192.168.78.0 0.0.0.255 area 0
ServiceRouter(config-ospf)#
```

Related Commands

Command	Description
router ospf	Enables the OSPF routing process.

no (Global configuration)

To undo a command in Global configuration mode or set its defaults, use the **no** form of a command in Global configuration mode.

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 to identify the commands available for a specific device.

Syntax Description

command	Specifies the command type; see the Usage Guidelines section for valid values.

Command Defaults

None

Command Modes

Global configuration (config) mode.

Usage Guidelines

Valid values for *command* are as follows:

aaa	Configures AAA[1].
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.
banner	Defines a login banner.
bitrate	Configures the bit rate.
cdsm	Configures the CDSM settings.
clock	Configures the time-of-day clock.
cms	Configures the CMS[2].
device	Configures the device mode.
direct-server-return	Configures direct-server-return.
disk	Configures disk-related settings.
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 LDAP[3] parameters.
logging	Configures the syslog[4].
network-filesystem	Configures the network file system server and client.
ntp	Configures the NTP[5].
offline-operation	Configures the offline service operation.
pace	Configures the Movie Streamer 7H90C0CHand WMT 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 RTSP[6]-related parameters.
rule	Configures the Rules Template.
snmp-server	Configures the SNMP server.
sshd	Configures the SSH[7] service.
tcp	Configures global TCP parameters.
telnet enable	Configures Telnet services.
transaction-logs	Configures the transaction logging.
username	Establishes username authentication.
wmt	Configures WMT[8] parameters.

1. AAA = authentication, authorization, and accounting
2. CMS = Centralized Management System
3. LDAP = Lightweight Directory Access Protocol
4. syslog = system logging
5. NTP = Network Time Protocol
6. RTSP = Real-time Streaming Protocol
7. SSH = Secure Shell
8. WMT = Windows Media Technologies7H90C0CH

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 command in interface configuration mode or set its defaults, use the **no** command in interface configuration mode.

no interface {**GigabitEthernet** *slot/port* **| PortChannel** {**1** | **2**} **| Standby** *group_num*}

Syntax Description

GigabitEthernet	Selects a Gigabit Ethernet interface to configure.
slot/port	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 be configured.
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.
group_num	Group number for the selected interface. The group number range is 1 to 4.

Command Defaults

None

Command Modes

Interface configuration (config-if) mode.

Related Commands

Command	Description
interface	Configures a Gigabit Ethernet or port channel interface.
show interface	Displays the hardware interface information.
show running-config	Displays the current running configuration information on the terminal.
show startup-config	Displays the startup configuration.

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** command in Global configuration mode. 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.
ip_address	NTP server IP address.
hostname	NTP server hostname.
ip_addresses	(Optional) IP address of the time server providing the clock synchronization (maximum of four).
hostnames	(Optional) Hostname of the time server providing the clock synchronization (maximum of four).

Command Defaults

None

Command Modes

Global configuration (config) mode.

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.

Note When the time is configured through **ntp server** command, then the **ntpdate** command should not be used to set the time. If **ntpdate** is used then, an error message will be displayed.

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** command in EXEC configuration mode. 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 shows how to configure the IP address of the time server providing the clock synchronization:

```
ServiceEngine(config)# ntp 172.16.22.44
```

The following example shows how to reset the time server providing the clock synchronization:

```
ServiceEngine(config)# no ntp 172.16.22.44
```

Related Commands

Command	Description
clock	Sets or clears clock functions or updates the calendar.
show clock	Displays the system clock.
show ntp status	Displays the Network Time Protocol parameters.

ntpdate

To set the software clock (time and date) using a Network Time Protocol (NTP) server, use the **ntpdate** command in EXEC configuration mode.

ntpdate {*hostname* | *ip_address*}

Syntax Description

hostname	NTP hostname.
ip_address	NTP server IP address.

Command Defaults

None

Command Modes

EXEC configuration mode.

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 shows how to set the software clock of the SE using an NTP server:

```
ServiceEngine# ntpdate 10.11.23.40
```

Related Commands

Command	Description
clock set	Sets the time and date.
show clock	Displays the system clock.

ping

To send echo packets for diagnosing basic network connectivity on networks, use the **ping** command in EXEC configuration mode.

On the CDSM and SE:

ping {*hostname* | *ip_address*}

On the SR:

ping {*hostname* | *ip_address* | **srp** {*hostname* | *ip_address*}}

Syntax Description

hostname	Hostname of system to ping.
ip_address	IP address of system to ping.
srp	Pings the Service Routing Protocol.

Command Defaults

None

Command Modes

EXEC configuration mode.

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` message 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#
```

ping srp

To ping the Service Routing Protocol ring, use the **ping** command in EXEC configuration mode.

ping srp

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

In an ipv4 or ipv6 environment, the **ping** command uses the ipv4 or ipv6 address. The **ping srp** command uses The DHT key (64 bits hex-id).

In the example below, the node that owns the DHT key (node SR-205-5) responds to this ping. The TTL is 64, and the response time is 0.330585 ms.

Examples

The following example shows how to test the basic network connectivity with a host:

```
ServiceRouter# ping srp
6aab6568d794a77bc20633b0cb3aef14d906e4aef00a3fa2a93973524337e40c
Ping response from SR-205-5:9000, ttl=64, time=0.330585 ms
  id=6aab6568d794a77bc20633b0cb3aef14d906e4aef00a3fa2a93973524337e40c
Ping response from SR-205-5:9000, ttl=64, time=0.282069 ms
  id=6aab6568d794a77bc20633b0cb3aef14d906e4aef00a3fa2a93973524337e40c
Ping response from SR-205-5:9000, ttl=64, time=0.278821 ms
  id=6aab6568d794a77bc20633b0cb3aef14d906e4aef00a3fa2a93973524337e40c
Ping response from SR-205-5:9000, ttl=64, time=0.279144 ms
  id=6aab6568d794a77bc20633b0cb3aef14d906e4aef00a3fa2a93973524337e40c
Ping response from SR-205-5:9000, ttl=64, time=0.283236 ms
  id=6aab6568d794a77bc20633b0cb3aef14d906e4aef00a3fa2a93973524337e40c

ServiceRouter#
```

Related Commands

Command	Description
traceroute srp	Traces the route of the Service Routing Protocol ring.

ping6

To ping the IPv6 address, use the **ping6** command in EXEC configuration mode.

ping6 *line ip_address*

Syntax Description

line	Destination Host or IP Address.
ip_address	IP address of system to ping.

Command Defaults

None

Command Modes

EXEC configuration mode.

Examples

The following example shows how to ping the IPv6 address:

```
ServiceEngine# ping6 fec0::100/64
```

Related Commands

Command	Description
ping	Sends echo packets for diagnosing basic network connectivity on networks.

port-channel

To configure the port channel load balancing, use the **port-channel** command in Global configuration mode. To disable load balancing, use the **no** form of this command.

port-channel load-balance {**dst-ip** | **dst-mac** | **dst-port** | **round-robin** | **src-dst-mac** | **src-dst-port** | **src-port**}

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 MAC addresses.
dst-port	Specifies the load balancing method using destination Layer 4 port.
round-robin	Specifies the load balancing method using round-robin sequential, cyclical resource allocation (each interface in the channel group).
src-dst-mac	Specifies the load balancing method using source and destination MAC address.
src-dst-port	Specifies the load balancing method using source and destination port.
src-port	Specifies the load balancing method using source Layer 4 port.

Command Defaults

Round-robin is the default load balancing method.

Command Modes

Global configuration (config) mode.

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** keyword 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.

The other balancing options give you the flexibility to choose specific interfaces (by IP address, MAC address, port) when sending an Ethernet frame. The source and destination options, while calculating the outgoing interface, take into account both the source and destination (MAC address or port).

Because the Internet Streamer CDS software normally starts IP packets or Ethernet frames, it does not support hashing based on the source IP address and source MAC address. The **round-robin** keyword is the default load balancing algorithm to evenly distribute traffic among several identical network interfaces.

To remove a port channel, use the **no port-channel interface PortChannel** command.

Note Ingress traffic from NAS mounts is not distributed evenly over port channels. Separate interfaces can be used for NAS outside of the port-channel configuration to achieve better load balancing. Ingress traffic to the CDS is determined by the switch, this applies to all application traffic over port channels.

Note For load balancing, the round robin method alone is not supported with LACP.

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

Command	Description
interface	Configures a Gigabit Ethernet or port-channel interface

primary-interface

To configure the primary interface for the CDS network, use the **primary-interface** command in Global configuration mode. 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.
1-2/	Gigabit Ethernet slot numbers 1 or 2.
port	Port number of the Gigabit Ethernet interface.
PortChannel	Selects a port channel interface as the CDS network primary interface.
1-2	Port channel number 1 or 2.
Standby	Selects a standby group as the CDS network primary interface.
group_num	Standby group number.

Command 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 communicated 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.

Note Whenever the IP address of the primary interface is changed, the DNS server must be restarted.

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 (config) mode.

Usage Guidelines

The **primary-interface** command in Global configuration mode 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 Gigabit Ethernet 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 Gigabit Ethernet slot 2 port 0 as the primary interface on an SE:

```
ServiceEngine(config)# primary-interface GigabitEthernet 2/0
```

proximity algorithm bgp

To enable a Border Gateway Protocol (BGP) proximity algorithm option for the Proximity Engine, use the **proximity algorithm bgp** command in Global configuration mode. To disable a BGP proximity algorithm option, use the **no** form of the command.

proximity algorithm bgp {**best-path** | **location-community** [**strict**] | **redirect**}

no proximity algorithm bgp {**best-path** | **location-community** [**strict**] | **redirect**}

Syntax Description

best-path	Specifies the BGP Autonomous Systems (AS) path length-based proximity.
location-community	Specifies that the community-based proximity algorithm be used.
strict	(Optional) Strict matching.
redirect	Specifies the BGP AS-based redirection.

Command Defaults

By default, the BGP algorithms are turned off.

Command Modes

Global configuration (config) mode.

Usage Guidelines

When BGP is configured as the routing protocol, the **proximity algorithm bgp** command enables a BGP proximity option for the Proximity Engine. The **Proximity algorithm bgp** commands are not effective unless BGP is configured first.

Best-Path

When the BGP routing protocol is configured the Proximity Engine learns routes from other AS, and therefore can rank proximity target addressees (PTAs) that originate in an external AS using not only the basic BGP proximity (which ranks the PTAs based on their next-hop), but also based on the AS path length of the PTAs. This capability is enabled by the **proximity algorithm bgp best-path** command. A PTA that has a longer AS path length is less preferred. It should be noted that the Proximity Engines takes into account the AS path length of the PTAs only if the proximity source address (PSA) is originated in the same AS as the Proximity Engine, since the AS path length learnt by the Proximity Engine is with reference to its own AS. If the PSA originates in an external AS, it is recommended that the **proximity algorithm bgp redirect** be enabled to redirect the request to a Proximity Engine in the same AS as the PSA if such a Proximity Engine exists.

Location Community

When the **proximity algorithm bgp location-community** command is enabled, additional location information is included in the proximity calculation to influence application-level traffic optimization in the network. Many service providers are already using BGP community values to identify prefixes originated from a given POP. Taking advantage of the community information can greatly improve the scalability and flexibility of the proximity calculation algorithm.

BGP community-based proximity is used when community-based proximity option is enabled and the PSA has a BGP community string that is configured in the **location community** command. PTAs that have the same BGP community string as the PSA are ranked as more preferred than PTAs that do not have the same BGP community string as the PSA. For the remaining PTAs that have different community strings, they are ranked by either IGP or BGP proximity.

Community-based proximity requires the use of the **location community** command to configure the Proximity Engine community values. Each Proximity Engine must be configured with the community numbers that are used within the network to locate the prefix origination point.

When community values are configured, the Proximity Engine creates and maintains a sorted table of communities within BGP. Currently, location community configurations must be manually configured on each Proximity Engine.

Redirect

If the PSA, where the proximity request is initiated, is learned from another AS, the current Proximity Engine does not have the best knowledge to handle the proximity request. If the proximity redirect option is enabled, the Proximity Engine sends back a Redirect response to the Service Router. The Redirect response contains the list of Proximity Engines that reside in the same AS as the PSA. The Service Router then sends the proximity request to one of these Proximity Engines.

Configuring Proximity Algorithm BGP

Perform the following steps to configure Proximity Algorithm BGP:

Step 1 Turn on BGP Best Path algorithm in the Proximity Engine.

```
ServiceRouter(config)# proximity engine enable
ServiceRouter(config)# proximity algorithm bgp best-path
```

Step 2 Enable router bgp 1:

```
ServiceRouter(config)# router bgp 1
ServiceRouter(config)# neighbor 26.0.0.6 remote-as 1
```

Step 3 Turn on EBGP in the routers.

Result Analysis

When PSA is 3.1.5.0 and PTA is 33.1.5.0, the returned proximity cost is 2164260884.

```
ServiceRouter# show ip rib route

3.1.5.0/24, 1 ucast next-hops, 0 mcast next-hops, attached
*via 3.1.5.3, GigabitEthernet 1/0, [0/0], 00:01:59, direct
26.0.0.0/8, 1 ucast next-hops, 0 mcast next-hops, attached
*via 26.0.0.2, GigabitEthernet 2/0, [0/0], 00:01:59, direct
33.1.5.0/24, 1 ucast next-hops, 0 mcast next-hops
*via 26.0.0.6, GigabitEthernet 2/0, [200/0], 00:00:29, bgp-1, internal, tag 2
extended route information: AS Hops 1, BGP PxEer AS 1
62.0.0.0/8, 1 ucast next-hops, 0 mcast next-hops
*via 26.0.0.6, GigabitEthernet 2/0, [115/20], 00:01:27, isis-p1, L1
```

The AS Path length can be calculated from the **show ip route** command:

AS Path length for PTA 33.1.5.0 - 1

The 31st community bit set to 1 since no location community match, AS Path length is 1(set the 24th bit to 1), the IGP cost is 20.

2147483648+ 16777216 + 20 = 2164260884

The proximity calculation rendered using the following formula:

rating(PSA,PTA)= 2^31Cc comm_match(PSA,PTA) +2^24CBPAS_path_len(PTA)+ IGP_rating(PSA,PTA)

- The result is given in 32 bits.
- The 31st Location community is zero if the location community matches. It is effective only when the BGP location community algorithm is turned on.
- The bits (24-30) denote the AS Best path distance. It is effective only on turning on the BGP redirect algorithm.
- The the remaining 24 bits hold the IGP rating returned by the IGP daemons. The IGP daemons returns 32-bit values that are normalized to occupy the 24 bits.

Examples

Proximity Algorithm Redirect

The following example shows how to use the proximity redirect option:

```
ServiceRouter(config)# proximity algorithm bgp redirect
```

First, each Proximity Engine must form a DHT ring.

```
ProximityEngine1(config)# router srp
ProximityEngine1(config-srp)# domain 100

ProximityEngine2(config)# router srp
ProximityEngine2(config-srp)# domain 100
ProximityEngine1(config-srp)# bootstrap 3.4.0.7
```

Configure both the Proximity Servers on the Service Router and enable proximity-based-routing:

```
ServiceRouter(config)# service-router proximity-based-routing proximity-server 3.4.0.7
ServiceRouter(config)# service-router proximity-based-routing proximity-server 3.1.14.17
ServiceRouter(config)# service-router proximity-based-routing enable
```

Next, enable BGP on both the Proximity Engines such that both are in different AS:

```
ProximityEngine1(config)# router bgp 1
ProximityEngine1(config-bgp)# neighbor 3.4.0.12 remote-as 1

ProximityEngine2(config)# router bgp 2
ProximityEngine2(config-bgp)# neighbor 3.1.14.12 remote-as 2
```

For Proximity Redirect to work efficiently, it is recommended that there are at least two Proximity Servers, one each in a different autonomous system.

In the above example each Proximity Engine is connected with routers and routers advertise the routes to the respective Proximity Engines and the neighbor IP addresses are the corresponding neighbor router's directly connected interfaces:

```
ProximityEngine1# sh ip bgp all

BGP routing table information for address family IPv4 Unicast
BGP table version is 5, local router ID is 3.4.0.7
Status: s-suppressed, x-deleted, S-stale, d-dampened, h-history, *-valid, >-best
Path type: i-internal, e-external, c-confed, l-local, a-aggregate, r-redist
Origin codes: I - IGP, E - EGP, ? - incomplete

Network Next Hop Metric LocPrf Weight Path
```

```
*>i3.1.14.0/24 3.4.0.12 0 100 0 2 I
*>i3.4.0.0/16 3.4.0.12 0 100 0 I

BGP routing table information for address family IPv4 Multicast

ProximityEngine2# sh ip bgp all

BGP routing table information for address family IPv4 Unicast
BGP table version is 5, local router ID is 3.4.0.8
Status: s-suppressed, x-deleted, S-stale, d-dampened, h-history, *-valid, >-best
Path type: i-internal, e-external, c-confed, l-local, a-aggregate, r-redist
Origin codes: I - IGP, E - EGP, ? - incomplete

Network Next Hop Metric LocPrf Weight Path
*>i3.1.14.0/24 3.1.14.12 0 100 0 I
*>i3.4.0.0/16 3.1.14.12 0 100 0 1 I

BGP routing table information for address family IPv4 Multicast
```

Next, it needs to be checked if the DHT Ring is formed appropriately:

```
ServiceRouter# show srp neighbor
Codes: T - local node, L - leafset, P - primary, S - secondary, B - backup
I - Intransitive, R - Replicate Set, D - delay, ND - New Delay
H - hold time, U - up time

Number of neighbors in the database: 1
RPL c152b683f000c6be3ff82214e4d8084d52a44dee85b29d67c49e60fbaf3e4737
via U6-CDE205-2 [3.1.14.17] 9000, D=0.223891 ms, ND=0.230440 ms
H=00:00:07, U=00:00:15

ProximityEngine2# show srp neighbor

Codes: T - local node, L - leafset, P - primary, S - secondary, B - backup
I - Intransitive, R - Replicate Set, D - delay, ND - New Delay
H - hold time, U - up time

Number of neighbors in the database: 1
RPL 97d35b9f3cb020799d9cbfec2adcca50e9644f2613f041648734459d29f88a0d
via U6-CDE205-1 [3.4.0.7] 9000, D=0.229732 ms, ND=0.223568 ms
H=00:00:08, U=00:00:22
```

Where 3.4.0.7 is ProximityEngine1's interface and 3.1.14.17 is ProximityEngine2's interface and is stored in each other tables.

When a request arrives from the client machine, whose client IP belongs to the 3.4.0.0/16 network (which happens to be from AS-1), say for example, 3.4.0.10, the SR looks up in the configured Proximity Servers and selects the Proximity Server with the lowest IP address, which in this case happens to be 3.1.14.17.

The SR would send the SOAP request with the PSA 3.4.0.10 to ProximityEngine2 (3.1.14.17).

ProximityEngine2, would lookup the URIB table to find out if there is another Proximity Engine from the same AS. Since, in this case, there is ProximityEngine1 in AS-1 from where the request has emanated, it returns a Redirect message with ProximityEngine1's IP address as the request end-point.

The SR redirects the SOAP request to the ProximityEngine1.

ProximityEngine1 would look up its URIB table and return the cost for the available PTAs.

The Service Router, upon receiving the cost from the ProximityEngine1, would choose the PTA with lowest cost and give the SE redirection to the client.

The client would now contact the SE and play the content.

Community-Based Proximity Algorithm Example

The following example shows how to use the **proximity algorithm bgp** command to enable the community-based proximity algorithm:

```
ServiceRouter(config)# proximity algorithm bgp location-community
ServiceRouter(config)# exit
ServiceRouter# show ip proximity algorithm
Proximity algorithm: bgp community
```

The following example shows how to configure community values. In this example, the first **location community** command configures the community value 100:10 and the second command configures community values from 100:100 to 100:200:

```
ServiceRouter(config)# router bgp 23
ServiceRouter(config-bgp)# location community 100:10
ServiceRouter(config-bgp)# location community 100:100-100:200
```

The following example shows how to enable the proximity redirect option:

```
ServiceRouter(config)# proximity algorithm bgp redirect
```

First, each Proximity Engine must form a DHT ring:

```
ServiceRouter(config)# router srp
ServiceRouter(config-srp)# domain 100
ServiceRouter(config-srp)# bootstrap 192.168.10.1
```

Each Proximity Engine must advertise its interface address to the BGP cloud by configuring IGP for OSPF and IS-IS or configuring BGP with the neighbor.

The following example is for OSPF:

```
ServiceRouter(config)# router ospf
ServiceRouter(config-ospf)# network 192.168.10.0 255.255.255.0 area 0
```

The following example is for configuring BGP:

```
ServiceRouter(config)# router bgp
ServiceRouter(config-bgp)# neighbor 192.168.82.1 remote-as 23
```

The following examples shows how to configure the BGP AS path length-based proximity. This example is for the same AS configuration:

```
ServiceRouter(config)# proximity algorithm bgp best-path
ServiceRouter(config)# router bgp 23
ServiceRouter(config-bgp)# neighbor 192.168.82.1 remote-as 23
```

The following example is for a different AS configuration:

```
ServiceRouter(config)# proximity algorithm bgp best-path
ServiceRouter(config)# router bgp 10
ServiceRouter(config-bgp)# neighbor 192.168.82.1 remote-as 23
```

Proximity Algorith BGP Best-Path Example

The following example shows how to turn on the BGP Best-Path algorithm:

```
ProximityEngine(config)# proximity algorithm bgp best-path

ProximityEngine# show ip bgp 3.1.14.0
BGP routing table entry for 3.1.14.0/24, version 4
Paths: (1 available, best #1)
Flags: on xmit-list, is in urib, is best urib route
```

```
Path type: internal, path is valid, is best path
AS-Path: 2 , path sourced external to AS
3.4.0.12 (metric 0) from 3.4.0.12 (3.4.0.12)
Origin IGP, MED 0, localpref 100, weight 0
Community: 1:1

Not advertised to any peer
```

The following is a sample of the service-router logs with respect to the cost returned by the Proximity Engine:

```
02/08/2010 07:34:42.290(Local)(5792)TRCE:SRNetProxClient.cpp:86->
Target
Hostname => U6-WAE612-2
IpAddress => 3.4.0.14
Rating => 2147483648
02/08/2010 07:34:42.290(Local)(5792)TRCE:SRNetProxClient.cpp:86->
Target
Hostname => U6-WAE612-1
IpAddress => 3.1.14.7
Rating => 2164260864
```

In the previous example, since the PTA 3.1.14.7 has a higher cost, the PTA 3.4.0.17 gets a higher preference owing to the lower cost.

The following example shows how to verify proper connectivity between the two Proximity Engines:

```
ProximityEngine1# show srp neighbor
Codes: T - local node, L - leafset, P - primary, S - secondary, B - backup
I - Intransitive, R - Replicate Set, D - delay, ND - New Delay
H - hold time, U - up time

Number of neighbors in the database: 1
RPL c152b683f000c6be3ff82214e4d8084d52a44dee85b29d67c49e60fbaf3e4737
via U6-CDE205-2 [3.1.14.17] 9000, D=0.395056 ms, ND=0.378471 ms
H=00:00:09, U=00:38:37

ProximityEngine1# show srp database
c9bc3e170457a6a08d8a218a15a00d8feb73e4295d06f7e014b6f66fee01c9e4: 793
```

Enter the same commands to check the SRP connection on the other Proximity engine:

```
ServiceRouter# show srp neighbor
Codes: T - local node, L - leafset, P - primary, S - secondary, B - backup
I - Intransitive, R - Replicate Set, D - delay, ND - New Delay
H - hold time, U - up time

Number of neighbors in the database: 1
RPL 97d35b9f3cb020799d9cbfec2adcca50e9644f2613f041648734459d29f88a0d
via U6-CDE205-1 [3.4.0.7] 9000, D=0.495889 ms, ND=0.470399 ms
H=00:00:07, U=00:40:57

ProximityEngine2# show srp database
c9bc3e170457a6a08d8a218a15a00d8feb73e4295d06f7e014b6f66fee01c9e4: 793
```

Related Commands

Command	Description
show ip proximity algorithm	Displays the proximity algorithm options currently in use by this Proximity Engine.

proximity engine enable

To enable the Proximity Engine, use the **proximity engine enable** command in Global configuration mode. To disable the Proximity Engine, use the **no** form of this command.

proximity engine enable

no proximity engine enable

Syntax Description

This command has no arguments or keywords.

Command Modes

Global configuration (config) mode.

Usage Guidelines

The Proximity Engine is a device mode which needs to be enabled on the Service Router in order to enable dynamic routing protocols OSPF/IS-IS/BGP. You can turn on the Proximity Engine functionality using the **proximity engine enable** command. Only after enabling the Proximity Engine, all the routing functionality is enabled and related commands are unlocked. Once the Proximity Engine is enabled, you can turn on either OSPF or IS-IS for IGP and/or BGP. But in the Proximity Engine device, we do not make use of the OSPF process-id, which we generally do on the router.

When disabling the Proximity Engine after issuing the **no proximity engine enable** command, you are asked to confirm this action because all Proximity Engine configurations are lost when you enter this command.

Examples

The following example shows how to enable the Proximity Engine:

```
ServiceRouter# configure terminal
ServiceRouter(config)# proximity engine enable
```

The following example shows how to disable the Proximity Engine:

```
ServiceRouter# configure terminal
ServiceRouter(config)# no proximity engine enable
All Proximity Engine configuration will be lost! Proceed? [ no ] yes
ServiceRouter(config)#
```

The following example shows how to enable OSPF:

```
ServiceRouter# config
ServiceRouter (config)# proximity engine enable
Starting Proximity Engine ....
Proximity Engine Started.
ServiceRouter (config)# router ospf
ServiceRouter (config-ospf)# network 15.0.0.0 ?
  A.B.C.D  IP wildcard mask
ServiceRouter (config-ospf)# network 15.0.0.0 0.255.255.255 ?
  area  Configure area properties
ServiceRouter (config-ospf)# network 15.0.0.0 0.255.255.255 area 0 ServiceRouter#
ServiceRouter (config-ospf)#
```

Note OSPF process ID is used.

Enter the following commands on the router:

```
Router (config)# router ospf 1
Router (config-ospf)# network 15.0.0.0 0.255.255.255 area 0
Router (config-ospf)#

<Turned on OSPF debugging on Router>

*Jun 29 01:14:08.642: OSPF: Interface GigabitEthernet0/0 going Up *Jun 29 01:14:09.142:
OSPF: Build router LSA for area 0, router ID 2.2.2.2, seq 0x80000001, process 1 *Jun 29
... Output omitted

<2.2.2.2 is the Router-id of the Router>
```

Verify adjacency on the Proximity Engine by entering the following commands:

```
ServiceRouter# show ip ospf route
 OSPF Process ID p1 context default, Routing Table
  (D) denotes route is directly attached      (R) denotes route is in
RIB
15.0.0.0/8 (intra)(D) area 0
     via 15.0.0.1/GigabitEthernet 2/0*, cost 65535, adv router 3.1.5.2

ServiceRouter# show ip ospf database
        OSPF Router with ID (3.1.5.2) (Process ID p1 context default)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link
Count
2.2.2.2         2.2.2.2         140         0x80000002 0xb04d   1
3.1.5.2         3.1.5.2         140         0x80000002 0x100d   1

                Network Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
15.0.0.1        3.1.5.2         140         0x80000001 0x2408
```

The following example shows how to enable BGP:

```
ServiceRouter# config
ServiceRouter(config)# proximity algorithm bgp location-community
!
ServiceRouter(config)# router bgp 1
ServiceRouter(config-bgp)# neighbor 5.45.1.101 remote-as 1 <-- configures a BGP peer in
Autonomous System (AS) 1. This peer advertises BGP routes to the PxE.
ServiceRouter(config-bgp)# location community 1:1 <-- configures 1:1 as a
location-community used by BGP location-community proximity algorithm.
ServiceRouter(config-bgp)# exit
```

The following example shows how to enable IS-IS:

```
ServiceRouter# config
ServiceRouter(config)# router isis
ServiceRouter(config-isis)# net 49.0000.0000.0205.0002.00 <-- Configures the Network
Entity Title (NET).
ServiceRouter(config-isis)# interface GigabitEthernet 1/0 <-- PxE interface actively
running IS-IS.
ServiceRouter(config-isis)# ip router isis
ServiceRouter(config-isis)# exit
ServiceRouter(config-isis)# interface GigabitEthernet 2/0 <-- PxE interface actively
running IS-IS.
```

```
ServiceRouter(config-isis)# ip router isis
ServiceRouter(config-isis)# exit
```

The following example shows how to enable SRP:

```
ServiceRouter# config
ServiceRouter(config)# router srp
ServiceRouter(config-srp)# bootstrap 172.20.168.89 <-- A boot-strap-node is an existing
member of the DHT ring.
ServiceRouter(config-srp)# domain 1 <-- All SRP nodes have the same domain number to be in
a DHT ring
ServiceRouter(config-srp)# exit
```

Related Commands

Command	Description
service-router proximity-based-routing	Configures proximity-based routing on the Service Router.

pwd

To view the present working directory, use the **pwd** command in EXEC configuration mode.

pwd

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

EXEC configuration mode.

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

Command	Description
cd	Changes from one directory to another directory.
dir	Displays a detailed list of files contained within the working directory, including names, sizes, and time created.
lls	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.
ls	Lists the files or subdirectory names within a directory.

radius-server

To configure RADIUS authentication parameters, use the r**adius-server** command in Global configuration mode. To disable RADIUS authentication parameters, use the **no** form of this command.

radius-server {**enable | host** {*hostname* | *host_ipaddr*} [**auth-port** *port*] | **key** *keyword* | **redirect** {**enable | message** *reply* **location** *url*} | **retransmit** *retries* | **timeout** *seconds*}

no radius-server {**enable | host** {*hostname* | *host_ipaddr*} | **key** | **redirect** {**enable | message** *reply* **location** *url*} | **retransmit | timeout**}

Syntax Description

enable	Enables HTTP RADIUS authentication.
host	Specifies a RADIUS server.
hostname	Hostname of the RADIUS server.
host_ipaddr	IP address of the RADIUS server.
auth-port	(Optional) Sets the UDP port for the RADIUS Authentication Server.
port	UDP port number (from 1 to 65535). The default is 1645.
key	Specifies the encryption key shared with the RADIUS server.
keyword	Text of the shared key (maximum of 15 characters).
redirect	Redirects the response if an authentication request fails.
enable	Enables the redirect feature.
message	Replies with an authentication failure message.
reply	Reply message text string (maximum of 24 characters).
location	Sets the HTML page location, for example, http://www.cisco.com.
url	URL destination of authentication failure instructions.
retransmit	Specifies the number of transmission attempts to an active server.
retries	Number of transmission attempts for a transaction (from 1 to 3).
timeout	Time to wait for a RADIUS server to reply.
seconds	Wait time in seconds (from 1 to 20).

Command Defaults

auth-port *port*: UDP port 1645

retransmit *retries*: 2

timeout *seconds*: 5

Command Modes

Global configuration (config) mode.

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 sent. If you do not configure a RADIUS key, packets are not encrypted. The key itself is never sent 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 Through RADIUS" section on page 2-291.
- 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 2-292.

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** keyword 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** keyword 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 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 CDSM GUI or the CLI to enable RADIUS authentication on an SE.

Tip From the CDSM GUI, choose **Devices > General Settings > Authentication**. Use the displayed Authentication Configuration window.

To use the SE CLI to enable RADIUS authentication on an SE, enable RADIUS authentication for normal login mode by entering the **authentication login radius** command in Global configuration mode as follows:

```
ServiceEngine(config)# authentication login radius enable [primary] [secondary]
```

Use the **authentication configuration radius** command in Global configuration mode 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** command in Global configuration mode.

Examples

The following example shows how to enable the RADIUS client, specify a RADIUS server, specify the RADIUS key, accept 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

Command	Description
debug authentication user	Debugs the user login against the system authentication.
rule	Sets the rules by which the SE filters HTTP, HTTPS, and RTSP traffic.
show radius-server	Displays RADIUS information.

rcp

To enable the Remote Copy Program (RCP), use the **rcp** command in Global configuration mode. To disable RCP, use the **no** form of this command.

rcp enable

no rcp enable

Syntax Description

enable	Enables RCP services.

Command Defaults

None

Command Modes

Global configuration (config) mode.

Examples

The following example shows how to enable RCP:

```
ServiceEngine(config)#  rcp enable
```

Related Commands

Command	Description
show rcp	Displays RCP information.

reload

To halt and perform a cold restart on the SE, use the **reload** command in EXEC configuration mode.

reload [**force**]

Syntax Description

force	(Optional) Forces a reboot without further prompting.

Command Defaults

None

Command Modes

EXEC configuration mode.

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 shows how to reload the SE after you have saved the configuration changes.

```
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 .....
```

The following example forces a reboot on the SE:

```
ServiceEngine# reload force
```

Related Commands

Command	Description
cache synchronize	Saves any file system contents to disk from memory before a restart.
write	Saves startup configurations.
write erase	Erases the startup configuration from NVRAM.

rename

To rename a file on the SE, use the **rename** command in EXEC configuration mode.

rename *old_filename new_filename*

Syntax Description

old_filename	Original filename.
new_filename	New filename.

Command Defaults

None

Command Modes

EXEC configuration mode.

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

Command	Description
cpfile	Creates a copy of a file.

restore

To restore the device to its manufactured default status, removing the user data from the disk and flash memory, use the **restore** command in EXEC configuration mode. 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	(Optional) Selects basic network configurations.

Command Defaults

None

Command Modes

EXEC configuration mode.

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 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, 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. If you want to re-enable the CDS network after using the **restore factory-default preserve basic-config** command, 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 disks** command after the **restore** command verifies that the **restore** command has removed data from the partitioned file systems (sysfs and cdnfs):

```
ServiceEngine# show disks

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** command continues 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

Command	Description
cms database backup	Backs up the existing management database for the CDSM.
cms database restore	Restores the database management tables using the backup local filename.
show disks	Displays the names of the disks currently attached to the SE.
show running-config	Displays the current running configuration information on the terminal.
show startup-config	Displays the startup configuration.
show wmt	Displays WMT bandwidth and proxy mode configuration.

rmdir

To delete a directory, use the **rmdir** command in EXEC configuration mode.

rmdir *directory*

Syntax Description

directory	Name of the directory that you want to delete.

Command Defaults

None

Command Modes

EXEC configuration mode.

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 shows how to remove the oldfiles directory under /local1:

```
ServiceEngine# rmdir /local1/oldfiles
```

Related Commands

Command	Description
lls	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.
ls	Lists the files or subdirectory names within a directory.
mkdir	Creates a new directory or subdirectory in the SE file system.

router bgp

To configure a BGP routing process, use the **router bgp** command in Global configuration mode. To remove a BGP routing process, use the **no** form of this command.

router bgp *as_number*

no router bgp *as_number*

Syntax Description

as_number	Number of an Autonomous System (AS) that identifies the router to other BGP routers, and tags the routing information that is passed along.

Command Defaults

No BGP routing process is configured.

Command Modes

Global configuration (config) mode.

Usage Guidelines

This command is used to set up a distributed routing core that automatically guarantees the loop-free exchange of routing information between autonomous systems.

Enable the Proximity Engine by entering the **proximity engine enable** command before executing this command.

For the proximity function to work, one of the following is required:

- Enabled link-state protocol, such as OSPF or IS-IS for IGP proximity.
- Enabled policy routing protocol, such as BGP for best-path proximity, and one of the IGP (OSPF or IS-IS) is required for next hop resolution.

Note All BGP routes must resolve to IGP next hops or directly connected routes.

Examples

The following example shows how to configure a BGP process for autonomous system 23:

```
ServiceRouter(config)# router bgp 23
ServiceRouter(config-bgp)#
```

Related Commands

Command	Description
location community	Configures the community values that are associated with a Proximity Engine.
log-neighbor-changes	Enables logging of BGP neighbor resets.
neighbor	Configures the BGP neighbors.

router isis

To enable the IS-IS routing protocol and to specify an IS-IS process, use the **router isis** command in Global configuration mode. To disable IS-IS routing, use the **no** form of this command.

router isis

no router isis

Syntax Description

This command has no arguments or keywords.

Command Defaults

IS-IS routing is disabled.

Command Modes

Global configuration (config) mode.

Usage Guidelines

This command is used to enable routing for an area. An appropriate network entity title (NET) must be configured to specify the area address and the system ID of the router. Routing must be enabled on one or more interfaces before adjacencies can be established and dynamic routing is made possible.

Enable the Proximity Engine by entering the **proximity engine enable** command before executing this command.

Note It is not possible to configure IS-IS and OSPF simultaneously. If you are running OSPF and try to enter the **router isis** command, you receive the following warning message:

```
%Cannot configure both IS-IS and OSPF together. Please remove 'router ospf' first. (Error
number: 1137)
```

If you want to configure IS-IS and you already have OSPF running, you must enter the **no router ospf** command first before entering the **router isis** command.

Examples

The following example shows how to configure IS-IS for IP routing. In this example, system ID is set to 0001.0c11.1111.00 and area is set to ID 47.0004.004d.0001. IS-IS is configured to form adjacencies on Ethernet interface 0 and serial interface 0. The IP prefix assigned to Ethernet interface 0 is advertised to other IS-IS routers.

```
ServiceRouter# show node-type
PROXIMITY_ENGINE

ServiceRouter# config t
ServiceRouter(config)# router isis
ServiceRouter(config-isis)# net 47.0004.004d.0001.0001.0c11.1111.00
ServiceRouter(config-isis)# interface GigabitEthernet 1/0
ServiceRouter(config-isis-if)# ip router isis
ServiceRouter(config-isis-if)# end
ServiceRouter#
```

Related Commands

Command	Description
authentication	Configures the authentication parameters.
authentication-check	Enables the checking of received packets on the corresponding level.
authentication-type	Specifies the cleartext or MD5 authentication for the corresponding level.
interface	Configures a Gigabit Ethernet or port channel interface. Provides access to interface configuration mode.
is-type	Configures a Proximity Engine to act as a Level 1 (intra-area) router, as both a Level 1 router and a Level 2 (intra-area) router, or as an inter-area router only.
log-adjacency-changes	Configures the router to send a syslog message when an IS-IS neighbor goes up or down.
lsp-mtu	Sets the maximum transmission unit MTU size of IS-IS LSPs.
net	Configures an IS-IS NET for a CLNS routing process.

router ospf

To enable the Open Shortest Path First (OSPF) routing process, use the **router ospf** command in Global configuration mode. To terminate the OSPF process, use the **no** form of this command.

router ospf

no router ospf

Syntax Description

This command has no arguments or keywords.

Command Defaults

This command is disabled by default.

Command Modes

Global configuration (config) mode.

Usage Guidelines

For Proximity Engine, the fixed process ID “p1” is used internally. This allows only one instance of the OSPF process, but it supports multiple areas. Routing must be enabled on one or more interfaces before adjacencies can be established and before dynamic routing is possible.

Enable the Proximity Engine by entering the **proximity engine enable** command before executing this command.

Note It is not possible to configure IS-IS and OSPF simultaneously. If you are running IS-IS and try to enter the **router ospf** command, you receive the following warning message:

%Cannot configure both IS-IS and OSPF together. Please remove 'router ospf' first. (Error number: 1137)

If you want to configure OSPF and you already have IS-IS running, you must enter the **no router isis** command first before entering the **router ospf** command.

Examples

The following example shows how to configure an OSPF routing process:

```
ServiceRouter# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ServiceRouter(config)# router ospf
ServiceRouter(config-ospf)# end
ServiceRouter#
```

Related Commands

Command	Description
area	Configures the area.
authentication	Configures the authentication parameters.
authentication-check	Enables the checking of received packets on the corresponding level.
authentication-type	Specifies the cleartext or MD5 authentication for the corresponding level.
interface	Configures a Gigabit Ethernet or port channel interface. Provides access to interface configuration mode.
log-adjacency-changes	Configures the router to send a syslog message when an IS-IS neighbor goes up or down.
network area	Defines the interfaces on which OSPF runs and defines the area ID for those interfaces.

router srp

To enter SRP configuration mode, use the **router srp** command in Global configuration mode. To negate the SRP daemon and remove all SRP running configuration, use the **no** form of this command.

router srp

no router srp

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

Global configuration (config) mode.

Usage Guidelines

This command is used to enter SRP configuration mode, where a system administrator can configure different parameters of the SRP.

Enable the Proximity Engine by entering the **proximity engine enable** command before executing this command.

For SRP to run properly, it is necessary to configure the NTP server on the SR. Configure NTP as follows:

```
ServiceRouter(config)# ntp server 171.68.10.150
ServiceRouter(config)# end
ServiceRouter# sh ntp status ntp enabled server list: 2.8.1.2 171.68.10.150
remote refid st t when poll reach delay offset jitter
==============================================================================
2.8.1.2 0.0.0.0 16 u - 64 0 0.000 0.000 4000.00
*ntp-sj1.cisco.c ntp02-syd.cisco 2 u 63m 137m 177 1.625 -1.806 0.881
ServiceRouter#
```

Examples

The following example shows the use of **router srp**:

```
ServiceRouter# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ServiceRouter(config)# router srp
ServiceRouter(config-srp)#
```

Related Commands

Command	Description
bootstrap-node	Configures a bootstrap node IP address.
domain	Sets the domain ID for an SRP.
flooding	Configures the flooding threshold.

rtsp

To configure the Real-Time Streaming Protocol (RTSP)-related parameters, use the **rtsp** command in Global configuration mode. 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.
ip_address	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.
time_delay	The RTSP advanced maximum initial setup delay, in seconds. The range is from 0 to 2147483647.
max-request-rate	Specifies the maximum incoming requests allowed by the RTSP Gateway per second.
num	The maximum requests per second. The range is from 1 to 2147483647.
ip-address	Configures the IP address for the RTSP gateway.

Command Defaults

max-initial-setup-delay *time_delay*: 10

max-request-rate *num*: 40 requests

Command Modes

Global configuration (config) mode.

Usage Guidelines

Real-Time Streaming Protocol (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:

- URL and its position in the Unified Name Space (UNS)
- User agent
- IP address of the final destination
- 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 3-11 lists the default settings for the RTSP gateway.

Table 3-11 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 3-11 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).
- 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 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

Command	Description
show rtsp	Displays the RTSP configurations.

rule

To set the rules by which the SE filters HTTP, HTTPS, and RTSP traffic, use the **rule** command in Global configuration mode. To disable individual options, use the **no** form of this command.

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** *key_id* {**key-id-number** *key_id_number*} {**pattern-list** *patterm_list_num*} [**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**}] | **enable** | **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-regsub** *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** *key_id* {**key-id-number** *key_id_number*} {**pattern-list** *patterm_list_num*} [**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**}] | **enable** | **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-regsub** *url_regexp url_sub*}}}

Syntax Description

action	Describes the action that the rule is to take.
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.
pattern-list	Configures the pattern list.
list_num	Pattern list number. The range is from 1 to 512.
protocol	Specifies the protocol for which this rule is to be matched.
all	Matches this rule with all applicable protocols for this action.
protocol_type	Protocol types that support rule actions, namely, **http**, **https**, and **rtsp**. **Note** The term **http** traffic is used to see 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.

pattern_type	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 which ranges from 1 to 32. The key is a shared secret string.
key_id	Owner of the key.
key-id-number	Specifies the identification number of the key. The range is from 1 to 16.
key_id_num	Identification number of the key.
pattern-list	Specifies the number of the pattern list. The range is from 1 to 512. Valid patterns are domain, url-regex, or dst-ip.
pattern_list_num	Specifies the number of the pattern list.
no-cache	Does not cache the object.
redirect	Redirects the request to the rewritten URL.
url	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.
service_name	Service name used for handling a request through an ICAP server.
validate-url-signature	Validates a signed URL.
error-redirect-url	Specifies the error HTTP URL. **Note** This keyword is only supported for HTTP URLs.
exclude	Specifies what field in the URL signature must be validated.
all	Specifies both client-ip and expiry time fields are excluded in validation.
client-ip	Specifies that the client-ip field is excluded in validation.
domain-name	Specifies that the domain-name is excluded in validation.
expiry-time	Specifies that the expire-time field is excluded in validation.
domain	Specifies the regular expression to match the domain name.
dn_regexp	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	Specifies the header field pattern of the request and substitute replacement pattern.
referer	Specifies the referer request header.
ref_regexp	Regular expression to be matched with the referer request header.
request-line	Specifies the request method line.
req_regexp	Regular expression to be matched with the request method line.
user-agent	Specifies the user agent request header.
ua_regexp	Regular expression to be matched with the User Agent request header.
src-ip	Specifies the source IP address of the request.
s_ipaddress	Source IP address of the request.
s_subnet	Source IP subnet mask.
url-regex	Specifies the regular expression to match a substring of the URL.
url_regexp	Regular expression to be matched with the URL string.
url-regsub	Sets the regular expression to match the URL and replacement pattern.
url_sub	URL string replacement pattern.

Command Defaults

The default is rule processing disabled.

The **group-type** pattern is OR by default.

Command Modes

Global configuration (config) mode.

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

Note The regsub attribute supports regular expressions, but only one substitution can be defined. Multiple substitutions are not supported. Also, only one url-regsub pattern list is supported. Multiple substitutions for the same pattern list are not supported.

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 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 rule actions for RTSP requests.

WMT supports all the rule action types—allow, block, no-cache, redirect, refresh, replace, rewrite, validate-url-signature, and generate-url-signature. RTMP and Movie Streamer only support allow, block, and validate-url-signature.

Note If the **rule action generate-url-signature** command with the parameter **include-client-src-ip key-id-owner 3 key-id-number 3 pattern-list 2** is entered, with and without protocol parameters, the "rule entry is duplicate" message is displayed. If the protocol is not specified in that particular pattern list, all protocols are accepted.

This command removes the trailing "protocol all" when it displays in the running-config. All service rule-related commands have this functionality. Also, the **rule action allow pattern-list 1 ?** command does not have a help message indicating "protocol all" is the default value if it is omitted.

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 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 is taken for all the traffic that goes through the SE.

Execution Order of Rule Actions

The order in which the rule actions are executed is different between the Web Engine and the other protocol engines (Windows Media Streaming, Movie Streamer, and Flash Media Streaming).

Note For the Web Engine, the Service Rule file must be used if service rules are to be configured. This is done though the CDSM, not the CLI. For more information, see Appendix F "Creating Service Rule Files" of the *Cisco Internet Streamer CDS 3.2 Software Configuration Guide*.

Note Configuring Service Rules for Flash Media Streaming is no longer done through the CLI; it is done through the Authorization Server Rules plug-in. See the "Configuring Service Rules" section in the *Cisco Internet Streamer CDS 3.2 Software Configuration Guide*.

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.

Web Engine Rule Action Order

The order in which the rule actions are executed for the Web Engine is as follows:

1. block or allow

Note The allow and block actions 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.

2. redirect (before cache lookup)
3. rewrite (before cache lookup)
4. use-icap-service
5. generate-url-signature
6. validate-url-signature
7. refresh (after cache lookup, in the case of cache hit)
8. no-cache

All Other Protocol Engine Rule Action Order

The order in which the rule actions are executed for the other protocol engines is the order in which they were configured, except for the validate-url-signature action. If the rule pattern associated with the validate-url-signature action is matched, regardless of the configuration order the rules, the validate-url-signature action is performed before any other action.

1. validate-url-signature
2. block or allow

Note The allow and block actions 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.

3. redirect (before cache lookup)
4. rewrite (before cache lookup)

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. Following are the four patterns of expected behavior:
  - **Pattern 1**

    rule pattern-list 22 group-type and

    rule pattern-list 22 url-regsub 10 airforce

    rule pattern-list 22 url-regsub wma wmv

    rule pattern-list 23 url-regsub 10 airforce

    rule pattern-list 23 url-regsub wma wmv
  - **Pattern 2**

    rule pattern-list 22 group-type and

    rule pattern-list 22 url-regsub 10 airforce

    rule pattern-list 23 url-regsub wma wmv
  - **Pattern 3**

    rule pattern-list 22 group-type or

    rule pattern-list 22 url-regsub 10 airforce

    rule pattern-list 22 url-regsub wma wmv

    rule pattern-list 23 url-regsub 10 airforce

    rule pattern-list 23 url-regsub wma wmv

– **Pattern 4**

rule pattern-list 22 group-type or

rule pattern-list 22 url-regsub 10 airforce

rule pattern-list 23 url-regsub wma wmv

Note The rules are that when AND is specified for a pattern-list ALL the conditions satisfy. When OR is specified, ANY of the condition are matched.

- **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-regsub**—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:

- If **allow** rules are configured, then it is an implicit deny.

  For example, if all URL requests that match HTML are blocked, implicitly, all requests that match other URL requests are allowed.

- If **deny** rules are configured then it is implicit allow.

  If all URL requests that match WMV are allowed, implicitly, all request that match other URL requests are blocked.

- If both **allow** and **deny** are configured, then it is an implicit allow.

  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-regsub 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 starts a request to the rewritten URL.

```
Cache(config)# rule pattern-list 2 url-regsub 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-regsub**. 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-regsub 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
```

The following example covers both uppercase and lowercase expressions of MP4 files:

```
ServiceEngine(config)# rule pattern-list 2 url-regex http://(.*.)cdsis.com/(.*.)[mM]
[pP]4(.*)
```

Related Commands

Command	Description
clear	Clears the HTTP object cache, the hardware interface, statistics, archive working transaction logs, and other settings.
show rule	Displays rules configuration information.

script

To execute a script provided by Cisco or check the script for errors, use the **script** command in EXEC configuration mode.

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.
file_name	Name of the script file.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The **script** command in EXEC configuration mode opens the script utility, which allows you to execute scripts supplied by Cisco 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 in scripts supplied by Cisco. You cannot execute script files that lack Cisco signatures or that have been corrupted or modified.

Examples

The following example shows how to check for errors in the script file foo.script:

```
ServiceEngine# script check foo.script

 Script file foo.script is valid.
```

service

To specify the type of service, use the **service** command in EXEC configuration mode.

On the CDSM:

service csm restart

On the SE:

service {**acquisition restart | csm restart | distribution restart | flash-media-streaming restart | ms restart | rtspg restart | web-engine restart | wmt restart**}

On the SR:

service {**cms restart | service-router restart**}

Syntax Description

acquisition	Specifies Acquisition services.
restart	Restarts the specified services.
csm	Specifies CMS services.
distribution	Specifies Distribution services.
flash-media-streaming	Specifies Flash Media Streaming services.
ms	Specifies Movie Streamer services.
rtspg	Specifies RTSP Gateway services.
service-router	Specifies Service Router services.
web-engine	Specifies Web Engine services.
wmt	Specifies Windows Media services.

Command Defaults

None

Command Modes

EXEC configuration mode.

Examples

The following example shows how to start acquisition service:

```
ServiceEngine# service acquisition restart
The service acquirer has been restarted successfully!
ServiceEngine#
```

service-router

To configure service routing, use the **service-router** command in Global configuration mode. To disable last-resort routing, use the **no** form of this command.

On the SE:

service-router {**keepalive-interval** *num* | **service-monitor** {**augmentation-alarm enable** | **license-universal enable** | **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** {**augmentation** *num* | **burstcnt** *num* | **cpu** *num* | **disk** *num* | **faildisk** *num* | **fms** *num* | **kmemory** *num* | **memory** *num* | **movie-streamer** *num* |**nic** *num* | **wmt** *num*} | **transaction-log enable** | **type** {**all** | **cpu** | **disk** | **fms** | **kmemory** | **memory**| **movie-streamer** | **nic** | **wmt**}}}

no service-router {**keepalive-interval** *num* | **service-monitor** {**augmentation-alarm enable** | **license-universal enable** | **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** {**augmentation** *num* | **burstcnt** *num* | **cpu** *num* | **disk** *num* | **faildisk** *num* | **fms** *num* | **kmemory** *num* | **memory** *num* | **movie-streamer** *num* |**nic** *num* | **wmt** *num*} | **transaction-log enable** | **type** {**all** | **cpu** | **disk** | **fms** | **kmemory** | **memory** | **movie-streamer** | **nic** | **wmt**}}}

On the SR:

service-router service-monitor {**augmentation-alarm enable** | **number-of-samples** {**all** *num* | **cpu** *num* | **disk** *num* | **kmemory** *num* | **memory** *num*} | **sample-period** {**all** *num* | **cpu** *num* | **disk** *num* | **kmemory** *num* | **memory** *num*} | **threshold** {**augmentation** *num* | **cpu** *num* | **disk** *num* | **faildisk** *num* | **kmemory** *num* | **memory** *num*} | **type** {**all** | **cpu** | **disk** | **kmemory** | **memory**}}

no service-router service-monitor {**augmentation-alarm enable** | **number-of-samples** {**all** *num* | **cpu** *num* | **disk** *num* | **kmemory** *num* | **memory** *num*} | **sample-period** {**all** *num* | **cpu** *num* | **disk** *num* | **kmemory** *num* | **memory** *num*} | **threshold** {**augmentation** *num* | **cpu** *num* | **disk** *num* | **faildisk** *num* | **kmemory** *num* | **memory** *num*} | **type** {**all** | **cpu** | **disk** | **kmemory** | **memory**}}

On the CDSM:

service-router {**access-policy enable** | **content-based-routing** {**enable** | **redundant** *num*} | **lastresort** {**domain** *name* {**allow all** | **alternate** *name port_num*} | **error-domain** *name* **error-file** *port_num* | **translator** *ip_address port_num*} | **location-based-routing** {**enable** | **location-cache timeout** *num*} | **proximity-based-routing** {**enable** | **proximity-cache timeout** *num* | **proximity-server** *ip_address* **password** *password*} | **redirect-burst-control** {**enable** | **rate** *num*} | **redirect-mode** {**dns-redirect** {**all** | **domain** *domain*} | **ip-redirect**} | **service-monitor** {**augmentation-alarm enable** | **number-of-samples** {**all** *num* | **cpu** *num* | **disk** *num* | **kmemory** *num* | **memory** *num*}} | **subscribe domain** *domain* | **threshold** {**augmentation** *num* | **cpu** *num* | **disk** *num* | **kmemory** *num* | **memory** *num* | **transaction-log enable**}}

no service-router {**access-policy enable** | **content-based-routing** {**enable** | **redundant** *num*} | **lastresort** {**domain** *name* {**allow all** | **alternate** *name port_num*} | **error-domain** *name* **error-file** *port_num* | **translator** *ip_address port_num*} | **location-based-routing** {**enable** | **location-cache timeout** *num*} | **proximity-based-routing** {**enable** | **proximity-cache timeout** *num* | **proximity-server** *ip_address* **password** *password*} | **redirect-burst-control** {**enable** |

rate *num*} | **redirect-mode** {**dns-redirect** {**all** | **domain** *domain*} | **ip-redirect**} | **service-monitor** {**augmentation-alarm enable** | **number-of-samples** {**all** *num* | **cpu** *num* | **disk** *num* | **kmemory** *num* | **memory** *num*}} | **subscribe domain** *domain* | **threshold** {**augmentation** *num* | **cpu** *num* | **disk** *num* | **kmemory** *num* | **memory** *num* | **transaction-log enable**}}

Syntax Description

keepalive-interval	Specifies the SR keepalive interval in seconds.
keepalive_interval _num	Number of seconds. The range is from 1 to 120.
service-monitor	Configures Service Monitor related parameters.
augmentation-alarm	Alarm for checking the device level loads.
enable	Enables the augmentation alarm.
license-universal	Universal license feature to clear all alarms for Protocol Engines.
enable	Enables the universal license feature.
number-of-samples	Counts the latest sampled values to be used when calculating average.
all	Sets to all monitor types.
num	Count of latest sampled values to be used when calculating average. The range is from 1 to 120.
cpu	Enables the monitor CPU load.
disk	Sets the disk monitor type.
fms	Sets the FMS[1] monitor type.
kmemory	Sets the monitor kernel memory type.
memory	Sets the monitor memory type.
movie-streamer	Monitors the Movie Streamer stream count.
wmt	Sets the WMT[2] monitor type.
nic	Sets the Network Interface Card monitor type.
sample-period	Configures the time interval, in seconds, between two consecutive samples.
num	Time interval between two consecutive samples, in seconds. The range is from 1 to 60.
threshold	Configures threshold values.
augmentation	Applies the Augmentation alarm threshold as a percentage of the device parameter threshold.
num	Configures the Augmentation threshold values in percentage (1 to 100).
burstcnt	Configures the Protocol Engine Burst License Control monitor type.
num	Protocol Engine Burst License Control threshold value.
faildisk	Sets the disk failure monitor type.
num	Configures the Disk Failure Count threshold percentage (1-100). The default is 75 percent.
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 the access-policy.
enable	Enables the CDN Selector.

content-based-routing	Configures content based routing.
enable	Enables content based routing.
redundant	Specifies the number of redundant copies of the content.
num	Number of redundant copies of the content. The range is from 1 to 4.
lastresort	Configures the lastresort domain.
domain	Configures the domain.
name	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.
name	Alternate domain name.
error-domain	Configures error domain.
name	Error domain name.
translator	Configures the external translator IP address.
ip_address	External translator IP address.
port	(Optional) Specifies the port number.
port_num	Port number (1-65535).
error-file	Configures error file name.
port_num	Error file name.
location-based-routing	Configures location-based routing.
enable	Enables location-based routing.
location-cache	Configures the location cache.
timeout	Configures the location cache timeout.
num	Location cache timeout in seconds (0 to864000).
proximity-based-routing	Configures proximity-based routing.
enable	Enables proximity-based routing.
proximity-cache	Configures proximity cache.
timeout	Configures proximity cache timeout.
num	Proximity cache timeout, in seconds. The range is from 1 to 86400.
proximity-server	Configures proximity server IP address and port.
ip_address	IP address of proximity server.
redirect-burst-control	Configures the redirect burst control.
enable	Enables redirect burst control.
rate	Configures the redirect burst control rate (requests per second).
num	Redirect burst control rate. The range is from 1 to 100000.
redirect-mode	Enables the redirect mode. The redirect mode is disabled by default.

dns-redirect	Sets the redirect mode to DNS-based redirection. **Note** The TTL for the DNS proxy requests is one second. A one-second TTL ensures that the DNS proxy keeps sending requests to the Request Routing Engine, which in turn causes the Request Routing Engine to determine the best Service Engine at that point in time, and not to redirect the request to the same SE.
all	Enables the DNS-based redirection for all domains.
domain	Enables the DNS-based redirection for a specific domain.
domain	Name of the domain.
ip-redirect	Sets the redirect mode to IP-based 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.
num	Count of latest sampled values to be used when calculating average. The range is from 1 to 120.
cpu	Sets the CPU monitor type.
disk	Sets the disk monitor type.
kmemory	Sets the monitor kernel memory.
memory	Sets the monitor memory.
faildisk	Sets the disk failure monitor type.
sample-period	Configures the time interval between two consecutive samples.
subscribe	Configures the domains to which the service router should be subscribed.
domain	Configures the domain.
domain	Specifies the domain name.
threshold	Configures threshold values.
transaction-log	Configures Transaction logging for the Service Monitor.
enable	Enables transaction logging for the Service Monitor.
type	Configures the type to be monitored.

1. FMS = Flash Media Server
2. WMT = Windows Media Technology

Command Defaults

keepalive-interval: 2

redundant copies: 1

dns-ttl: 60

burstcnt: 1

location cache timeout: 691200 seconds (8 days)

content-based-routing: disabled

proximity cache timeout: 1800

sample-period: 1

nic sample-period: 3

number of samples: 2

faildisk: 75 percent

augmentation-alarm: disabled

transaction-logs: disabled

port number: 80

Command Modes

Global configuration (config) mode.

Usage Guidelines

To configure last-resort routing, use the **service-router** command in Global configuration mode, 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.

Augmentation Alarms

Augmentation alarms on the Service Monitor are soft alarms that send alerts before the threshold is reached. These alarms are applicable to all devices—Service Engines, Service Routers and CDSMs. Augmentation thresholds apply to device and Protocol Engine parameters.

Note For system disks (disks that contain SYSTEM partitions), only when all system disks are bad is the disk failure augmentation and threshold alarms raised. The disk fail threshold does not apply to system disks. The threshold only applies to CDNFS disks, which is also the case for the augmentation thresholds. This is because the system disks use RAID1. There is a separate alarm for bad RAID. With the RAID system, if the critical primary disk fails, the other mirrored disk (mirroring only occurs for SYSTEM partitions) seamlessly continues operation. However, if the disk drive that is marked bad is a critical disk drive (by definition this is a disk with a SYSTEM partition), the redundancy of the system disks for this device is affected.

As the **show disk** details command output reports, if disks have both SYSTEM and CDNFS partitions, they are treated as only system disks, which means they are not included in the accounting of the CDNFS disk calculation.

Location-Based Routing

The Geo-Location servers were introduced with the location-based routing method. Once you enable location-based routing, you must specify the Geo-Location servers.

The Authorization Service uses an XML file to allow or deny client requests based on the client's IP address or geographic location. The country, state, and city names in the Authorization XML file must match what is used by the Geo-Location server and the names are case sensitive.

Cross Domain 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.

Last-Resort Routing

Last-resort routing is not supported when dns-based-redirect is enabled.

Configuring the license-universal Command

Universal license is like a regular license but with higher BW and it applies to all PEs. When the user buys a universal license and configures this command, alarm data for all PEs is cleared. Thereafter monitoring of the PEs continues as usual for any future alarms. If universal license was already configured upon box reload (through saved configuration in the **show run** command), the existing licenses on the PEs is cleared and the PEs are monitored as usual for any future alarms.

The following information is cleared when you execute the **service-router service-monitor license-universal enable** command:

- Protocol Engine minor and major alarms

Note Alarm history commands continue to show all alarms as this is a different module.

- Protocol Engine internal vectors
- Protocol Engine alarm backup files in /tmp and /state

Burst Streaming License Control

Previously, the license limit was set to 500 Mbps and each protocol engine had a maximum number of sessions allowed. The base license limit is set to 200 sessions and 200 Mbps bandwidth.

When the number of sessions or current bandwidth usage exceeds the configured license limit on the Service Engine, the protocol engine raises an alarm and sends a `threshold exceeded` notification to the Service Router. Any new requests for that protocol engine are not routed to that Service Engine.

Note This feature only applies to the Windows Media Streaming engine, the Flash Media Streaming engine, and the Movie Streamer engine.

Configure Burst Count

The protocol engines can trigger multiple minor alarms for session and bandwidth exceeded threshold conditions. If multiple minor alarms are triggered for a protocol engine in a single day (24-hour interval), they are recorded as a single alarm.

The burst count, which indicates the number of days after which a major alarm is raised, is configurable. On the Service Engine, use the service-router service-monitor threshold burstcnt command to configure the burst count. The default setting is one (1), which means all the minor alarms that occur in a single day (24-hour interval) are counted as one single alarm. If the service-router service-monitor threshold burstcnt command is set to two, all minor alarms that occur in two days (48-hour interval) are counted as a single alarm.

Configure Universal License

A universal license is similar to a regular license, except it has a higher bandwidth and applies to all protocol engines (except Web Engine). When a universal license is purchased and configured, the alarm data for all protocol engines are cleared. Thereafter, the monitoring of the protocol engines continues as usual for any future alarms.

On the Service Engine, use the service-router service-monitor license-universal enable command to enable the universal license. The service-router service-monitor license-universal command is disabled by default.

Disk Failure Count Threshold

When the number of failed disks exceeds this threshold, no further requests are sent to this device and an alarm is raised. The Disk Failure Count Threshold is only for the CDNFS disks. Disk threshold configuration is the overall percentage of CDNFS disk failures after which an alarm is raised.

Note When an alarm is received for a SYSTEM disk, it is immediately marked as a failed disk. It is not checked against the Disk Failure Count Threshold. The SR continues redirecting to the SE, unless all SYSTEM disks on the SE are marked as failed disks

Domain Subscription

The **service-router subscribe domain** command allows us to specify domains to which the service router should be subscribed. By default the service-router takes all the domains specified in the CDSM. Even if you configure only one domain subscription through this command, the SR takes the list of domains subscribed through the CLI to be the complete list.

URL Translator

Use the **service-router lastresort domain** *domain* **translator** *ipaddress* command to configure the IP address of the third party URL translator. If a translator configuration is not present for any domain, it falls back to the alternate domain configuration. A maximum of one translator can be configured per content origin.

Service Router Transaction Log Fields

Table 3-12 describes the fields for the Service Router transaction log.

Table 3-12 Service Router Transaction Log Fields

Field	Description
c-ip	Source Internet Protocol (IP) address of the connected socket. This may be the IP address of a proxy server or firewall.
user-agent	Browser type used if the player was embedded in a browser. If the player was not embedded, this field refers to the user agent of the client that generated the log.
date	Date, in international date format, when a client is connected.
time	Time when the client is connected. The time format is either in Coordinated Universal Time (UTC) or local time, depending on how the logging plug-in is configured.
url	URL requested by the client.
protocol	Protocol used to access the content.
server-picked	Service Engine selected by the Service Router.
status	Status code.
routing-method	Routing method chosen. The routing-method field has the following possible values: • Last-Resort • Network • Proximity • Zero-Network • Geo-Location
routed-path	Request URL to redirect the client to a different CDN.

Service Monitor Transaction Logs

Service Monitor transaction logs provide an additional tool for analyzing the health history of a device and the protocol engines.

The device and service health information are periodically logged on the device in transaction log files. Transaction logs provide a useful mechanism to monitor and debug the system. The transaction log fields include both device and protocol engine information applicable to Service Engines and Service Routers that are useful for capacity monitoring. Additionally, when a device or protocol engine threshold is exceeded, detailed information is sent to a file (threshold_exceeded.log) to capture the processes that triggered the threshold alarm.

The Service Monitor transaction log filename has the following format: service_monitor_<*ipaddr*>_*yyyymmdd_hhmmss*_<>, where:

- <*ipaddr*> represents the IP address of the SE, SR, or CDSM.
- *yyyymmdd_hhmmss* represents the date and time when the log was created.

For example, service_monitor_192.168.1.52_20110630_230001_00336 is the filename for the log file on the device with the IP address of 192.168.1.52 and a time stamp of June 30, 2011 at 3:36 AM.

The Service Monitor transaction log file is located in the /local1/logs/service_monitor directory.

An entry to the Service Monitor transaction log is made every two seconds.

Note The following rules apply to Service Monitor transaction logs:

- A transaction log value is only logged if the Service Monitor is enabled for that component or protocol engine on the device. For example, if CPU monitoring is not enabled, the transaction log value "–" is displayed.
- If Service Monitor is enabled for a protocol engine, but the protocol engine is not enabled, the value is not displayed in the log file.
- If a log field can have more than one value, the values are delimited by the pipe (|) character.
- If a value can have sub-values, the sub-values are delimited by the carrot (^) character.
- Some of the fields display aggregate values. If the statistics are cleared using the clear statistics command, the value after clearing the statistics may be less than the previous values, or may be zero (0).

Table 3-13 describes the fields for the Service Monitor transaction log on an SE.

Table 3-13 SE Service Monitor Transaction Log Fields

Field	Sample Output	Description	Corresponding CLI Command
date	2011-06-30	Date of log.	–
time	22:52:02	Time of log.	–
cpu_avg	21	Moving average value in percentage of CPU usage.	show service-router service-monitor Device status—CPU—Average load
mem_avg	44	Moving average value in percentage of memory usage.	show service-router service-monitor Device status—Mem—Average used memory
kernel_mem_avg	11	Moving average value in percentage of kernel memory.	show service-router service-monitor Device status—KMEM—Average kernel memory
disk_avg	2	Moving average value in percentage of disk usage.	show service-router service-monitor Device status—Disk—Average load
disk_fail_count_ threshold	Y	Boolean value to indicate if disk fail count threshold has been reached.	show service-router service-monitor Device status—Device Status—Disk—Status
per_disk_load	disk03-01^2| disk04-02^5	Current load per disk, as a percentage. The sample output indicates that disk03–partition01 has a 2 percent load and disk04–partition02 have a 5 percent load.	–

Table 3-13 SE Service Monitor Transaction Log Fields (continued)

Field	Sample Output	Description	Corresponding CLI Command
bandwidth_avg	Port_Channel_ 1^2^4| Port_Channel_ 2^0^0	Moving average bandwidth used, as a percentage, of bandwidth in and bandwidth out per interface. The sample output indicates that port channel 1 has an average bandwidth of 2 percent for receiving and 4 percent for transmitting, and port channel 2 average bandwidth usage is 0.	**show service-router service-monitor** Device status—NIC—Average BW In/ Average BW Out
file_desc_count	1023	Total count of file descriptors open on the device. File descriptors are internal data structures maintained by the Linux kernel for each open file.	–
tcp_server_connections	35	Number of TCP server connections open.	**show statistics tcp** TCP Statistics—Server connection openings
tcp_client_connections	24	Number of TCP client connections open.	**show statistics tcp** TCP Statistics—Client connection openings
processes_count	42	Number of processes running on the device.	**show processes**
dataserver_cpu_ percentage	1	Percentage of the CPU used for the dataserver process.	–
ms_threshold_exceeded	–	Boolean value to indicate if the Movie Streamer threshold has been exceeded.	**show service-router service-monitor** Services status—MS—Threshold
ms_augment_threshold_ Exceeded	–	Boolean value to indicate if Movie Streamer augmentation alarm threshold has been exceeded.	–
ms_stopped	–	Boolean value to indicate if the Movie Streamer protocol engine has stopped.	**show service-router service-monitor** Services status—MS—Stopped
ms_rtsp_sessions_ count	–	Total Movie Streamer RTSP session count (aggregate value).	**show statistics movie-streamer all** Total RTSP sessions
ms_rtp_sessions_count	–	Total Movie Streamer RTP session count (aggregate value).	**show statistics movie-streamer all** Total RTP connections
fms_threshold_ exceeded	N	Boolean value to indicate if threshold is exceeded.	**show service-router service-monitor** Services status—FMS—Threshold
fms_augment_threshold_ exceeded	N	Boolean value to indicate if Flash Media Streaming augmentation alarm threshold has been exceeded.	–
fms_stopped	N	Boolean value to indicate if Flash Media Streaming has stopped.	**show service-router service-monitor** Services status—FMS—Stopped
fms_connections_count	2	Total Flash Media Streaming connection count (aggregate value).	**show statistics flash-media-streaming** Connections—Total

Table 3-13 SE Service Monitor Transaction Log Fields (continued)

Field	Sample Output	Description	Corresponding CLI Command
web_ engine_ threshold_exceeded	Y	Boolean value to indicate if the Web Engine threshold has been exceeded.	**show service-router service-monitor** Services status—Web—Threshold
web_ engine_augment_ threshold_exceeded	Y	Boolean value to indicate if Web Engine augmentation alarm threshold has been exceeded.	–
web_ engine_stopped	N	Boolean value to indicate if Web Engine has stopped.	**show service-router service-monitor** Services status—Web—Stopped
web_engine_cpu_ percentage	3	Percentage of the CPU used by the Web Engine.	–
web_engine_mem (bytes)	3500	Memory (in bytes) used by the Web Engine.	**show web-engine health** Total memory usage
web_engine_get_ requests	250	Count of get requests received by the Web Engine (Aggregate value)	**show statistics web-engine detail** HTTP Request Type Statistics—Get requests
web_engine_sessions	5	Count of HTTP connections.	**show statistics web-engine detail** Web-Engine Detail Statistics—Total HTTP Connection + Active Session
web_engine_upstream_ connections	2	Count of HTTP connections to upstream SE or origin server.	**show statistics web-engine detail** Web-Engine Detail Statistics—Total HTTP Connection
wmt_threshold_ exceeded	N	Boolean value to indicate if Windows Media Streaming threshold has been exceeded.	**show service-router service-monitor** Services status—WMT—Threshold
wmt_augment _threshold_exceeded	N	Boolean value to indicate if the Windows Media Streaming augmentation alarm threshold has been exceeded.	–
wmt_stopped	Y	Boolean value to indicate if Windows Media Streaming has stopped.	**show service-router service-monitor** Services status—WMT—Stopped
wmt_ml_cpu_percentage	21	Percentage of the CPU used by the WMT_ML process.	–
wmt_ml_mem (bytes)	32456	Memory (in bytes) used by WMT_ML process	–
wmt_core_cpu_ percentage	21	Percentage of the CPU used by the WMT_Core process.	–
wmt_core_mem (bytes)	32456	Memory (in bytes) used by the WMT_Core process.	–
wmt_unicast_sessions	22	Number of current concurrent unicast client sessions.	**show statistics wmt usage** Concurrent Unicast Client Sessions—Current
wmt_remote_sessions	24	Number of current concurrent remote server sessions.	**show statistics wmt usage** Concurrent Remote Server Sessions

Table 3-13 SE Service Monitor Transaction Log Fields (continued)

Field	Sample Output	Description	Corresponding CLI Command
wmt_live_requests	21	Total count of Windows Media Streaming live requests (Aggregate value).	**show statistics wmt requests** By Type of Content—Live content
wmt_vod_requests	22	Total count of Windows Media Streaming VOD requests (Aggregate value).	**show statistics wmt requests** By Type of Content—On-Demand Content
wmt_http_requests	11	Total count of Windows Media Streaming HTTP requests (Aggregate value).	**show statistics wmt requests** By Transport Protocol—HTTP
wmt_rtsp_requests	8	Total count of Windows Media Streaming RTSP requests (Aggregate value).	**show statistics wmt requests** By Transport Protocol—RTSPT/RTSPU
rtspg_tps	12	Current RTSP Gateway transactions per second (TPS).	–
uns_cpu_percentage	3	Percentage of CPU used by the Unified Namespace (UNS) process.	–
uns_mem (bytes)	3500	Memory used by the UNS process.	–

Table 3-14 describes the fields for the Service Monitor transaction log on a SR.

Table 3-14 SR Service Monitor Transaction Log Fields

Field	Sample Output	Description	Corresponding CLI Command
date	2011-06-30	Date of log.	–
time	22:52:02	Time of log.	–
cpu_avg	21	Moving average value in percentage of CPU usage.	**show service-router service-monitor Device status**—CPU—Average load
mem_avg	44	Moving average value in percentage of memory usage.	**show service-router service-monitor Device status**—Mem—Average used memory
kernel_mem_avg	11	Moving average value in percentage of kernel memory.	**show service-router service-monitor** Device status—KMEM—Average kernel memory
disk_avg	2	Moving average value in percentage of disk usage.	**show service-router service-monitor** Device status—Disk—Average load
disk_fail_count_ threshold	Y	Boolean value to indicate if disk fail count threshold has been reached.	**show service-router service-monitor** Device status—Device Status—Disk—Status
file_desc_count	1023	Total count of file descriptors open on the device. File descriptors are internal data structures maintained by the Linux kernel for each open file.	–

Table 3-14 SR Service Monitor Transaction Log Fields (continued)

Field	Sample Output	Description	Corresponding CLI Command
tcp_server_connections	35	Number of TCP server connections open.	**show statistics tcp** TCP Statistics—Server connection openings
tcp_client_connections	24	Number of TCP client connections open.	**show statistics tcp** TCP Statistics—Client connection openings
processes_count	42	Number of processes running on the device.	**show processes**
dataserver_cpu_ percentage	1	Percentage of the CPU used for the dataserver process.	–
sr_cpu_percentage	12	Cpu percentage used by SR.	–
sr_mem (bytes)	750000	Memory (in bytes) used by SR.	**show processes memory** and search for service_router
requests_received	34	Total count of requests received by SR (aggregate value)	**show statistics service-router summary** Requests Received
http_normal_requests_ received	5	Total count of normal HTTP requests received by SR (aggregate value).	**show statistics service-router summary** HTTP Requests (normal)
http_asx_requests_ received	5	Total count of ASX HTTP requests received by SR (aggregate value).	**show statistics service-router summary**- HTTP Requests (ASX)
rtsp_requests_received	5	Total count of RTSP requests received by SR (aggregate value).	**show statistics service-router summary** RTSP Requests
rtmp_requests_received	5	Total count of RTMP requests received by SR (aggregate value).	**show statistics service-router summary** RTMP Requests
dns_requests_received	6	Total count of DNS requests received by SR (aggregate value).	**show statistics service-router dns** Total DNS queries

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
```

Augmentation Alarms

The augmentation alarms threshold is a percentage, that applies to the CPU, memory, kernel memory, disk, disk fail count, NIC, and protocol engine usages. By default it is set to 80 percent.

As an example of an augmentation alarm, if the threshold configured for CPU usage is 80 percent, and the augmentation threshold is set to 80 percent, then the augmentation alarm for CPU usage is raised when the CPU usage crosses 64 percent.

If "A" represents the Service Monitor threshold configured, and "B" represents the augmentation threshold configured, then the threshold for raising an augmentation alarm = (A * B) / 100 percent.

The threshold value range is 1–100. The following command shows how to set the augmentation alarms threshold to 70 percent:

```
ServiceRouter(config)# service router service-monitor threshold augmentation 70
```

The following command shows how to reset the augmentation alarm threshold to the default:

```
ServiceRouter(config)# no service router service-monitor threshold augmentation 70
```

The **show service-router service monitor** command displays the augmentation alarm threshold configuration.

The **show alarms** command displays the alarms output.

The **show alarms history detail** command displays the history details.

The **show alarms detail** command displays the alarms details.

The **show alarms detail support** command displays the support information.

Cross Domain 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
```

The following example shows how to configure Proximity Engine cache on an SR:

```
ServiceRouter(config)# proximity engine enable
Starting Proximity Engine....
Proximity Engine Started.

ServiceRouter(config)# service-router proximity-based-routing proximity-server 127.0.0.1

ServiceRouter(config)# service-router proximity-based-routing proximity-cache timeout 600

ServiceRouter(config)# service-router proximity-based-routing enable
Please ensure you have purchased License for this advanced feature
ServiceRouter(config)# end
```

The following example shows how to enable DNS-based redirection with the cdsfms.com domain as the domain used to redirect all client requests to:

```
ServiceRouter(config)# service-router redirect-mode dns-redirect domain cdsfms.com
```

The following example shows how to display information about the redirect mode by entering the **show service-router redirect-mode** command:

```
ServiceRouter# show service-router redirect-mode
    ip-redirect is enabled
    dns-redirect domain fms.cds.com
    dns-redirect domain cds.com
    dns-redirect domain abc.com
    dns-redirect domain cdsfms.com
```

The following example shows how to subscribe the SR to a domain named test3.com:

```
    ServiceRouter(config)# service-router subscribe domain test3.com
    ServiceRouter(config)#
```

The following example shows how to configure the failed disk threshold to 40 percent:

```
ServiceEngine(config)# service-router service-monitor threshold faildisk 40
U2-205-2(config)#end
U2-205-2#show running-config | include threshold
service-router service-monitor threshold faildisk 40
ServiceEngine#
```

To display the statistics, use the **show statistics service-router summary** command and the **show statistics se** *sename* command. The new output for the DNS-Based Redirection feature is highlighted in boldface type in the examples below. In addition to these two **show** commands, there is also the **show statistics service-router dns** command, which displays the same output as before:

```
ServiceRouter# show statistics service-router summary

----- SR Summary Statistics -----

Requests Received        :                2
  HTTP Requests (normal) :                0
  HTTP Requests (ASX)    :                0
  RTSP Requests          :                0
  RTMP Requests          :                0
  DNS Requests           :                2

Requests Served          :                0
  HTTP Requests Served   :                0

Requests Redirected      :                1
  HTTP 302 Redirects     :                0
  ASX Redirects          :                0
  RTSP redirects         :                0
  RTMP redirects         :                0
  DNS redirects          :                1

Requests Overflowed      :                1
  HTTP 302 Redirects     :                0
  ASX Redirects          :                0
  RTSP redirects         :                0
  RTMP redirects         :                0
  DNS redirects          :                1

Requests Not Redirected  :                0
  No SE Covering Client  :                0
  Unknown Content Origin :                0
  Route Table Locked     :                0

  "Stale SE" Requests    :                0

ServiceRouter# show statistics service-router se temp2

----- Statistics Of SE: temp2 -----
IP Address              : 2.225.2.59
Aliveness               : up
HTTP 302 Redirects      :                  0
ASX Redirects           :                  0
RTSP Redirects          :                  0
RTMP Redirects          :                  0
DNS Redirects           :                  1
Number Of Keepalives    :              85261
```

The following example shows how to enable the Service Monitor transaction logging:

```
ServiceEngine(config)# transaction-logs enable
ServiceEngine(config)# service-router service-monitor transaction-log enable
```

The following example shows how to configure the URL translator:

```
ServiceRouter(config)# service-router last-resort domain cds.com translator 171.XX.XX.XXX
ServiceRouter(config)# service-router last-resort domain cdsis.com translator
171.XX.XX.XXX port 8080
ServiceRouter#
```

The following example shows how to verify the current last resort configuration details:

```
ServiceRouter# show service-router last-resort
Domain cds.com translator 171.XX.XX.XXX
Domain cdsis.com translator 171.XX.XX.XXX port 8080
```

Related Commands

Command	Description
show service-router	Displays the Service Router configuration.

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** command in EXEC configuration mode. You can also use the **setup** command in EXEC configuration mode to complete basic configuration after upgrading.

setup

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

EXEC configuration mode.

Examples

The following example shows the part of the output when you enter the **setup** command in EXEC configuration mode 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 aaa

To display the accounting, authentication, and authorization configuration, use the **show aaa** command in EXEC configuration mode.

show aaa {**commands** [**accounting** | **authorization**] | **enable** [**authentication**] | **exec** [**accounting** | **authorization**] | **login** [**authentication**] | **system** [**accounting** | **authorization**]}

Syntax Description

commands	Configures exec (shell) commands.
accounting	(Optional) Displays the Accounting configuration.
authorization	(Optional) Displays the Authorization configuration.
enable	Configures enable.
authentication	(Optional) Displays Authentication configuration.
exec	Configures starting an exec (shell).
login	Configures the user's login to the system.
system	Configures system events.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 3-15 describes the fields shown in the **show aaa commands** command display.

Table 3-15 show aaa commands Field Descriptions

Field	Description
Configuration commands Authorization	Authorization through Tacacs+ for configuration mode commands is enabled or disabled.
Commands on console Line Authorization	Authorization through TACACS+ for all commands issued from console line is enabled or disabled.
Exec commands Authorization: Normal Users	
Exec commands Authorization: Super Users	
Tacacs+	Authorization through Tacacs+ for exec (shell) commands issued by normal users is enabled or disabled.

Table 3-15 show aaa commands Field Descriptions (continued)

Field	Description
Exec Commands Accounting: Normal Users	
Tacacs+	Authorization through Tacacs+ for exec (shell) commands issued by super users is enabled or disabled.
Exec Commands Accounting: Super Users	
Tacacs+	Accounting through Tacacs+ for exec (shell) commands issued by normal users is enabled or disabled.

Table 3-16 describes the fields shown in the **show aaa enable** command display.

Table 3-16 show aaa enable Field Descriptions

Field	Description
Enable Authentication: All Users	
Enable	Authentication through local configured Enable password for enable is enabled or disabled.
Radius	Authentication through Radius for enable is enabled or disabled.
Tacacs+	Authentication through Tacacs+ for enable is enabled or disabled.

Table 3-17 describes the fields shown in the **show aaa exec** command display.

Table 3-17 show aaa exec Field Descriptions

Field	Description
Starting exec Authorization:	
Local	Authorization through local for starting exec is enabled or disabled.
Radius	Authorization through Radius for starting exec is enabled or disabled.
Tacacs+	Authorization through Tacacs+ for starting exec is enabled or disabled.
Exec events Accounting	
Tacacs+	Accounting through Tacacs+ for exec event is enabled or disabled.

Table 3-18 describes the fields shown in the **show aaa login** command display.

Table 3-18 show aaa login Field Descriptions

Field	Description
Login Authentication	
Local	Authentication through local configured user password for login is enabled or disabled.
Radius	Authentication through Radius for login is enabled or disabled.
Tacacs+	Authentication through Tacacs+ for login is enabled or disabled.

Table 3-19 describes the fields shown in the **show aaa system** command display.

Table 3-19 show aaa system Field Descriptions

Field	Description
System events Accounting	
Tacacs+	Accounting through Tacacs+ for system event is enabled or disabled.

Related Commands

Command	Description
aaa	Configures accounting, authentication and authorization methods.
show aaa	Displays the accounting, authentication and authorization configuration.
show statistics aaa	Displays accounting, authentication and authorization statistics.

show access-lists 300

To display the access control list (ACL) configuration, use the **show access-lists 300** command in EXEC configuration mode.

show access-lists 300

Syntax Description

This command has no arguments or keywords**.**

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 3-20 describes the fields shown in the **show access-lists 300** display.

Table 3-20 show access-lists Field Descriptions

Field	Description
Access Control List is enabled	Configuration status of the access control list.
Groupname and username-based List	Lists the group name-based access control lists.

Related Commands

Command	Description
access-lists	Configures access control list entries.

show acquirer

To display the acquirer information and progress of content acquisition for a specified channel number or name, use the **show acquirer** command in EXEC configuration mode.

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	(Optional) Displays acquirer information for the delivery service.
delivery-service-id	Displays the ID for the delivery service.
delivery_service_id	Delivery service ID.
delivery-service-name	Displays the name for the delivery service.
delivery_service_name	Delivery service name.
progress	(Optional) Displays the acquisition progress for the specified channel.
proxy	(Optional) Displays the proxy information for the acquirer.
authentication	(Optional) Displays the proxy authentication details for the acquirer.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The **show acquirer progress** command displays information for all channels for which the SE is the Content Acquirer. 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** command in Global configuration mode 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** command in Global configuration mode.

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.

The **show acquirer progress** command in EXEC configuration mode 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 3-21 describes the fields shown in the **show acquirer progress** display.

Table 3-21 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 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** command in Global configuration mode:

```
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** command in Global configuration mode:

```
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

Command	Description
acquirer (Global configuration)	Provides authentication when the acquirer obtains content through a proxy server.
http	Configures HTTP-related parameters.
show statistics acquirer	Displays SE acquirer channel statistics.

show alarms

To display information on various types of alarms, their status, and history, use the **show alarms** command in EXEC configuration mode.

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.
start_num	(Optional) Alarm number that appears first in the alarm history (1 to 100).
end_num	(Optional) Alarm number that appears last in the alarm history (1 to 100).
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.

Command Defaults

None

Command Modes

EXEC configuration mode.

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 to prevent a serious fault from occurring.

You can configure alarms using the **snmp-server enable traps alarm** command in Global configuration mode.

Use the **show alarms critical** command in EXEC configuration mode to display the current critical alarms being generated by the Internet Streamer CDS software applications. Use the **show alarms critical detail** command in EXEC configuration mode to display additional details for each of the critical alarms being generated. Use the **show alarms critical detail support** command in EXEC configuration mode 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** command in EXEC configuration modes to display the details of major and minor alarms.

Use the **show alarms history** command in EXEC configuration mode 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** command in EXEC configuration mode to display the status of current alarms and the SE's alarm overload status and alarm overload configuration.

Note The maximum concurrent sessions limit for the Web Engine is based on the CDE; for the CDE220-2M0 and CDE220-2S6 the maximum is 30,000 and for the CDE205 the maximum is 20,000.

Brstcnt Threshold Alarm

When the number of sessions or current bandwidth usage exceeds the configured license limit on the Service Engine, the protocol engine raises an alarm and sends a `threshold exceeded` notification to the Service Router. Any new requests for that protocol engine are not routed to that Service Engine.

Note This feature only applies to the Windows Media Streaming engine, the Flash Media Streaming engine, and the Movie Streamer engine.

Table 3-22 describes the fields shown in the **show alarms history** display.

Table 3-22 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 3-23 describes the fields shown in the **show alarms status** display.

Table 3-23 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.
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

Command	Description
alarm	Configure alarms.
snmp-server enable traps	Enables the SE to send SNMP traps.

show arp

To display the Address Resolution Protocol (ARP) table, use the **show arp** command in EXEC configuration mode.

show arp

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The **show arp** command displays the Internet-to-Ethernet address translation tables of the ARP. Without flags, the current ARP entry for the hostname is displayed.

Table 3-24 describes the fields shown in the **show arp** display.

Table 3-24 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** command in EXEC configuration mode.

show authentication user

Syntax Description

user	Displays the authentication configuration for the user login to the system.

Command Defaults

None

Command Modes

EXEC configuration mode.

Related Commands

Command	Description
aaa	Specifies accounting, authentication and authorization methods.
clear	Clears the HTTP object cache, the hardware interface, statistics, archive working transaction logs, and other settings.

show authsvr

To display the status of the Authorization server, use the **show authsvr** command in EXEC configuration mode.

show authsvr [**unknown-server | location-server**]

Syntax Description

unknown-server	(Optional) Shows the allow and deny rule for unknown configured servers or domains.
location-server	(Optional) Shows the Location server configuration. It includes both primary and secondary geo location server information.

Command Defaults

None

Command Modes

EXEC configuration mode.

Examples

The following example shows how to display the status of the Authorization server:

```
ServiceEngine# show authsvr
Authserver is Enabled
```

The following example shows the status of the Location server:

```
ServiceEngine# show authsvr location-server
        Primary geo location server 4.0.1.3 7000
        Secondary geo location server 171.71.50.140 7000
```

Related Commands

Command	Description
authsvr	Enables and configures the Authorization server.

show bandwidth

To display the bandwidth allocated to a particular device, use the **show bandwidth** command in EXEC configuration mode.

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.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 3-25 describes the fields shown in the **show bandwidth** display.

Table 3-25 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 kbps[1] 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).

Table 3-25 show bandwidth Field Descriptions (continued)

Field	Description
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.

1. kbps = kilobits per second

Related Commands

Command	Description
bandwidth (Global configuration)	Sets an allowable bandwidth usage limit and its duration for Cisco Streaming Engine WMT streaming media.

show banner

To display information on various types of banners, use the **show banner** command in EXEC configuration mode.

show banner

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 3-26 describes the fields shown in the **show banner** display.

Table 3-26 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

Command	Description
banner	Configures the EXEC, login, and message-of-the-day (MOTD) banners.

show bitrate

To display the bit rate allocated to a particular device, use the **show bitrate** command in EXEC configuration mode.

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.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 3-27 describes the fields shown in the **show bitrate** display.

Table 3-27 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

Command	Description
bitrate	Configures the maximum pacing bit rate for large files for the Movie Streamer and separately configures WMT bit-rate settings.

show cache

To display a list of cached contents, use the **show cache** command in EXEC configuration mode.

show cache content *num*

Syntax Description

content	Displays a list of cached contents in order of decreasing priority.
num	(Optional) Number of cached contents to be displayed. The range is from 1 to 1000.

Command Defaults

Number of cached contents is 100.

Command Modes

EXEC configuration mode.

Usage Guidelines

The **show cache** command allows users to check the cached content in an SE.

Use the **show cache content** command to display cache contents, such as priority, size, and URL, and to verify that content has been cached under the correct storage URL. The **show cache content** command also displays the eviction protection information. For relative contents such as WMT and MS, it only displays the parent URL information.

Note When executing the **show cache content** command, the service engine might take sometime if there are prepositioned contents in the **cache**.

Note The **show cache content** command does not display priority (popularity), to see popularity use the **show content-mgr content cache** command or view the Content Manager transaction log entries.

Note When executing the **show cache content url** *url* command on prepositioned content, the output shows as "prepositioned." However, when executing the **show cache content url** *url* command on hybrid content, it shows as "cached" instead of "prepositioned." To correct this, use the **detail** option.

Examples

The following example shows how to display the cached contents:

```
ServiceEngine# show cache content 1000
Max-cached-entries is set as 20000000
Number of cal cached assets: 3913
Eviction protection is disabled.
Cache eviction-preferred-size configured is large
-----------------------------------------------
Size         URL
-----------------------------------------------
200000       http://7.6.200.3/B480-Sep18-TEST1/62/file-0-7372
200000       http://7.6.200.3/B480-Sep18-TEST1/62/file-0-6461
```

```
200000       http://7.6.200.3/B480-Sep18-TEST1/99/file-0-9701
200000       http://7.6.200.3/B480-Sep18-TEST1/99/file-0-4429
200000       http://7.6.200.3/B480-Sep18-TEST1/99/file-0-8867
200000       http://7.6.200.3/B480-Sep18-TEST1/67/file-0-3360
200000       http://7.6.200.3/B480-Sep18-TEST1/927/file-0-4481
200000       http://7.6.200.3/B480-Sep18-TEST1/927/file-0-5002
200000       http://7.6.200.3/B480-Sep18-TEST1/44/file-0-4454
200000       http://7.6.200.3/B480-Sep18-TEST1/105/file-0-4643
200000       http://7.6.200.3/B480-Sep18-TEST1/291/file-0-544
<Output truncated>
```

Related Commands

Command	Description
cache	Configures the cached content maximum entries in the CDS.

show cache-router

To Display cache-router information for various Protocol Engines, use the **show cache-route** command in EXEC configuration mode.

show cache-router {**routes** {**dss-engine** *url* | **fms-engine** *url* | **web-engine** *url* | **wmt-engine** *url* | **upstream-status**}

Syntax Description

routes	Displays the cache-route information for various PEs.
dss-engine	Displays all RTSP protocol-related cache route information.
url	URL string.
fms-engine	Displays all Flash Media-related cache route information.
web-engine	Displays all HTTP protocol-related cache route information.
wmt-engine	Displays all Windows Media-related cache route information.
upstream-status	Displays Liveness information of upstream.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

This command can only be run on an SE to see the route taken by the appropriate Protocol Engine through the CDN (from the current SE where this command is executed) to retrieve the asset for a given URL.

The **sh cache-router routes** command route calculation is agnostic of whether or not the URL is valid.

When a new SE is added to a delivery service, the get_cache_route does not vie the path, the command dumps the cached output and does not perform a liveness query. You must first enter the **show cache router upstream status** command and then the commands in the following example:

Examples

The following examples show the cache route information:

```
ServiceEngine# sh cache-router routes web-engine http://7.25.0.7/index.html
The route: [ 7.25.0.15/7.25.0.13/ ] will be used to cache the asset for
URL=http://7.25.0.7/index.html

ServiceEngine# sh cache-router routes web-engine http://7.25.0.7/index.html
The route: [ 7.25.0.13/ ] will be used to cache the asset for
URL=http://7.25.0.7/index.html

ServiceEngine# sh cache-router routes web-engine http://7.25.0.7/index.html
The route: [ (null) ] will be used to cache the asset for URL=http://7.25.0.7/index.html

ServiceEngine# sh cache-router routes web-engine
               http://ccp-ccp-images.gslb.bdn.lab.xcal.tv/image1
The route: [ 69.241.50.154/69.252.83.150/69.241.118.14/ ] will be used to cache the asset
for URL=http://ccp-ccp-images.gslb.bdn.lab.xcal.tv/image1.
```

show capability

To display the capabilities of the Cap-X profile ID, use the **show capability** command in EXEC configuration mode.

show capability profile ID *profile_id*

Syntax Description

profile ID	Displays information for the Cap-X profile.
profile_id	Profile ID number. The range is from 1 to 65535.

Command Defaults

None

Command Modes

EXEC configuration mode.

Related Commands

Command	Description
capability	Modifies the capability configuration.

show cdn-select

To display the status of the CDN Selector, use the **show cdn-select** command in EXEC configuration mode.

show cdn-select

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

EXEC configuration mode.

Related Commands

Command	Description
cdn-select	Enables the CDN Selector for third-party service selection.
geo-location-server	Redirects requests to different CDNs based on the geographic location of the client.
show statistics cdn-select	Displays the statistics for the CDN Selector.

show cdnfs

To display CDS network file system (CDNFS) information, use the **show cdnfs** command in EXEC configuration mode.

show cdnfs {**usage** | **volumes**}

Syntax Description

usage	Displays Content Delivery Network (CDN) current usage.
volumes	Displays CDSNFS volumes.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

If there are any **clear cache all** commands in progress, the **show cdnfs usage** command displays the progress. If any disks are marked for not creation, then the disk is listed here and the reason is provided.

Table 3-28 describes the fields shown in the **show cdnfs volumes** display.

Table 3-28 show cdnfs volumes Field Descriptions

Field	Description
cdnfs 00–04	CDS network file system and disk number.
nnnnnnKB	Size of the volume in kilobytes.

Table 3-29 describes the fields shown in the **show cdnfs usage** display.

Table 3-29 show cdnfs usage Field Descriptions

Field	Description
Total number of CDNFS entries	Shows the total number of CDNFS entries.
Total space	Shows the total disk space.
Total bytes available	Shows the available disk space.
Total cache size	Shows the total cache size
Total cached entries	Shows the total cache and preposition entries.
Cache-content mgr status	Shows the current status of whether or not the Content Manager is cachable.

Examples

The following example shows how to display the CDNFS usage on an SE:

```
ServiceEngine# show cdnfs usage
Total number of CDNFS entries  :   13437532
Total space                    :     5037.9 GB
Total bytes available          :     2425.6 GB
Total cache size               :     2521.4 GB
Total cached entries           :   13436995
Cache-content mgr status       :        Cacheable
 Units: 1KB = 1024B; 1MB = 1024KB; 1GB = 1024MB
```

The following example shows how to display the CDNFS volumes:

```
ServiceEngine# show cdnfs volumes
cdnfs 00: /disk00-06          444200480KB
cdnfs 01: /disk01-06          444200480KB
cdnfs 02: /disk03-01          488246296KB
cdnfs 03: /disk04-01          488247316KB
cdnfs 04: /disk05-01          488246296KB
cdnfs 05: /disk06-01          488244924KB
cdnfs 06: /disk07-01          488244924KB
cdnfs 07: /disk09-01          488244924KB
cdnfs 08: /disk10-01          488244924KB
cdnfs 09: /disk11-01          488246296KB
cdnfs 10: /disk08-01          488377368KB
```

Related Commands

Command	Description
cdnfs	Manages the Internet Streamer CDS network file system (cdnfs).
disk (EXEC)	Configures disks and allocates disk space for devices that are using the CDS software.
show disks	Displays the names of the disks currently attached to the SE.
show statistics cdnfs	Displays SE CDS network file system (cdnfs) statistics.

show clock

To display the system clock, use the **show clock** command in EXEC configuration mode.

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 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.
timezone	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.
region_name	Name of the region.

Command Defaults

None

Command Modes

EXEC configuration mode.

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 adjusts 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** command in EXEC configuration mode 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.

Table 3-30 describes the field in the **show clock** display.

Table 3-30 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 3-31 describes the fields shown in the **show clock detail** display.

Table 3-31 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** command in EXEC configuration mode. As the following example shows all 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** command in EXEC configuration mode. 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/
Brazil/
CET
.
.
.
```

The following example shows an excerpt of the output from the **show clock standard-timezones zones** command in EXEC configuration mode. 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** command in EXEC configuration mode. 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

Command	Description
clock (EXEC)	Sets or clears clock functions or updates the calendar.
clock (Global configuration	Sets the summer daylight saving time and time zone for display purposes.

show cms

To display the Centralized Management System (CMS)-embedded database content and maintenance status and other information, use the **show cms** command in EXEC configuration mode.

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.
filename	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.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 3-32 describes the fields shown in the CDSM **show cms info** display.

Table 3-32 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_cdsm is running	Status of the cms_cdsm management service (running or not running). This field is specific to the CDSM only.

Table 3-33 describes the fields shown in the SE **show cms info** display.

Table 3-33 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** command in Global configuration mode. 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

Command	Description
cms (EXEC)	Configures the CMS-embedded database parameters.
cms (global)	Schedules maintenance and enables the CMS on a given node.

show content

To display all content entries in the CDS, use the **show content** command in EXEC configuration mode.

show content {**all** [**brief** | **foreground**] | **diskpath** [**brief** | **detail**] | **last-folder-url** [**brief**] | **url** *url* [**brief** | **detail**]}

Syntax Description

all	Displays all cached content into a file.
name	Output file to log cache content query results.
brief	(Optional) Indicates that this brief display mode should be used.
foreground	(Optional) Indicates that this command should be run in the foreground.
diskpath	Displays cached content objects with the original diskpath.
detail	(Optional) Indicates that the detail display mode should be used.
last-folder-url	Displays all content with relative diskpath from the given url without a filename.
url	Displays the cached content object with original URL.
url	The original URL for cache content object query.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

This command allows users to check the cached or prepositioned content in an SE. Through this command, users can view content attributes such as status and file size.

Note For the value of the symlink output field to be correct for the Flash Media Streaming engine, you must configure the play server as HTTP by using the Manifest file.

The **show content all** command scans through the entire disk and transfers the information to the file specified by the user. This command runs in the background unless the foreground option is specified.

The **show content url** command displays cached content and Web Engine metadata attributes, and it helps debug header validation issues. It also displays additional information including start, end time, UNS, and relative content information. If the input URL is parent, then it shows the child disk path. The Authorization field is only applicable for preposition content and this field is moved to the **show content url detail** output.

When executing the **show content url** command with live URL, it displays as preposition content. This is because the object stored on CDNFS is either cache content or preposition content.

Examples

The following command shows how to display cached content and Web Engine attributes for a URL:

```
ServiceEngine# show content url  http://172.XX.XX.XXX/diff.new detail

CAL content object attributes:
        URL: http://we-os.cds.com/vod/pinball.wmv
        Status is 3 (Servable)
        Content is Complete
        File size is 0 Bytes
        Playable by WebEngine WMT
        Linked to
[rtsp://http-we-os.cds.com-s6kmyz359zgyulqfiavhgw/vod/pinball.wmv]
        Content is PREPOSITIONED
        Start Time : Not present
        End Time : Not present
        Internal path to data file
[/disk00-06/p/we-os.cds.com/1d/a1/1da1394af838bbcb45af78fd5681abeb/pinball.w
mv]

Protocol Engine Metadata:
        Authorization is Not Required
        uns_attr_symlink :
http-we-os.cds.com-s6kmyz359zgyulqfiavhgw/vod/pinball.wmv
        UNS_NV_CALC_N_CACHED : PREPOSITIONED
        cdn_uns_id : Rm+7u02g2S8PsuaCfnOKAQ..
        content-type : video/x-ms-wmv
        etag : "9601c7-cc3d0-11016c00"
        file_duration : 25
        ignore_query_string : 1
        last-modified : Wed, 06 Oct 2010 22:12:00 GMT
        server : Apache/2.2.3 (Red Hat)
```

The following example shows how to display 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 shows how to display 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
```

The following example shows how to display cached content objects with the original diskpath.

```
ServiceEngine# show content diskpath
/disk02-01/c/171.71.51.234/66/66/6666cd76f96956469e7be39d750cc7d9/1mbs.wmv.hdr

CAL content object attributes:
        URL: rtsp://171.XX.XX.XXX/1mbs.wmv.hdr
        Status is 3 (Servable)
        Content is Incomplete
        File size is 4096 Bytes
        Playable by WMT
        Authorization is Not Required
        Content is CACHED with priority 0.303707
```

The following example shows how to display all the contents matching to that last-folder-url with the brief option:

```
ServiceEngine# show content last-folder-url http://172.XX.XX.XXX/vod/types brief
Protocol will be ignored with last-folder-url.
-----------------------------------------------------------------
Type URL                                        Size(K)   Status
-----------------------------------------------------------------
C    http://172.XX.XX.XXX/vod/types/sample_s  81        Servable
     orenson.mov
C    http://172.XX.XX.XXX/vod/types/sample_1  912       Servable
     00kbit.mp4
C    http://172.XX.XX.XXX/vod/types/brodeo.m  3745      Servable
     p3
```

The following example shows how to display all the contents matching to that last-folder-url without the brief option:

```
ServiceEngine# show content last-folder-url  http://172.XX.XX.XXX/vod/types
Protocol will be ignored with last-folder-url.

CAL content object attributes:
        URL: http://172.XX.XX.XXX/vod/types/sample_sorenson.mov
        Status is 3 (Servable)
        Content is Complete
        File size is 82395 Bytes
        Playable by WebEngine
        Content is CACHED

CAL content object attributes:
        URL: http://172.XX.XX.XXX/vod/types/sample_100kbit.mp4
        Status is 3 (Servable)
        Content is Complete
        File size is 933456 Bytes
        Playable by WebEngine
        Content is CACHED

CAL content object attributes:
        URL: http://172.XX.XX.XXX/vod/types/brodeo.mp3
        Status is 3 (Servable)
        Content is Complete
        File size is 3834862 Bytes
        Playable by WebEngine
        Content is CACHED
```

show content-mgr

To display all content management information in the CDS, use the **show content-mgr** command in EXEC configuration mode.

show content-mgr {**content** {**all** {**all-disk-volumes output-file** *filename* | **disk-volume output-file** *filename*| **cache** {**all-disk-volumes output-file** *filename* | **disk-volume output-file** *filename* | **prepos** {**all-disk-volumes output-file** *filename* | **disk-volume output-file** *filename}* | **disk-info** | **eviction-list size** *num* {**all-disk-volumes output-file** *filename* | **disk-volume output-file** *filename* | **eviction-protection output-file** *filename* | **health-info**}

Syntax Description

content	Dumps Content Manager objects with priority, url, or disk path.
all	Dumps cached and prepositioned contents.
all-disk-volumes	Dumps all disks.
output-file	Specifies the output filename to write to.
filename	The output file name to write to.
cache	Dump cached contents.
disk-volume	Specifies the disks to be dumped.
prepos	Dump prepositioned contents.
disk-info	Displays disk information.
eviction-list	Dumps the list of contents which is evicted first.
size	Specifies the eviction size (in MB).
eviction-protection	Dumps eviction protection table.
health-info	Displays health information.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The **show content-mgr content all** command dumps all the contents to the specified output file. This process goes through the entire Content Manager data structure to collect file information, and then writes it into the file specified by the user. When the Content Manager begins to dump the records, it states the number of records it prepares to write and how many are actually written in the ~/errorlog/content_manager.current file.

The following example shows a dump with no object being deleted:

```
03/18/2011 23:32:34.945(Local)(9633)LOG :ContentMgr.cpp:968-> Scheduled prepositioned
entries[1] for dump
03/18/2011 23:32:34.945(Local)(9633)LOG :CMgrDumpStore.cpp:75-> Starting dump, entries[1]
03/18/2011 23:32:34.946(Local)(9633)LOG :CMgrDumpStore.cpp:97-> Dump finished.
```

The following example shows a dump with objects being deleted:

```
14:03/18/2011 23:36:20.195(Local)(9633)LOG :ContentMgr.cpp:951-> Scheduled cached
entries[81931] for dump
```

```
14:03/18/2011 23:36:20.195(Local)(9633)LOG :CMgrDumpStore.cpp:75-> Starting dump,
entries[81931]
14:03/18/2011 23:36:23.764(Local)(9633)LOG :CMgrDumpStore.cpp:97-> Dump finished. Entries
removed during dump[41931]. These will not show up in the output file.
```

The **show content-mgr disk-info** command prints disk and asset information for the Content Manager monitors.

Examples

The following example shows how to display all the Content Manager disk information in an output file:

```
ServiceEngine# show content-mgr content all all-disk-volumes output-file dumps
#type-tail dumps
#ContentType Priority URL DiskPath
cached-content 6 http://5.3.3.10/a_1/file_10005542
/disk00-06/c/5.3.3.10/5f/37/5f37c0748805ddf6e58a63853b3677af/file_10005542.http
prepos-content 0 http://172.22.67.108/vod/FootballHD.flv
/disk08-01/p/172.22.67.108/1d/a1/1da1394af838bbcb45af78fd5681abeb/FootballHD.flv
prepos-content 0
://172.22.67.108/manifest-Channel_5683.xml-FNtiIA2L9GVRqiFKzK-h3w
/disk04-01/p/172.22.67.108/66/66/6666cd76f96956469e7be39d750cc7d9/_7279f4d
49c9963f509d8ad2cd772fdf6
prepos-content 0
://http-172.22.67.108-89xld465l9xq3fuq2dgi5w/vod/abc.html
/disk06-01/p/http-172.22.67.108-89xld465l9xq3fuq2dgi5w/1d/a1/1da1394af838bbcb45af7
8fd5681abeb/abc.html
```

The following example shows how to display the Content Manager disk information:

```
ServiceEngine# show content-mgr disk-info
Mount point : /disk00-01
     Bucket Number Assigned to Disk : 0
     File system                    : CDNFS
     Total space                    : 423.6 GB
     Free space                     : 415.1 GB
     Disk Eviction low watermark    : 381.3 GB
     Disk Eviction high watermark   : 394.0 GB
     Writable                       : Yes
     Usable                         : Yes
     Preposition Asset Count        : 0
     Cache Asset Count              : 0
     Preposition Asset Size         : 0 B
     Cache Asset Size               : 0 B
```

The following example shows how to display the Content Manager health information:

```
ServiceEngine# show content-mgr health-info

Deletion Task Count           : 0
Deletion Store Size
     disk00-06                : 0 B
     disk01-06                : 0 B
     disk02-01                : 0 B
Protection Table Size         : 0 B
Snapshot In Progress          : No
Eviction In Progress          : No
Slow scan In Progress         : No
Sanity In Progress            : No
Clear Cache All In Progress   : No
Dump In Progress              : No
Priority Queue Asset Count    : 0
HitCount Decay Half Life (days): 14
Disk Bucket Alarm Threshold(%): 30
```

```
------------------------   Printing All Asset Info   ------------------------

Mount Point                   : disk00-06
Preposition Asset Count       : 4
Cache Asset Count             : 0
Preposition Asset Size        : 104 B
Cache Asset Size              : 0 B

Mount Point                   : disk01-06
Preposition Asset Count       : 8
Cache Asset Count             : 0
Preposition Asset Size        : 312 B
Cache Asset Size              : 0 B

Mount Point                   : disk02-01
Preposition Asset Count       : 2
Cache Asset Count             : 0
Preposition Asset Size        : 52 B
Cache Asset Size              : 0 B

Memory pool statistics   : [      Used][      Free][  Max Used]
Cached File Nodes        : [         0][         0][         0]
Cached Child Nodes       : [         0][         0][         0]
Cached Dir Nodes         : [         1][       818][         1]
Prepos File Nodes        : [        14][    220738][        15]
Prepos Child Nodes       : [        48][    262096][        49]
Prepos Dir Nodes         : [        35][       784][        35]

------------------------   Printing Process Status  ------------------------
CPU Usage Percent             : 0.00
Threads Count                 : 33
Virtual Memory Size           : 189.6 MB
Resident Memory Size          : 33.4 MB

------------------------ Printing Delivery Services ------------------------

Delivery Service Id           : 1450
Origin FQDN                   : 172.22.67.227
Routing Domain Name           : vodplay1.com

Delivery Service Id           : 1272
Origin FQDN                   : 1.2.3.5
Routing Domain Name           : livewmtplay.com

Delivery Service Id           : 1262
Origin FQDN                   : 171.71.51.234
Routing Domain Name           : wmtplay.com

Delivery Service Id           : 1260
Origin FQDN                   : 172.22.67.108
Routing Domain Name           : vodplay.com
```

Related Commands

Command	Description
contentmgr	Configures the Content Manager.
content-mgr disk-info force-reset	Forces the Content Manager to reset the disk share memory information.
show statistics content-mgr	Displays the Content Manager statistics.

show content-origin

To display information about the Network-attached Storage (NAS) mount, use the **show content-origin** command in user EXEC configuration mode.

show content-origin request-fqdn *domain*

Syntax Description

request-fqdn	Configures the request FQDN.
domain	Domain of the request FQDN.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

Table 3-33 describes the fields shown in the **show content-origin** display.

Table 3-34 show content-origin Field Descriptions

Field	Description
FQDN	Fully Qualified Domain Name of the content origin.
Protocol	Protocol used.
SharePoint	SharePoint IP address.
MountPoint	MountPoint type.
Status	Indicates if it succeeded or failed.
MaxRetry	Maximum number of retries allowed.
RetryCount	Actual number of retries.

The following syslog messages are displayed if the NAS mount fails:

```
Cds Origin Manager writes syslog messages when NAS mount fails. Below are some sample
syslog messages:
Apr 28 04:25:26 nas-se CdsOriginMgr: %SE-CdsOriginMgr-3-802100: Failed to mount NFS vod/0
for NAS share 14.1.2.12:/ifs/data
```

Examples

The following example shows how to display the content origin information:

```
ServiceEngine# show content-origin
FQDN: www.cisco.com
      Protocol: CIFS
      SharePoint: 171.XX.XX.X:/wmroot
      MountPoint: WMS
      Status: Success

      Protocol: NFS
      SharePoint: 171.XX.XX.XXX:/usr/local/apache2/htdocs/WMT
```

```
        MountPoint: WMT
        Status: Failed
        MaxRetry: 10
        RetryCount: 17

        Protocol: NFS
        SharePoint: 171.XX.XX.XXX:/usr/local/apache2/htdocs/Zeri
        MountPoint: ZERI
        Status: Failed
        MaxRetry: 10
        RetryCount: 17
ServiceEngine#
```

Related Commands

Command	Description
content-origin	Supports multiple origin servers within a content origin.

show debugging

To display the state of each debugging option, use the **show debugging** user command in user EXEC configuration mode.

show debugging [**ip** {**bgp** | **ospf** | **proximity** | **rib**} | **isis** | **srp** | **svc** {**desci** | **registry**}]

Syntax Description

ip	(Optional) Displays the debug options for IP.
bgp	Displays the debugging flags that have been set for BGP.
ospf	Displays the debug options for OSPF processes that are enabled.
proximity	Displays the debug options that are enabled for the proximity process.
rib	Displays the debug options that are enabled for the rib process.
isis	(Optional) Displays the debug options that are enabled for the IS-IS process.
srp	(Optional) This command displays the debug flags that are turned on for the SRP.
svc	(Optional)
desci	Descriptor Interpreter Library.
registry	Service Registration Daemon.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

The **show debugging ip bgp** command is used to display the debugging flags that have been set for BGP.

The **show debugging ip ospf** command is used to display debug options for OSPF processes that are enabled.

The **show debugging ip rib** command is used to display debug options for rib processes that are enabled.

The **show debugging isis** command is used to display debug options for IS-IS processes that are enabled.

The **show debugging srp** command is used to displays the debug flags that are turned on for the SRP.

Examples

The following is sample output from the **show debugging ip bgp** command:

```
ServiceRouter# debug ip bgp keepalives
ServiceRouter# show debugging ip bgp
BGP keepalives debug is on
ServiceRouter# debug ip bgp all
ServiceRouter# show debugging ip bgp
BGP events debug is on
BGP internal debug is on
BGP RIB debug is on
BGP BRIB debug is on
BGP updates debug is on
```

```
BGP keepalives debug is on
BGP packets debug is on
BGP IO debug is on
BGP list debug is on
BGP dampening debug is on

ServiceRouter#
```

The following is sample output from the **show debugging ip ospf** command:

```
ServiceRouter# show debugging ip ospf

All OSPF debug is on
Adjacency events debug is on
OSPF LSDB changes debug is on
OSPF LSDB timers debug is on
OSPF related events debug is on
LSA flooding debug is on

ServiceRouter#
```

The following is sample output from the **show debugging isis** command.

```
ServiceRouter# show debugging isis

SRP error debug is on
SRP api debug is on
SRP multicast debug is on
SRP session debug is on
SRP srhp packet debug is on
SRP replica debug is on
SRP packet asiii debug is on
SRP function debug is on
SRP replay is on

ServiceRouter#
```

The following example shows the use of **show srp debug** command:

```
ServiceRouter# show debugging srp

SRP packet debug is on
SRP error debug is on
SRP database debug is on
SRP api debug is on
SRP host debug is on
SRP multicast packet debug is on
SRP session debug is on
SRP srhp packet debug is on
SRP replica debug is on
SRP sync debug is on
SRP configuration debug is on
SRP ippc debug is on
SRP packet ascii debug is on
SRP function debug is on

ServiceRouter#
```

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

Command	Description
debug	Monitors and records caching application functions.
undebug	Disables debugging functions.

show debugging srp

To display the debug flags that are turned on for SRP, use the **show debugging srp** command in privileged EXEC mode.

show debugging srp

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Privileged EXEC configuration mode.

Examples

The following example shows the use of **show debugging srp**:

```
ServiceRouter# show debugging srp

SRP packet debug is on
SRP error debug is on
SRP database debug is on
SRP api debug is on
SRP host debug is on
SRP multicast packet debug is on
SRP session debug is on
SRP srhp packet debug is on
SRP replica debug is on
SRP sync debug is on
SRP configuration debug is on
SRP ippc debug is on
SRP packet ascii debug is on
SRP function debug is on

ServiceRouter#
```

show device-mode

To display the configured or current mode of a device, use the **show device-mode** command in EXEC configuration mode.

show device-mode {**configured** | **current**}

Syntax Description

configured	Displays the configured device mode.
current	Displays the current device mode.

Command Defaults

None

Command Modes

EXEC configuration mode.

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 **show device-mode current** command 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
```

```
..

Acmehost# show device-mode configured
Configured device mode: service-router
Acmehost# show device-mode current
Current device mode: service-router
```

Related Commands

Command	Description
device	Configures the mode of operation on a device as a CDSM, SE or SR.

show direct-server-return

To display the Direct Server return information, use the **show direct-server-return** command in EXEC configuration mode.

show direct-server-return

Syntax Description

This command has no keywords or arguments.

Command Defaults

None

Command Modes

EXEC configuration mode.

Examples

The following example shows how to display the Direct Server return information:

```
ServiceEngine# show direct-server-return
direct-server-return vip 11.11.11.11
```

Related Commands

Command	Description
direct-server-return	Enables a VIP for direct server return.

show disks

To view information about your disks, use the **show disks** command in EXEC configuration mode.

show disks [**current** | **details** | **error-handling** [**details**] | **raid-state** | **SMART-info** [**details**]]

Syntax Description

current	(Optional) Displays currently effective configurations.
details	(Optional) Displays currently effective configurations with more details.
error-handling	(Optional) Displays the disk error-handling statistics.
details	(Optional) Displays the detail disk and sector errors.
raid-state	(Optional) Displays 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 SMART disk monitoring info with more details.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The **show disks** command displays the names of the disks currently attached to the SE.

Table 3-35 describes the fields shown in the **show disks details** display.

Table 3-35 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 are not 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.

The **show disks error-handling** command displays the current level of disk and sector-related errors.

Table 3-36 describes the fields shown in the **show disks error-handling details** display.

I/O e

Table 3-36 show disks error-handling details Field Descriptions

Field	Description
Disk errors since last boot	Number of disk errors since the device was last rebooted.
Disk total bad sectors	Total number of bad sector errors.
Total errors	Total number of bad sector and disk errors.
Diskname Sector LBA	Each bad sector's Logical Block Address (LBA).
I/O errors	Number of I/O errors.

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 about the operating and environmental conditions that may indicate an impending disk failure.

To display more detailed information, enter the **show disks SMART-info details** command in EXEC configuration mode. The output from the **show disks SMART-info** and the **show disks SMART-info details** commands 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** command in EXEC configuration mode also includes SMART information.

Table 3-37 describes some typical fields in the **show disks SMART-info** display.

Table 3-37 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.

Table 3-37 show disks SMART-info Field Descriptions (continued)

Field	Description
Temperature Warning Enabled	Temperature warning status: Enabled or Disabled.
SMART Health Status:	Health status of the disk: OK or Failed.

Examples

The following example displays output for two disks experiencing sector errors:

```
ServiceEngine# show disks error-handling
Disk errors since last boot:
disk05 total bad sectors = 1, total errors = 2
disk10 total bad sectors = 3, total errors = 9
```

If the **details** option is given, then each bad sector's Logical Block Address (LBA) displays along with its corresponding I/O error count:

```
ServiceEngine# show disks error-handling details
Disk errors since last boot:
 disk05 total bad sectors = 1, total errors = 2
# diskname  Sector (LBA)      I/O errors:
    disk05  3000005           2

disk10 total bad sectors = 3, total errors = 9
# diskname  Sector (LBA)      I/O errors:
    disk10  16000             3
    disk10  170001            4
    disk10  180001            2

Total errors (since system boot) across all disks = 11
```

Note For additional disk health statistics, execute the **show disks smart-info** or **show alarms** commands.

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** command in EXEC configuration mode 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
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
```

The following example shows the output from the **show dis raid-state** command, which shows all the disk partitions on a CDE:

```
ServiceEngine# #show disks raid-state
SYSTEM : RAID-1
        Status: Normal
        Partitions: disk00/05 disk02/05
SYSTEM: RAID-1
        Status: Normal
        Partitions: disk00/01 disk02/01
SYSTEM: RAID-1
        Status: Normal
        Partitions: disk00/02 disk02/02
SYSTEM: RAID-1
        Status: Normal
        Partitions: disk00/04 disk02/04
```

Related Commands

Command	Description
disk (EXEC)	Configures disks and allocates disk space for devices using CDS software.

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** command in EXEC configuration mode.

show distribution [**delivery-services** {**delivery-service-id** *delivery_service_num* | **delivery-service-name** *delivery_service_name*} | **forwarder-list** {**delivery-service-id** *delivery_service_num* | **delivery-service-name** *delivery_service_name*} | **location** {**forwarder-load-weight** | **live-load-weight** | **location-leader-preference**} {**delivery-service-id** *delivery_service_num* | **delivery-service-name** *delivery_service_name*} | **mcast-data-receiver** {**channels** | **cloud detail**} | **mcast-data-sender** {**channels** | **cloud detail**} | **object-status** *object_url* | **processes** | **remote** *ip_address* {**metadata-sender** {**delivery-service-id** *delivery_service_num* [**start-generation-id** *gen_id* **end-generation-id** *gen_id*] | {**delivery-service-name** *delivery_service_name* [**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*}} | **delivery-service-name** *delivery_service_name* {**cdn-url** *cdn_url* | **probe** | **relative-cdn-url** *cdn_url*}} | **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.
delivery_service_num	Delivery service number (64-bit number).
delivery-service-name	(Optional) Specifies the delivery service name.
delivery_service_name	Delivery service name.
forwarder-list	(Optional) Displays the 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 2-389.
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 2-391.
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 2-390.
mcast-data-receiver	Display Multicast Data Receiver information.
channels	(Optional) Displays the list of channels assigned.
cloud	(Optional) Displays the cloud configuration.
detail	(Optional) Displays detailed cloud configuration.
mcast-data-sender	Displays Multicast Data Sender information.
object-status	(Optional) Displays information on the status of a prepositioned object.

object_url	URL of the prepositioned object.
processes	(Optional) Displays information on distribution processes.
remote	(Optional) Displays delivery service information about a remote SE.
ip_address	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.
gen_id	Beginning database value.
end-generation-id	Specifies the ending database value of the current version of the multicast cloud.
gen_id	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.
cdn_url	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 Content Acquirer in a manner similar to the **traceroute** command.
delivery-service-id	Specifies the delivery service ID with which the unicast sender is associated.
delivery_service_num	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.
maxhop_num	Maximum number of hops. The range is from 1 to 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 Content Acquirer.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Note This command is only available on Cisco Internet Streamer CDS Release 3.1.1.

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 prepositioned 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—Home SE cannot find the forwarder because the home SE has a limit on the forwarder lookup level.
- FAIL—Home SE cannot find the forwarder because there is a failed SE along the path within the specified forwarder lookup level.
- NGWT—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.

Use the **show distribution mcast-data-sender** and **show distribution mcast-data-receiver** commands to see a list of assigned channels and cloud configuration for the Multicast data senders and receivers that were added to the Multicast cloud using the **multicast** command.

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 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 selects 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 are not balanced across the different delivery services. The same SE is 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 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 is 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 Content Acquirer:

```
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
Transfered 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 Authentation     :                       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 ==========

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             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 Origin server failover information for delivery service ID 373:

```
ServiceEngine# show distribution delivery-service delivery-service-name os-failover

Delivery Service Configuration
----------------------
Delivery Service ID                     :                  373
Delivery Service Name                   :          os-failover
Content Origin Name                     :                os-01
Content Origin fqdn                     :          sr.test.com
Content Origin Origin FQDN              :              1.2.3.4
Delivery Service Priority               :                  500
Configured Distribution Type            :         Unicast only

Content Acquirer Information
-------------------
ID of Configured Content Acquirer       :                          193
Name of Configured Content Acquirer     :                        se-01
IP of Configured Content Acquirer       :                   10.20.30.40
ID of Effective Content Acquirer        :                          193
Current content-Acquirer-uid            :                   1359094251
This SE's Role                          :    Configured Content Acquirer
This SE in Full Reload                  :                           No

Content Acquirer Failover/Fallback Information
--------------------------------------
Content Acquirer Failover/Fallback Interval:             120 Mins
```

```
Origin Server Failover Information
--------------------
Origin Server Failover Status           :                           On
Failure Alarm Duration                  :                        5 min
Recovery Alarm Duration                 :                        8 min
Primary   OS(Address/Retry/Timeout)     :          1.2.3.4/  7/  5 sec
Alternate OS(Address/Retry/Timeout)     :          2.3.4.5/  0/  5 sec
Working Server of WebEngine             :                    1.2.3.4

Metadata Information
--------------------
Metadata-Forwarder ID                   :                  0
Metadata-Forwarder Name                 :                N/A
Metadata-Forwarder Primary IP           :                N/A
Metadata-Forwarder NAT IP/Port          :                N/A
Address to Poll Metadata-Forwarder      :                N/A
Metadata-Forwarder Status               :                N/A
Last gen-id Switch                      :    2248695 Secs ago
Current low-water-marker                :                  1
Current max-gen-id                      :                  0
Current max-del-gen-id                  :                  0

Unicast Information
--------------------
Ucast-Forwarder ID                      :                  0
Ucast-Forwarder Name                    :                N/A
Ucast-Forwarder Primary IP              :                N/A
Ucast-Forwarder NAT IP/Port             :                N/A
Address to Poll Ucast-Forwarder         :                N/A
Ucast-Forwarder Status                  :                N/A

QoS Configuration
-----------------
MetaData QoS (effective system config)  :     0 (Not Enabled)
Unicast QoS (system config)             :           0 [0X  0]
Unicast QoS (delivery service config)   :      Not Configured
Effective Unicast QoS config            :           0 [0X  0]


  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 "Working Server of WebEngine" makes sense only on Content Acquirer. It will always keep empty on those Service Engine which are not Content Acquirer.

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

Content Acquirer Information
-------------------
ID of Configured Content Acquirer       :                 462
Name of Configured Content Acquirer     :         Rack89-SE-11
IP of Configured Content Acquirer       :           2.43.27.38
ID of Effective Content Acquirer        :                 462
Current root-ce-uid                     :          1110247321
This SE's Role                          :        Not a Content Acquirer
This SE in Full Reload                  :                  No

Content Acquirer Failover/Fallback Information
---------------------------------------
Content Acquirer Failover/Fallback Interval :             120 Mins

Origin Server Failover Information
--------------------
Origin Server Failover Status           :                           Off

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

  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 Content Acquirer. It is only available on a receiver SE.

The following example provides the forwarder list information for delivery service ID 6290:

```
ServiceEngine# show distribution forwarder-list delivery-service-id 6290 detail
************************** delivery service     6290 ***************************Topology
Information:
  Delivery Service  : (    6290) akot1
  Content Origin    : (    6289) ako
  Home SE           : (    6162) W14-CDE205-1
  Home Location     : (    6189) W14-CDE205-1-location
  Content Acquirer  : (    6181) W14-612-1
  Root Location     : (    6182) W14-612-1-location

======================= Forwarder Result Start ========================
Latest information for unicast Meta-Data reception
               and for unicast Data reception.

USABLE Forwarder:
  SE ID             : (    6181) W14-612-1
  SE Location       : (    6182) W14-612-1-location
  SE IP address     : 114.0.92.11 SE Fowarder Level : 2
  SE attributes     : resides in root location
                      is the Content Acquirer for the Delivery Service
  SE state          : USABLE
                      applies until Thu Jul  8 05:42:43 2010
  Result Status     :
                      Am Location Leader               : Yes

POLLABLE Forwarder:
  None.

-----------------------------------------------------------------------
Location Path:
    List of locations from Home-Location to Root-Location
    Number of locations : 3
        (    6189) W14-CDE205-1-location
        (    6068) L1
        (    6182) W14-612-1-location
    ---------------------------------------------------------------
    List of Delivery-Service-subscribed locations from Home-Location to Root-Location
    Number of locations : 3
        (    6189) W14-CDE205-1-location
        (    6068) L1
```

```
        (    6182) W14-612-1-location
------------------------------------------------------------------------
Forwarder Lists:
Location W14-CDE205-1-location(6189) REACHABLE.

    Showing Forwarder list for
        Location : (    6189) W14-CDE205-1-location
        Number of forwarders in location : 1
        ---------------------------------------
        Configured Forwarder SE List:
          <EMPTY>
        Non-configured Forwarder SE List:
          <EMPTY>
    ------------------------------------------------------------------
Location L1(6068) REACHABLE.

    Showing Forwarder list for
        Location : (    6068) L1
        Number of forwarders in location : 0
        ---------------------------------------
        Configured Forwarder SE List:
          <EMPTY>
        Non-configured Forwarder SE List:
          <EMPTY>
    ------------------------------------------------------------------
Location W14-612-1-location(6182) REACHABLE.

    Showing Forwarder list for
        Location : (    6182) W14-612-1-location
        Number of forwarders in location : 1
        ---------------------------------------
        Configured Forwarder SE List:
          SE ID (    6181) W14-612-1  IP 114.0.92.11  state USABLE (Content Origin)
        Non-configured Forwarder SE List:
          <EMPTY>
```

Related Commands

Command	Description
clear	Clears the HTTP object cache, the hardware interface, statistics, archive working transaction logs, and other settings.
distribution	Reschedules and refreshes content redistribution for a specified delivery service ID or name
show statistics distribution	Displays the statistics of the content distribution components.

show flash

To display the flash memory version and usage information, use the **show flash** command in EXEC configuration mode.

show flash

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

EXEC configuration mode.

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 runs on the device after reload.

Note If you update the CDS software on an SE, the new version displays in the **show flash** command output, but it says, "Pending software change will occur on next bootup." You must reboot the device for the software update to take effect.

Examples

The following example shows how to display 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 3-38 describes the fields shown in the **show flash** display.

Table 3-38 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:	

Table 3-38 show flash Field Descriptions

Field	Description
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.

Related Commands

Command	Description
show version	Displays the version information about the software.

show flash-media-streaming

To display the Flash Media Streaming information, use the **show flash-media-streaming** command in EXEC configuration mode.

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	(Optional) Shows the Flash Media Streaming licenses.
logging	(Optional) Sets the Tar Flash Media Streaming transaction logs to /local/local1/filename.tar.gz.
name	(Optional) Filename.
mtrack	(Optional) Displays the Flash Media Streaming memory usage.
stream-status	(Optional) Displays the Flash Media Streaming stream status.
dvrcast	Displays dvrcast stream status.
all	(Optional) Dumps detail statistics into /local/local1/filename.
live	(Optional) Displays the live stream status.

Command Defaults

None

Command Modes

EXEC configuration mode.

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 shows how to display 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.
ServiceEngine#
```

Related Commands

Command	Description
flash-media-streaming	Enables and configures Flash Media Streaming.
show statistics flash-media-streaming	Displays the statistics for Flash Media Streaming.

show ftp

To display the caching configuration of the File Transfer Protocol (FTP), use the **show ftp** command in EXEC configuration mode.

show ftp

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

EXEC configuration mode.

Examples

The following example shows how to display 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** command in EXEC configuration mode.

show hardware [**all** | **core** | **cpuinfo** | **dmi** [**all** | **baseboard** | **bios** | **cache** | **chassis** | **connector** | **memory** | **processor** | **slot** | **system**] | **mapping** {**disk** [**all** | *diskname*] | **interface** [**all** | **GigabitEthernet** *slot/port_num* | **TenGigabitEthernet** *slot/port_num*]} | **meminfo** | **pci** [**details** | **drivers** | **ids** | **tree**]]

Syntax Description

all	(Optional) Displays all hardware class information.
core	(Optional) Displays core hardware information.
cpuinfo	(Optional) Displays CPU information.
dmi	(Optional) Displays DMI[1].
all	(Optional) Displays all DMI information.
baseboard	(Optional) Displays motherboard information.
bios	(Optional) Displays BIOS information.
cache	(Optional) Displays processor cache information.
chassis	(Optional) Displays chassis information.
connector	(Optional) Displays connector information.
memory	(Optional) Displays physical memory information.
processor	(Optional) Displays processor information.
slot	(Optional) Displays PCI slot information.
system	(Optional) Displays system information.
mapping	(Optional) Shows mapping between Cisco and Linux hardware names.
disk	Maps Cisco disk name to Linux device name.
diskname	Name of the disk (disk00).
interface	Maps Cisco interface name to Linux device name.
all	Displays all interface information.
GigabitEthernet	Selects a 1G ethernet interface.
slot/port_num	Slot and port number for the selected interface. The slot range is from 1 to 14; the port range is from 0 to 0. The slot number and port number are separated with a forward slash character (/).
TenGigabitEthernet	Selects a 10G ethernet interface.
meminfo	(Optional) Displays RAM information.
pci	(Optional) Displays PCI information.
details	(Optional) Show output with PCI addresses and names.
drivers	(Optional) Identify driver names and availability.
ids	(Optional) Show PCI vendor and device codes.
tree	(Optional) Show a tree-like diagram containing all buses, bridges and devices.

1. Desktop Management Interface

Command Defaults None

Command Modes EXEC configuration mode.

Usage Guidelines The output of the **show hardware** command in EXEC configuration mode displays all core or Desktop Management Interface (DMI) information. The DMI output can also be filtered by optional keywords.

Table 3-39 describes the fields shown in the **show hardware** display.

Table 3-39 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.

Table 3-39 show hardware Field Descriptions (continued)

Field	Description
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.
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.
Memory Information	
MemTotal	
MemFree	
Buffers	
Cached	
SwapCached	
Active	
Inactive	
Active(anon)	
Inactive(anon)	
Active(file)	
Inactive(file)	
Unevictable	
Mlocked	
SwapTotal	
SwapFree	
Dirty	
Writeback	
AnonPages	
Mapped	
Shmem	
Slab	
SReclaimable	

Table 3-39 show hardware Field Descriptions (continued)

Field	Description
SUnreclaim	
KernelStack	
PageTables	
NFS_Unstable	
Bounce	
WritebackTmp	
CommitLimit	
Committed_AS	
VmallocTotal	
VmallocUsed	
VmallocChunk	
DirectMap4k	
DirectMap2M	
PCI Information	

Examples

The following example shows how to display the core hardware information:

```
ServiceEngine# show hardware core
Content Delivery System Software (CDS)
Copyright (c) 1999-2011 by Cisco Systems, Inc.
Content Delivery System Software Release 2.6.0 (build
b460 Aug 28 2011)
Version: cde220-2g2-DEVELOPMENT[vcn-build1:/auto/v
cn-u1/cdsis_release_builds/cdsis_2.6.0-b460/spcdn]

Compiled 05:55:01 Aug 28 2011 by ipvbuild
Compile Time Options: KQ SS

System was restarted on Mon Aug 29 11:56:58 2011.
The system has been up for 1 day, 5 hours, 5 minut
es, 2 seconds.

CPU 0 is GenuineIntel Intel(R) Xeon(R) CPU
   L5410  @ 2.33GHz (rev 23) running at 2333MHz.
CPU 1 is GenuineIntel Intel(R) Xeon(R) CPU
   L5410  @ 2.33GHz (rev 23) running at 2333MHz.
CPU 2 is GenuineIntel Intel(R) Xeon(R) CPU
   L5410  @ 2.33GHz (rev 23) running at 2333MHz.
CPU 3 is GenuineIntel Intel(R) Xeon(R) CPU
   L5410  @ 2.33GHz (rev 23) running at 2333MHz.
CPU 4 is GenuineIntel Intel(R) Xeon(R) CPU
   L5410  @ 2.33GHz (rev 23) running at 2333MHz.
CPU 5 is GenuineIntel Intel(R) Xeon(R) CPU
   L5410  @ 2.33GHz (rev 23) running at 2333MHz.
CPU 6 is GenuineIntel Intel(R) Xeon(R) CPU
   L5410  @ 2.33GHz (rev 23) running at 2333MHz.
CPU 7 is GenuineIntel Intel(R) Xeon(R) CPU
   L5410  @ 2.33GHz (rev 23) running at 2333MHz.
```

```
Total 8 CPUs.
16000 Mbytes of Physical memory.
10 GigabitEthernet interfaces
1 Console interface
2 USB interfaces [Not supported in this version of
 software]

  Cookie info:
    Base PID: CDE220-2G2               VID: 00
    SerialNumber: 99999999999
    Model Type:
    SerialNumber (raw): 57 57 57 57 57 57 57 57 57
 57 57
    TestDate: 12-19-2002
    ExtModel: CDE220-2G2
    ModelNum (raw): 55 0 0 0 1
    HWVersion: 1
    PartNumber: 53 54 55 56 57
    BoardRevision: 1
    ChipRev: 1
    VendID: 0
    CookieVer: 2
    Chksum: 0xfb9e

List of all disk drives:
disk00: Normal          (h02 c00 i00 l00 -       m
ptsas)  476940MB(465.8GB)
        disk00/01: SYSTEM         5120MB(  5.0GB)
mounted internally
        disk00/02: SYSTEM         3072MB(  3.0GB)
mounted internally
        disk00/04: SYSTEM         2048MB(  2.0GB)
mounted internally
        disk00/05: SYSFS         32768MB( 32.0GB)
mounted at /local1
        disk00/06: CDNFS        433917MB(423.7GB)
mounted internally
disk01: Normal          (h02 c00 i01 l00 -       m
ptsas)  476940MB(465.8GB)
        disk01/01: SYSTEM         5120MB(  5.0GB)
mounted internally
        disk01/02: SYSTEM         3072MB(  3.0GB)
mounted internally
        disk01/04: SYSTEM         2048MB(  2.0GB)
mounted internally
        disk01/05: SYSFS         32768MB( 32.0GB)
mounted at /local1
<Output truncated>
```

The following example shows how to display the DMI information:

```
ServiceEngine# show hardware dmi
--------------------- DMI Information -------------
# dmidecode 2.9
SMBIOS 2.5 present.
70 structures occupying 2793 bytes.
Table at 0xCFF66000.

Handle 0x0000, DMI type 0, 24 bytes
BIOS Information
        Vendor: Phoenix Technologies LTD
        Version: 1.2a
        Release Date: 04/09/2009
        Address: 0xE3DD0
```

```
        Runtime Size: 115248 bytes
        ROM Size: 2048 kB
        Characteristics:
                PCI is supported
                PNP is supported
                BIOS is upgradeable
                BIOS shadowing is allowed
                ESCD support is available
                Boot from CD is supported
ServiceEngine#
```

Related Commands

Command	Description
show version	Displays version information about the SE software.

show hosts

To view the hosts on your SE, use the **show hosts** command in EXEC configuration mode.

show hosts

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

EXEC configuration mode.

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 3-40 describes the fields shown in the **show hosts** display.

Table 3-40 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 DNS[1] name server or servers.
Host Table	
hostname	FQDN[2] (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** command in Global configuration mode.

1. DNS = Domain Name Server
2. FQDN = fully qualified domain name

show interface

To display the hardware interface information, use the **show interface** command in EXEC configuration mode.

show interface {**all** | **GigabitEthernet** *slot/port* | **PortChannel** {**1** [**lacp**] | **2**} | **standby** *group_num* | **TenGigabitEthernet** *slot/port*}

Syntax Description

all	Displays information for all interfaces.
GigabitEthernet	Displays information for the Gigabit Ethernet device.
slot/port	Slot and port number for the selected interface. The range is from 1 to 14. The slot number and port number are separated with a forward slash character (/).
PortChannel	Displays information for the Ethernet channel of the device.
1	Sets the Ethernet channel interface number to 1.
lacp	(Optional) Displays the LACP port channel status.
2	Sets the Ethernet channel interface number to 2.
standby	Displays information for the standby group for the interface.
group_num	Group number for the selected interface. The group number range is 1 to 4.
TenGigabitEthernet	Displays information for the Ten Gigabit Ethernet device.
slot/port	Slot and port number for the selected interface. The range is from 1 to 14. The slot number and port number are separated with a forward slash character (/).

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 3-41 describes the fields shown in the **show interface GigabitEthernet** display.

Table 3-41 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.

Table 3-41 show interface GigabitEthernet Field Descriptions (continued)

Field	Description
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.
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 3-42 describes the fields shown in the **show interface PortChannel** display.

Table 3-42 show interface PortChannel Field Descriptions

Field	Description
Description	Description of the device, as configured by using the **description** keyword of the **interface** command in Global configuration mode.
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.
IPv6	IPv6 address of the 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.

Table 3-42 show interface PortChannel Field Descriptions (continued)

Field	Description
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.
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.
Interface PortChannel 1 (8 physical interface(s)	
Protocol	Indicates if the LACP is turned on or off.
Mode	Port channel load balancing method (dst-ip, dst-mix-ip-port, dst-port, round-robin, src-dst-ip, src-dst-mac, src-dst-mixed-ip-port, src-dst-port, src-mixed-ip-port, src-port)
Port ID	Interface name.
Admin-State	Interface admin state. This is the interface state that the user configured from the command line. For example, if the user configured “no shut” on the interface, the admin state is up.
Link-State	Interface physical status. Indicates if the link is up or down.
LACP-State	Provides a better detection for the link status through LACP protocol. It tells the upper layer if the physical link is up or down.
Aggregate ID	When LACP is turned on, the interface on the same port channel is grouped into the same aggregate ID.

Table 3-43 describes the fields shown in the **show interface standby** display.

Table 3-43 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** keyword of the **interface** command in Global configuration mode.
IP address, netmask	IP address and netmask of the standby group.

Table 3-43 show interface standby Field Descriptions (continued)

Field	Description
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.

Table 3-44 describes the fields shown in the **show interface TenGigabitEthernet** display.

Table 3-44 show interface TenGigabitEthernet Field Descriptions

Field	Description
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.
IPv6 address	IPv6 address of the 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 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.
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.
Interrupts	Number of interrupts on this interface.
Flags	Interface status indicators. Values include Up, Broadcast, Running, and Multicast.

Related Commands

Command	Description
interface	Configures a Gigabit Ethernet or port channel interface.
lacp	Turns on LACP.
show lacp	Displays LACP information.
show running-config	Displays the current running configuration information on the terminal.
show startup-config	Displays the startup configuration.

show inventory

To display the system inventory information, use the **show inventory** command in EXEC configuration mode.

show inventory

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

EXEC configuration mode.

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 that 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** command in EXEC configuration mode to display the SE's UDI. On older SE models, use the **show tech-support** command in EXEC configuration mode 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 3-45 describes the fields shown in the **show inventory** display.

Table 3-45 show inventory Field Descriptions

Field	Description
PID	Product 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** command in EXEC configuration mode 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

Command	Description
show tech-support	Displays system information necessary for Cisco Technical Support to assist you with your SE.

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** command in EXEC configuration mode.

show ip access-list [*acl_name* | *acl_num*]

Syntax Description

acl_name	(Optional) Information for a specific access list, using an alphanumeric identifier up to 30 characters, beginning with a letter.
acl_num	(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).

Command Defaults

Displays information about all defined access lists.

Command Modes

EXEC configuration mode.

Usage Guidelines

Use the **show ip access-list** command in EXEC configuration mode 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

Command	Description
clear	Clears the HTTP object cache, the hardware interface, statistics, archive working transaction logs, and other settings.
ip access-list	Creates and modifies access lists for controlling access to interfaces or applications.

show ip bgp

To display the contents of a particular host in the BGP routing table, use the **show ip bgp** user command in user EXEC configuration mode.

show ip bgp {*ip_address* | *prefix*/*prefix_length*}

Syntax Description

ip_address	(Optional) IP address entered to filter the output to display only a particular host in the BGP routing table.
prefix	(Optional) Prefix entered to filter the output to display only a particular network in the BGP routing table.
prefix_length	(Optional) Specifies the prefix length.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command requires a Proximity Engine license.

Examples

To display information about an entry in the BGP routing table (for example, 42.1.1.0/24), use the **show ip bgp 42.1.1.0/24** command. To locate information by IP address (for example, 42.1.1.1), use the **show ip bgp 42.1.1.1** command.

```
ServiceRouter# show ip bgp 42.1.1.0/24
BGP routing table entry for 42.1.1.0/24, version 12
Paths: (1 available, best # 1)
Flags: on xmit-list, is in urib, is best urib route

  Path type: internal, path is valid, is best path
  AS-Path: NONE, path sourced internal to AS
    192.168.86.3 (metric 0) from 192.168.86.3 (192.168.86.3)
      Origin incomplete, MED 0, localpref 100, weight 0

  Not advertised to any peer

ServiceRouter# show ip bgp 42.1.1.1

BGP routing table entry for 42.1.1.0/24, version 12
Paths: (1 available, best # 1)
Flags: on xmit-list, is in urib, is best urib route

  Path type: internal, path is valid, is best path
  AS-Path: NONE, path sourced internal to AS
    192.168.86.3 (metric 0) from 192.168.86.3 (192.168.86.3)
      Origin incomplete, MED 0, localpref 100, weight 0

Not advertised to any peer
```

```
ServiceRouter#
```

The following sample output shows the display when the advertised community and the configured location community matches:

```
ServiceRouter# sh ip bgp 1.1.1.1
BGP routing table entry for 1.1.1.1/32, version 4
Paths: (1 available, best # 1)
Flags: on xmit-list, is in urib, is best urib route

Path type: internal, path is valid, is best path
  AS-Path: NONE, path sourced internal to AS
    48.0.0.8 (metric 0) from 48.0.0.8 (1.1.1.1)
      Origin IGP, MED 0, localpref 100, weight 0
      Community: 1:1(location specific)
```

The following sample output shows the display when the community is not advertised to any peer:

```
ServiceRouter# sh ip bgp 33.1.5.0

BGP routing table entry for 33.1.5.0/24, version 4
Paths: (1 available, best #1)
Flags: on xmit-list, is in urib, is best urib route

  Path type: internal, path is valid, is best path
  AS-Path: 2 , path sourced external to AS
    62.0.0.2 (metric 20) from 26.0.0.6 (10.1.1.1)
      Origin IGP, MED 0, localpref 100, weight 0
      Community: 5:5(location specific)
```

Related Commands

Command	Description
clear ip bgp	Clears entries in the BGP route table.
router bgp	Configures a BGP routing process.

show ip bgp all

To display the contents of the BGP routing table, use the **show ip bgp** user command in user EXEC configuration mode.

show ip bgp {*ip_address* | *prefix*/*prefix_length* | **all**}

Syntax Description

ip_address	(Optional) IP address entered to filter the output to display only a particular host in the BGP routing table.
prefix	(Optional) Prefix entered to filter the output to display only a particular network in the BGP routing table.
prefix_length	(Optional) Specifies the prefix length.
all	(Optional) Displays all BGP routes received by the Proximity Engine.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command requires a Proximity Engine license.

Examples

The following example is sample output from the **show ip bgp** command. The output shows the contents of the BGP routing table:

```
ServiceRouter# show ip bgp all

BGP table version is 810399, local router ID is 172.20.168.47
Status: s-suppressed, x-deleted, S-stale, d-dampened, h-history,*-valid, >-best
Path type: i-internal, e-external, c-confed, l-local, a-aggregate, r-redist
Origin codes: I - IGP, E - EGP, ? - incomplete

   Network            Next Hop            Metric     LocPrf   Weight Path
   *>i5.5.5.5/32         192.168.86.3             20         100    0 ?
   *>i12.1.1.1/32        192.168.86.3             20         100    0 ?
   *>i13.1.1.1/32        192.168.86.3             20         100    0 ?
   *>i14.1.1.1/32        192.168.86.3             20         100    0 ?
   *>i22.22.22.22/32     192.168.86.3             20         100    0 ?
   *>i40.1.1.0/24        192.168.86.3              0         100    0 ?
   *>i41.1.1.0/24        192.168.86.3              0         100    0 ?
   *>i42.1.1.0/24        192.168.86.3              0         100    0 ?
   *>i43.1.1.0/24        192.168.86.3              0         100    0 ?
*>i45.1.1.0/24         192.168.86.3             0         100    0 ?
-- More --
```

Related Commands

Command	Description
clear ip bgp all	Clears all BGP neighbors.
router bgp	Configures a BGP routing process.

show ip bgp community

To display BGP routes that match a specified BGP community string, use the **show ip bgp community** user EXEC command.

show ip bgp community *community_string*

Syntax Description

community_string	Community string for which to display BGP routes.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

The **show ip bgp community** command is used to display BGP route information for a specified community string. To determine whether a community string exists in the BGP table, use the **show ip bgp summary** command. This command requires a Proximity Engine license.

The **show ip bgp community** command displays the origin AS and community values. Since the community list may be long, the output is limited to 80 columns. Other community unrelated fields longer display in this command; use the **show ip bgp all** command to display these fields.

Examples

In the following example, **show ip bgp summary** output can be used to determine that a community string 100:50 exists in the BGP table. The **show ip bgp community** command displays BGP route information for the community string 100:50. In this example, no route information is present for the community string 100:50:

```
ServiceRouter# show ip bgp summary
BGP router identifier 1.100.8.92, local AS number 23
BGP table version is 2, IPv4 Unicast config peers 2, capable peers 0
0 network entries and 0 paths using 0 bytes of memory
BGP attribute entries [ 0/0 ] , BGP AS path entries [ 0/0 ]
BGP community entries [ 0/0 ] , BGP clusterlist entries [ 0/0 ]
BGP Location Communities: 100:50-100:100

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd

192.168.82.1    4    23       0       0        0    0    0    4d10h Idle
192.168.82.10   4   100       0       0        0    0    0    4d10h Idle

ServiceRouter# show ip bgp community 100:50

BGP table version is 2, local router ID is 1.100.8.92
Status: s-suppressed, x-deleted, S-stale, d-dampened, h-history, *-valid, >-best

Path type: i-internal, e-external, c-confed, l-local, a-aggregate, r-redist
Origin codes: I - IGP, E - EGP, ? - incomplete

   Network            Next Hop            Metric     LocPrf     Weight Path
ServiceRouter#
```

The following example shows the output for the **show ip bgp community** command:

```
ServiceRouter# show ip bgp community
sh ip bgp community
BGP table version is 32, local router ID is 1.100.9.206
Status: s-suppressed, x-deleted, S-stale, d-dampened, h-history, *-valid, >-best
Path type: i-internal, e-external, c-confed, l-local, a-aggregate, r-redist
Community: @ - source, # - target

   Network            Next Hop        Origin AS  Community List
*>e2.4.1.0/24         192.168.82.2    33
*>e3.1.4.0/24         192.168.82.2    23         @23:999
*>e5.5.5.5/32         192.168.82.2    23         @23:999
*>e12.1.1.0/24        192.168.82.1    23
*>e12.1.1.1/32        192.168.82.2    23         @23:100 @#44:100
*>e13.1.1.0/24        192.168.82.1    23
*>e13.1.1.1/32        192.168.82.2    23         @#44:100
*>e14.1.1.1/32        192.168.82.2    23         @#44:100
*>e40.1.1.0/24        192.168.82.2    23         @23:999
*>e41.1.1.0/24        192.168.82.2    23         @23:999
*>e42.1.1.0/24        192.168.82.2    33
*>e43.1.1.0/24        192.168.82.2    33
*>e44.1.1.0/24        192.168.82.2    33
*>e45.1.1.0/24        192.168.82.2    33
*>e46.1.1.0/24        192.168.82.2    33
*>e50.1.1.0/24        192.168.82.2    23         @23:999
*>e51.1.1.0/24        192.168.82.2    23         @23:999
*>e52.1.1.0/24        192.168.82.2    33
*>e53.1.1.0/24        192.168.82.2    33
*>e54.1.1.0/24        192.168.82.2    33
*>e55.1.1.0/24        192.168.82.2    33
*>e62.1.1.1/32        192.168.82.2    23         @23:999
*>e62.62.62.0/24      192.168.82.2    23         @23:999
*>e108.0.32.0/24      192.168.82.2    33
*>e171.70.0.0/16      192.168.82.2    33
*>e171.71.0.0/16      192.168.82.2    33
*>e172.20.0.0/16      192.168.82.2    33
*>e192.168.81.0/24    192.168.82.2    23
*>e203.0.0.205/32     192.168.82.2    23         @23:999
ServiceRouter#
```

Related Commands

Command	Description
location community	BGP location-specific community configuration.
router bgp	Configures a BGP routing process.

show ip bgp ipv4 unicast

To display information relating to all IPv4 unicast routes in the BGP routing table, use the **show ip bgp ipv4 unicast** user command in user EXEC configuration mode.

show ip bgp ipv4 unicast

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

The **show ip bgp ipv4 unicast** command is used to display information relating to all IPv4 unicast routes in the BGP routing table. To see any route in the output of this command, BGP needs to connect successfully to at least one neighbor and receive route information from this neighbor. This command requires a Proximity Engine license.

Examples

The following is sample output from the **show ip bgp ipv4 unicast** command:

```
ServiceRouter# show ip bgp ipv4 unicast

BGP table version is 810674, local router ID is 172.20.168.47
Status: s-suppressed, x-deleted, S-stale, d-dampened, h-history, *-valid, >-best

Path type: i-internal, e-external, c-confed, l-local, a-aggregate, r-redist
Origin codes: I - IGP, E - EGP, ? - incomplete

   Network            Next Hop            Metric     LocPrf     Weight Path
*>i5.5.5.5/32         192.168.86.3             20        100          0 ?
*>i12.1.1.1/32        192.168.86.3             20        100          0 ?
*>i13.1.1.1/32        192.168.86.3             20        100          0 ?
*>i14.1.1.1/32        192.168.86.3             20        100          0 ?
*>i22.22.22.22/32     192.168.86.3             20        100          0 ?
*>i40.1.1.0/24        192.168.86.3              0        100          0 ?
*>i41.1.1.0/24        192.168.86.3              0        100          0 ?
*>i42.1.1.0/24        192.168.86.3              0        100          0 ?
*>i43.1.1.0/24        192.168.86.3              0        100          0 ?
*>i44.1.1.0/24        192.168.86.3              0        100          0 ?
*>i45.1.1.0/24        192.168.86.3              0        100          0 ?
*>i50.1.1.0/24        192.168.86.3              0        100          0 ?
*>i51.1.1.0/24        192.168.86.3              0        100          0 ?
-- More --
```

Related Commands

Command	Description
clear ip bgp all	Clears all BGP neighbors.
router bgp	Configures a BGP routing process.

show ip bgp memory

To display memory usage information of the running BGP daemon, use the **show ip bgp memory** user command in user EXEC configuration mode.

show ip bgp memory

Syntax Description

This command has no keywords or arguments.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command requires a Proximity Engine license.

Examples

The following example is sample output from the **show ip bgp memory** command:

```
ServiceRouter# show ip bgp memory

Shared memory information for /topos_shm_bgp,
Current-Size         HWM    Maximum-Size
      1727064     1727088       209715200


BGP memory usage stats

Private memory
Total mallocs/frees/failed : 31/9/0
Memory allocated           : 4258692 bytes
HWM allocated              : 4262700 bytes

Shared memory
Total mallocs/frees/failed : 19/3/0
Memory requested/allocated : 1534799/1727064 bytes
HWM requested/allocated    : 1534819/1727088 bytes

ServiceRouter#
```

Related Commands

Command	Description
router bgp	Configures a BGP routing process.

show ip bgp neighbors

To display information about the TCP and BGP connections to neighbors, use the s**how ip bgp neighbors** user command in user EXEC configuration mode.

show ip bgp neighbors [*ip_address*]

Syntax Description

ip_address	(Optional) IP address of a neighbor.

Command Defaults

The output of this command displays information for all neighbors for IPv4 address family sessions only.

Command Modes

User EXEC configuration mode.

Usage Guidelines

The **show ip bgp neighbors** command is used to display BGP and TCP connection information for neighbor sessions. For BGP, this includes detailed neighbor attribute, capability, path, and prefix information. For TCP, this includes statistics related to BGP neighbor session establishment and maintenance.

This command requires a Proximity Engine license.

Examples

The following example is sample output from the **show ip bgp neighbors** command. The example shows the 192.168.86.3 neighbor. This neighbor is an internal BGP (iBGP) peer. This neighbor supports the route refresh and graceful restart capabilities.

```
ServiceRouter# show ip bgp neighbors
BGP neighbor is 48.0.0.8, remote AS 2, ebgp link, Peer index 1
BGP version 4, remote router ID 48.0.0.8
BGP state = Established, up for 00:00:04
Peer is directly attached, interface GigabitEthernet 2/0
Last read 0.027030, hold time = 180, keepalive interval is 60 seconds
Last written 00:00:01, keepalive timer expiry due 00:00:58
Received 14265 messages, 0 notifications, 0 bytes in queue
Sent 5 messages, 0 notifications, 0 bytes in queue
Connections established 1; dropped 0
Last reset by us never, due to process restart
Last reset by peer never, due to process restart

Neighbor capabilities:
Dynamic capability: advertised (mp, refresh, gr)
Dynamic capability (old): advertised
Address family IPv4 Unicast: advertised

Capabilities parameter not sent by neighbor
Exchanging IPv4 Unicast NLRI by default

For address family: IPv4 Unicast
BGP table version 1, neighbor version 101573
142640 accepted paths consume 5135040 bytes of memory
0 sent paths

Local host: 48.0.0.4, Local port: 179
```

```
Foreign host: 48.0.0.8, Foreign port: 2867
fd = 42

ServiceRouter#
```

To display information for all BGP neighbors, use the **show ip bgp neighbors** command. In this example, the Proximity Engine has two BGP peers, 192.168.86.3 and 192.168.86.87.

```
ServiceRouter# show ip bgp neighbors

BGP neighbor is 192.168.86.3,  remote AS 23, ibgp link,  Peer index 1
  BGP version 4, remote router ID 192.168.86.3
  BGP state = Established, up for 1d05h
  Peer is directly attached, interface GigabitEthernet 2/0
  Last read 0.868226, hold time = 180, keepalive interval is 60 seconds
  Last written 00:00:09, keepalive timer expiry due 00:00:50
  Received 78444 messages, 0 notifications, 0 bytes in queue
  Sent 1788 messages, 0 notifications, 0 bytes in queue
  Connections established 1; dropped 0
  Last reset by us never, due to process restart
  Last reset by peer never, due to process restart

  Neighbor capabilities:
  Dynamic capability: advertised (mp, refresh, gr)
  Dynamic capability (old): advertised
  Route refresh capability (new): advertised received
  Route refresh capability (old): advertised received
  Address family IPv4 Unicast: advertised received

  For address family: IPv4 Unicast
  BGP table version 1, neighbor version 810749
  8518 accepted paths consume 613296 bytes of memory
  0 sent paths

  Local host: 192.168.86.47, Local port: 58920
  Foreign host: 192.168.86.3, Foreign port: 179
  fd = 35

BGP neighbor is 192.168.86.87,  remote AS 23, ibgp link,  Peer index 2
  BGP version 4, remote router ID 0.0.0.0
  BGP state = Idle, down for 00:00:10
  Last read never, hold time = 180, keepalive interval is 60 seconds
  Last written never, keepalive timer not running
  Received 0 messages, 0 notifications, 0 bytes in queue
  Sent 0 messages, 0 notifications, 0 bytes in queue
  Connections established 0; dropped 0
  Last reset by us never, due to process restart
  Last reset by peer never, due to process restart

  For address family: IPv4 Unicast
  BGP table version 1, neighbor version 0
  0 accepted paths consume 0 bytes of memory
  0 sent paths

No established BGP session with peer
```

Related Commands

Command	Description
clear ip bgp all	Clears all BGP neighbors.
router bgp	Configures a BGP routing process.

show ip bgp nexthop-database

To display the next-hop database information in the BGP routing table, use the **show ip bgp nexthop-database** user command in user EXEC configuration mode.

show ip bgp nexthop-database

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

The **show ip bgp nexthop-database** command is used to display the BGP next-hop information, including IGP cost, IGP route type, IGP preference, interface to reach this next-hop, time of last next-hop resolution, and reachability. This command requires a Proximity Engine license.

Examples

The following example is sample output from the **show ip bgp nexthop-database** command:

```
ServiceRouter# show ip bgp nexthop-database

Nexthop: 192.168.86.3, Refcount: 4021, IGP cost: 0
IGP Route type: 0, IGP preference: 0
Attached nexthop: 192.168.86.3, Interface: GigabitEthernet 2/0
Nexthop is attached not-local reachable
Nexthop last resolved: 1d05h, using 192.168.86.0/24
Metric next advertise: Never

ServiceRouter#
```

Related Commands

Command	Description
router bgp	Configures a BGP routing process.
show ip bgp all	Displays BGP route table information.

show ip bgp summary

To display the status of all BGP connections, use the **show ip bgp summary** user command in user EXEC configuration mode.

show ip bgp summary

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

The **show ip bgp summary** command is used to display BGP path, prefix, and attribute information for all connections to BGP neighbors.

A *path* is a route to a given destination. By default, BGP only installs a single path for each destination. If multipath routes are configured, BGP installs a path for each multipath route, and only one multipath route is marked as the best path. A prefix is an IP address and network mask. It can represent an entire network, a subset of a network, or a single host route.

BGP attribute and cache entries are displayed individually and in combinations that affect the best path selection process. The fields for this output are displayed when the related BGP feature is configured or when the BGP attribute is received. Memory usage is displayed in bytes.

This command requires a Proximity Engine license.

Examples

The following example is sample output from the **show ip bgp summary** command:

```
ServiceRouter# show ip bgp summary

BGP router identifier 1.100.8.40, local AS number 65204
BGP table version is 567, IPv4 Unicast config peers 1, capable peers 1
80 network entries and 80 paths using 16960 bytes of memory
BGP attribute entries [ 10/1600 ] , BGP AS path entries [ 10/174 ]
BGP community entries [ 10/160 ] , BGP clusterlist entries [ 0/0 ]
location community 100:1535 200:4566 123:3000-123:4000 350:2530 300:500-300:1000

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.52.10   4 65204    4363    4289      567    0    0 00:00:59 80

ServiceRouter#
```

Related Commands

Command	Description
router bgp	Configures a BGP routing process.
show ip bgp all	Displays BGP route table information.

show ip interface

To display the IP interface state and address/mask for all interfaces, use the **show ip interface** command in user EXEC configuration mode.

show ip interface

Syntax Description

brief	Displays a summary of the IP interface status and configuration.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command is used to display a Summary of the IP interface status and configuration.

Examples

The following example is sample output from the **show ip bgp summary** command:

```
ServiceRouter# show ip interface brief

Interface            IP Address      Interface Status
PortChannel 1        3.1.14.71       protocol-up/link-up/admin-up
PortChannel 2        4.0.8.12        protocol-up/link-up/admin-up

ServiceRouter#
```

show ip ospf

To display general information about OSPF routing processes, use the **show ip ospf** command in privileged EXEC configuration mode.

show ip ospf

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

Privileged EXEC configuration mode.

Usage Guidelines

This command requires a Proximity Engine license.

Examples

The following is sample output from the **show ip ospf** command:

```
ServiceRouter# show ip ospf

OSPF information:
 Routing Process p1 with ID 172.20.168.41 context default
 Stateful High Availability enabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Reference Bandwidth is 40000 Mbps
 Initial Inter-SPF schedule delay 200.000 msecs,
   backoff factor 2, capped at 1000.000 msecs,
   minimum Inter-SPF delay reset after 5000.000 msecs
 Minimum hold time for Router LSA throttle 5000.000 ms
 Minimum hold time for Network LSA throttle 5000.000 ms
 Minimum LSA arrival 1000.000 msec
 Maximum paths to destination 8
 Originating router LSA with maximum metric
   Condition: Always
 Number of external LSAs 22, checksum sum 0xdc4ba
 Number of opaque AS LSA 0, checksum sum 0
 Number of areas is 1, 1 normal, 0 stub, 0 nssa
 Number of active areas is 1, 1 normal, 0 stub, 0 nssa
   Area BACKBONE(0)
        Area has existed for 00:00:02
        Interfaces in this area: 1 Active interfaces: 1
        No authentication available
        SPF calculation has run 2 times
         Last SPF ran for 0.000054s
        Router LSA throttle timer due in 00:00:02
        Area ranges are
        Number of LSAs: 498, checksum sum 0xf5eb6b

ServiceRouter#
```

Table 3-46 describes the significant fields included in the display above.

Table 3-46 Significant fields included in output of show ip ospf command

Field	Description
Routing Process p1 with ID 172.20.168.41	Process ID p1 and OSPF router ID 172.20.168.41 (IP address of Proximity Engine). For Proximity Engine, p1 cannot be changed.
Supports …	Number of types of service supported (Type 0 only).
Summary Link update interval	Specifies summary update interval in hours:minutes:seconds, and time until next update.
External Link update interval	Specifies external update interval in hours:minutes:seconds, and time until next update.
Redistributing External Routes from	Lists of redistributed routes, by protocol.
Number of areas	Number of areas in router, area addresses, and so on.
Link State Update Interval.	Specifies router and network link-state update interval in hours:minutes:seconds, and time until next update.
Link State Age Interval	Specifies max-aged update deletion interval, and time until next database cleanup, in hours:minutes:seconds.
SPF Calculation	Number of times SPF calculation is done.

Related Commands

Command	Description
router ospf	Enables the OSPF routing process.

show ip ospf border-routers

To display general information about OSPF border routers, use the **show ip ospf border-routers** command in privileged EXEC configuration mode.

show ip ospf border-routers

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

Privileged EXEC configuration mode.

Usage Guidelines

This command requires a Proximity Engine license.

Examples

The following is sample output from the **show ip ospf** command:

```
ServiceRouter# show ip ospf border-routers
OSPF Process ID p1 context default, Internal Routing Table
Codes: i - Intra-area route, I - Inter-area route

intra 192.168.0.86 [65535], ASBR, Area 0, SPF 3
     via 192.168.86.3, GigabitEthernet 2/0
```

Related Commands

Command	Description
router ospf	Enables the OSPF routing process.

show ip ospf database

To display lists of information related to the OSPF database for a specific router, use the **show ip ospf database** user command in EXEC configuration mode. The various forms of this command deliver information about different OSPF link-state advertisements (LSAs).

show ip ospf database [**adv-router** [*ip_address*]] [**detail**] | [**asbr-summary**] [*link_state_id*] [**detail**] | [**database-summary**] | [**detail**] | [**external**] [*link_state_id*] [**detail**] | [**network**] [*link_state_id*] [**detail**] | [**nssa-external**] [*link_state_id*] [**detail**] | [**router**] [*link_state_id*] [**detail**] | [**self-originate**] [**detail**] | [**summary**] [*link_state_id*] [**detail**]

Syntax Description

adv-router [*ip_address*]	(Optional) Displays all the link-state advertisements (LSAs) of the specified router. If no IP address is included, the information displayed relates to the local router (in this case, the same as the **self-originate** keyword).
asbr-summary	(Optional) Displays information about only the Autonomous System Boundary Router (ASBR) summary LSAs.
link_state_id	(Optional) Portion of the Internet environment that is being described by the advertisement. The value entered depends on the type of the LSA. The value must be entered in the form of an IP address. When the LSA is describing a network, the *link_state_id* argument can take one of two forms: • Network IP address (as in Type 3 summary link advertisements and in autonomous system external link advertisements). • Derived address obtained from the link-state ID. (Note that masking a network links the advertisement link-state ID with the network subnet mask yielding the network IP address.) When the LSA is describing a router, the link-state ID is always the OSPF router ID of the described router. When an autonomous system external advertisement (Type 5) is describing a default route, its link-state ID is set to the default destination (0.0.0.0).
database-summary	(Optional) Displays how many of each type of LSA for each area there are in the database, and displays the total.
detail	(Optional) Displays LSA in detail.
external	(Optional) Displays information only about the external LSAs.
network	(Optional) Displays information only about the network LSAs.
nssa-external	(Optional) Displays information only about the Not-So-Stubby Area (NSSA) external LSAs.
router	(Optional) Displays information only about the router LSAs.
self-originate	(Optional) Displays only self-originated LSAs (from the local router).
summary	(Optional) Displays information only about the summary LSAs.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

This command requires a Proximity Engine license.

Examples

The following is sample output from the **show ip ospf database** command when no arguments or keywords are used:

```
ServiceRouter# show ip ospf database
    OSPF Router with ID (172.20.168.88) (Process ID p1 context default)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#     Checksum Link Count
172.20.168.88   172.20.168.88   1686        0x80000006 0x4531   1
192.168.0.4     192.168.0.4     1284        0x8000000a 0x80cf   1

                Network Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
192.168.20.2    192.168.0.4     1284        0x80000003 0x49d2

ServiceRouter#
```

Table 3-47 describes the significant fields included in the display above.

Table 3-47 Significant fields included in output of show ip ospf database

Field	Description
Link ID	Router ID number.
ADV Router	Advertising router ID.
Age	Link-state age.
Seq#	Link-state sequence number (detects old or duplicate LSAs).
Checksum	Fletcher checksum of the complete contents of the LSA
Link count	Number of interfaces detected for router.

The following is sample output from the **show ip ospf database** command with the **asbr-summary** keyword:

```
ServiceRouter# show ip ospf database asbr-summary
    OSPF Router with ID (172.20.168.41) (Process ID p1 context default)

                Summary ASBR Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
193.0.50.3      193.0.50.3      1281        0x800007a8 0x86d4
193.0.150.3     193.0.150.3     1281        0x800007ac 0x6f1f

                Summary ASBR Link States (Area 10)

Link ID         ADV Router      Age         Seq#       Checksum
193.0.50.3      172.20.168.41   345         0x8000002a 0x0a95
193.0.150.3     172.20.168.41   345         0x8000002a 0xb981

ServiceRouter#
```

Table 3-48 describes the significant fields included in the display above.

Table 3-48 Significant fields included in output of show ip ospf database asbr-summary

Field	Description
Link ID	Router ID number.
ADV Router	Advertising router ID.
Age	Link-state age.
Seq#	Link-state sequence number (detects old or duplicate LSAs).
Checksum	Fletcher checksum of the complete contents of the LSA.

The following is sample output from the **show ip ospf database** command with the **external** keyword:

```
ServiceRouter# show ip ospf database external

        OSPF Router with ID (172.20.168.41) (Process ID p1 context default)

                Type-5 AS External Link States

Link ID         ADV Router      Age         Seq#       Checksum Tag
30.0.0.0        193.0.50.3      1580        0x800007ab 0x7e24    0
30.0.0.0        193.0.150.3     1580        0x800007ae 0xb981    0
30.0.1.0        193.0.50.3      1580        0x800007ab 0x732e    0
30.0.1.0        193.0.150.3     1580        0x800007ae 0xae8b    0
30.0.2.0        193.0.50.3      1580        0x800007ab 0x6838    0
30.0.2.0        193.0.150.3     1580        0x800007ae 0xa395    0
30.0.3.0        193.0.50.3      1580        0x800007ab 0x5d42    0
30.0.3.0        193.0.150.3     1580        0x800007ae 0x989f    0

ServiceRouter#
```

Table 3-49 describes the significant fields included in the display above.

Table 3-49 Significant fields included in output of show ip ospf database external

Field	Description
Link ID	Router ID number.
ADV Router	Advertising router ID.
Age	Link-state age.
Seq#	Link-state sequence number (detects old or duplicate LSAs).
Checksum	Fletcher checksum of the complete contents of the LSA.
Tag	External route tag, a 32-bit field attached to each external route. This is not used by the OSPF protocol itself.

The following is sample output from the **show ip ospf database** command with the **network** keyword:

```
ServiceRouter# show ip ospf database network

    OSPF Router with ID (172.20.168.41) (Process ID p1 context default)

                Network Link States (Area 0)
```

```
Link ID         ADV Router      Age         Seq#       Checksum
192.168.78.4    100.73.1.4      312         0x80000135 0xeaeb
192.168.82.4    100.73.1.4      1311        0x8000009b 0xbc01
193.0.50.2      193.0.50.3      57          0x800007ad 0x7cec
193.0.61.2      193.0.61.3      57          0x80000fe4 0x0d5e
193.0.72.2      193.0.72.3      57          0x80000fe4 0x3906
193.0.83.2      193.0.83.3      57          0x800007a9 0xf362
193.0.84.2      193.0.83.3      57          0x800007a9 0xc9a1

ServiceRouter#
```

Table 3-50 describes the significant fields included in the display above.

Table 3-50 Significant fields included in output of show ip ospf database network

Field	Description
Link ID	Router ID number.
ADV Router	Advertising router ID.
Age	Link-state age.
Seq#	Link-state sequence number (detects old or duplicate LSAs).
Checksum	Fletcher checksum of the complete contents of the LSA.

The following is sample output from the **show ip ospf database** command with the **router** keyword:

```
ServiceRouter# show ip ospf database router

        OSPF Router with ID (172.20.168.41) (Process ID p1 context default)

                Router Link States (Area 0)

Link ID         ADV Router      Age      Seq#       Checksum Link Count
1.1.78.8        1.1.78.8        525      0x800007af 0x801b   2
1.1.78.9        1.1.78.9        525      0x800007ab 0x7ce8   2
100.73.1.4      100.73.1.4      780      0x800003bd 0x2dd9   2
172.20.168.41   172.20.168.41   1388     0x80000030 0x67fa   1
172.20.168.83   172.20.168.83   1179     0x80000039 0xfddd   1
192.168.82.1    192.168.82.1    1299     0x8000006f 0x06fe   2

                Router Link States (Area 10)

Link ID         ADV Router      Age      Seq#       Checksum Link Count
172.20.168.41   172.20.168.41   628      0x8000002c 0xf99d   1

ServiceRouter#
```

Table 3-51 describes the significant fields included in the display above.

Table 3-51 Significant fields included in output of show ip ospf database router

Field	Description
Link ID	Router ID number.
ADV Router	Advertising router ID.
Age	Link-state age.
Seq#	Link-state sequence number (detects old or duplicate LSAs).

Table 3-51 Significant fields included in output of show ip ospf database router (continued)

Field	Description
Checksum	Fletcher checksum of the complete contents of the LSA.
Link count	Number of interfaces detected for router.

The following is sample output from the **show ip ospf database** command with the **summary** keyword:

```
ServiceRouter# show ip ospf database summary

        OSPF Router with ID (172.20.168.41) (Process ID p1 context default)

                Summary Network Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
20.0.0.0        193.0.50.3      1325        0x800007ac 0xa496
20.0.0.0        193.0.150.3     1326        0x800007af 0xdff3
20.0.1.0        193.0.50.3      1325        0x800007ac 0x99a0
20.0.1.0        193.0.150.3     1326        0x800007af 0xd4fd
20.0.2.0        193.0.50.3      1325        0x800007ac 0x8eaa
20.0.2.0        193.0.150.3     1326        0x800007af 0xc908

                Summary Network Link States (Area 10)

Link ID         ADV Router      Age         Seq#       Checksum
192.168.78.0    172.20.168.41   370         0x8000002b 0xc127

ServiceRouter#
```

Table 3-52 describes the significant fields included in the display above.

Table 3-52 Significant fields included in output of show ip ospf database summary

Field	Description
Link ID	Router ID number.
ADV Router	Advertising router ID.
Age	Link-state age.
Seq#	Link-state sequence number (detects old or duplicate LSAs).
Checksum	Fletcher checksum of the complete contents of the LSA.

The following is sample output from the **show ip ospf database** command with the **database-summary** keyword:

```
ServiceRouter# show ip ospf database database-summary

    OSPF Router with ID (172.20.168.41) (Process ID p1 context default)

Area 0 database summary
  LSA Type            Count
  Opaque Link         0
  Router              156
  Network             296
  Summary Network     41
  Summary ASBR        2
  Type-7 AS External  0
  Opaque Area         0
```

```
  Subtotal            495

Area 10 database summary
  LSA Type            Count
  Opaque Link         0
  Router              1
  Network             0
  Summary Network     1
  Summary ASBR        2
  Type-7 AS External  0
  Opaque Area         0
  Subtotal            4

Process p1 database summary
  LSA Type            Count
  Opaque Link         0
  Router              157
  Network             296
  Summary Network     42
  Summary ASBR        4
  Type-7 AS External  0
  Opaque Area         0
  Type-5 AS External  20
  Opaque AS           0
  Total               519

ServiceRouter#
```

Table 3-53 describes the significant fields included in the display above.

Table 3-53 Significant fields included in output of show ip ospf database database-summary command

Field	Description
OSPF Router with id	Router ID number.
Process ID	OSPF process ID (for Proximity Engine, the id is p1)
LSA Type	Link-state type.
Area ID	Area number
Router	Number of router LSAs in that area
Network	Number of network LSAs in that area
Summary Network	Number of summary LSAs in that area
Summary ASBR	Number of summary ASBR LSAs in that area
Subtotal	Sum of Router, Network, Summary Network, and Summary ASBR for that area
AS External	Number of external LSAs.

Related Commands

Command	Description
router ospf	Enables the OSPF routing process.

show ip ospf interface

To display OSPF-related interface information, use the show **ip ospf interface** command in user EXEC configuration mode.

show ip ospf interface

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command requires a Proximity Engine license.

Examples

The following example shows how to display sample output from the **show ip ospf interface** command.

```
ServiceRouter# show ip ospf interface

Interface:  GigabitEthernet 1/0 is up, line protocol is up
    IP address 192.168.78.41/24, Process ID p1 context default, area 0
    State BDR, Network type BROADCAST, cost 1
    Index 1, Transmit delay 1 sec, Router Priority 1
    Designated Router ID: 100.73.1.4, address: 192.168.78.4
    Backup Designated Router ID: 172.20.168.41, address: 192.168.78.41
    4 Neighbors, flooding to 2, adjacent with 2
    Timer intervals: Hello 10, Dead 40, Wait 40, Retransmit 5
      Hello timer due in 00:00:01
    No authentication
    Number of link LSAs: 0, checksum sum 0
 GigabitEthernet 1/0 is up, line protocol is up
    IP address 172.20.168.41/24, Process ID p1 context default, area 10
    State DR, Network type BROADCAST, cost 1
    Index 2, Transmit delay 1 sec, Router Priority 1
    Designated Router ID: 172.20.168.41, address: 172.20.168.41
    No backup designated router on this network
    0 Neighbors, flooding to 0, adjacent with 0
    Timer intervals: Hello 10, Dead 40, Wait 40, Retransmit 5
      Hello timer due in 00:00:07
    No authentication
    Number of link LSAs: 0, checksum sum 0

ServiceRouter#
```

Table 3-54 describes the significant fields included in the display above.

Table 3-54 Significant fields included in output of the show ip ospf interface command

Field	Description
Interface	Status of physical link and operational status of the protocol.
IP address	Interface IP address, subnet mask, and area number/address.
State	Interface state (DR – Designated Router, BDR – Backup Designated Router).
Timer intervals configured	Configuration of timer intervals.
Transmit delay	Transmit delay, router priority.
Hello	Number of seconds until next hello packet is sent out this interface.
Neighbor Count	Count of network neighbors and list of adjacent neighbors.

Related Commands

Command	Description
router ospf	Enables the OSPF routing process.

show ip ospf memory

To display memory usage of the OSPF process, use the **show ip ospf memory** command in user EXEC configuration mode.

show ip ospf memory

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command requires a Proximity Engine license.

Examples

The following example shows how to display sample output from the **show ip ospf memory** command.

```
ServiceRouter# show ip ospf memory

OSPF memory usage statistics:

Shared memory information for /topos_shm_ospf,
Current-Size         HWM    Maximum-Size
          48     1088240         4194304


 OSPF Process ID p1, Memory statistics
  Byte usage:    needed 0, overhead 0, using 0 bytes
  Allocations:   current 0, created 0, failed 0, free 0
  Bitfields:     current 0, created 0, failed 0, free 0, using 0 bytes
  Slabs:         current 0, created 0, failed 0, free 0, using 8 bytes
  Index failure: Interface 0, Neighbor 0

  CurBytes  Current      HWM   Malloc     Free   Description
       728        1        1        1        0   area
    119712      516      520      526       10   lsdb entry
       320        2        2        2        0   ASBR route
       984        1        1        1        0   ospf interface
        16        1        1        1        0   backup safety memory
     48136      515      520     9465     8950   lsa
        60        1        2        2        1   lsa
         0        0      197      517      517   lsa
         0        0        2        2        2   redist work
   1048576        1        1        1        0   backup memory
      4192        1        1        1        0   ospf subrouter
      2920        1        1        1        0   ager wheel
     10100       11       11       13        2   pak buffer
        80        1        1        1        0   ospf table
        48        1        1        1        0   ager wheel holder
      2784        3        3        3        0   neighbor
        24        1        1        1        0   network configuration entry
```

Related Commands

Command	Description
router ospf	Enables the OSPF routing process.

show ip ospf neighbor

To display OSPF neighbor information, use the **show ip ospf neighbor** command in user EXEC configuration mode.

show ip ospf neighbor [*neighbor_id* | **detail** | **summary**]

Syntax Description

neighbor_id	(Optional) Neighbor ID or Router ID.
detail	(Optional) Displays details of neighbors.
summary	(Optional) Displays a summary of neighbors.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command requires a Proximity Engine license.

Examples

The following is sample output from the **show ip ospf neighbor** command. It shows a single line of summary information for each neighbor:

```
ServiceRouter# show ip ospf neighbors

 OSPF Process ID p1 context default
 Total number of neighbors: 2
 Neighbor ID     Pri State            Up Time  Address         Interface
 100.73.1.4        1 FULL/DR          1d00h    192.168.78.4     GigabitEthernet 1/0
 172.20.168.83     1 FULL/DROTHER     14:42:44 192.168.78.83    GigabitEthernet 1/0

ServiceRouter#
```

The following is sample output showing summary information about the neighbor that matches the specified neighbor ID:

```
ServiceRouter# show ip ospf neighbors 100.73.1.4

 OSPF Process ID p1 context default
 Total number of neighbors: 4
 Neighbor ID     Pri State            Up Time  Address         Interface
 100.73.1.4        1 FULL/DR          1d00h    192.168.78.4     GigabitEthernet 1/0

ServiceRouter#
```

The following is sample output from the **show ip ospf neighbor detail** command:

```
ServiceRouter# show ip ospf neighbors detail

Neighbor 100.73.1.4, interface address 192.168.78.4
    Process ID p1 context default, in area 0 via interface GigabitEthernet 1/0
    State is FULL, 6 state changes, last change 1d00h
    Neighbor priority is 1
```

```
    DR is 192.168.78.4 BDR is 192.168.78.41
    Hello options 0x12, dbd options 0x52
    Last non-hello packet received 0.301737
      Dead timer due in 00:00:40
 Neighbor 172.20.168.83, interface address 192.168.78.83
    Process ID p1 context default, in area 0 via interface GigabitEthernet 1/0
    State is FULL, 4 state changes, last change 14:47:09
    Neighbor priority is 1
    DR is 192.168.78.4 BDR is 192.168.78.41
    Hello options 0x2, dbd options 0x42
    Last non-hello packet received 00:00:08
      Dead timer due in 00:00:34
ServiceRouter#
```

The following is sample output from the **show ip ospf neighbor summary** command:

```
ServiceRouter# show ip ospf neighbors summary

 OSPF Process ID p1 context default, Neighbor Summary
 Interface Down Attempt Init TwoWay ExStart Exchange Loading Full Total
     Total    0       0    0      0       0        0       0    2     2
      GigabitEthernet 1/0    0       0    0      0       0        0       0    2     2

ServiceRouter#
```

Table 3-55 describes the significant fields included in the display above.

Table 3-55 Significant fields included in output of the* show ip ospf neighbor summary *Command

Field	Description
Neighbor	Neighbor router ID.
interface address	IP address of the interface.
in area	Area and interface through which the OSPF neighbor is known.
Neighbor priority	Router priority.
State	OSPF state.
state changes	Number of state changes since the neighbor was created. This value can be reset using the **clear ip ospf neighbor** command.
DR is	Router ID of the designated router for the interface.
BDR is	Router ID of the backup designated router for the interface.
Hello option	Hello packet options field contents (E-bit only).
Dead timer	Expected time before Proximity Engine declares the neighbor dead.
UP Time	Number of hours:minutes:seconds since the neighbor went into 2-way state.
Last non-hello packet	Number of hours:minutes:seconds since the last non-hello packet received

Related Commands

Command	Description
router ospf	Enables the OSPF routing process.

show ip ospf request-list

To display a list of all link-state advertisements (LSAs) requested by a router, use the **show ip ospf request-list** command in EXEC configuration mode.

show ip ospf request-list *neighbor interface*

Syntax Description

neighbor	Neighbor router ID.
interface	Interface name.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The output is useful in debugging OSPF routing operations. This command requires a Proximity Engine license.

Examples

The following example shows how to display sample output from the **show ip ospf request-list** command, with neighbor router ID set to 100.73.1.4, and interface set to 'GigabitEthernet 1/0':

```
ServiceRouter# show ip ospf request-list 100.73.1.4 GigabitEthernet 1/0

 OSPF Process ID p1 context default
 Neighbor 100.73.1.4, interface GigabitEthernet 1/0, address 192.168.78.4
 1 LSAs on request-list

 Type LSID            Adv Rtr         Seq No     Checksum Age
    1 192.168.1.12    192.168.1.12    0x8000020D 0x6572   5

ServiceRouter#
```

Related Commands

Command	Description
router ospf	Enables the OSPF routing process.

show ip ospf retransmission-list

To display a list of all link-state advertisements (LSAs) waiting to be re-sent, use the **show ip ospf retransmission-list** command in EXEC configuration mode.

show ip ospf retransmission-list *neighbor interface*

Syntax Description

neighbor	Neighbor router ID.
interface	Interface name.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

The output of this command is useful in debugging OSPF routing operations. This command requires a Proximity Engine license.

Examples

The following example shows how to display sample output from the **show ip ospf retransmission-list** command, with neighbor router ID set to '100.73.1.4', and interface set to 'GigabitEthernet 1/0':

```
ServiceRouter# show ip ospf retransmission-list 100.73.1.4 GigabitEthernet 1/0

 OSPF Process ID p1 context default
 Neighbor 100.73.1.4, interface GigabitEthernet 1/0, address 192.168.78.4

 Link state retransmission due in 00:00:04
 Type LSID            Adv Rtr         Seq No     Checksum Age
    1 172.20.168.41   172.20.168.41   0x80000044 0x3f0f   0

ServiceRouter#
```

Related Commands

Command	Description
router ospf	Enables the OSPF routing process.

show ip ospf route

To display the OSPF RSPF route for OSPF routes, use the **show ip ospf route** command in EXEC configuration mode.

show ip ospf route [**all** | *router_id*]

Syntax Description

all	(Optional) Displays for all OSPF routes.
router_id	(Optional) Displays for this router ID

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command requires a Proximity Engine license.

Examples

The following is sample output from the **show ip ospf route** command:

```
ServiceRouter# show ip ospf route

 OSPF Process ID p1 context default, Routing Table
  (D) denotes route is directly attached      (R) denotes route is in RIB
20.0.0.0/24 (inter) area 0
     via 192.168.78.8/GigabitEthernet 1/0, cost 65645
     via 192.168.78.9/GigabitEthernet 1/0, cost 65645
20.0.1.0/24 (inter) area 0
     via 192.168.78.8/GigabitEthernet 1/0, cost 65645
     via 192.168.78.9/GigabitEthernet 1/0, cost 65645
20.0.2.0/24 (inter) area 0
     via 192.168.78.8/GigabitEthernet 1/0, cost 65645
     via 192.168.78.9/GigabitEthernet 1/0, cost 65645
20.0.3.0/24 (inter) area 0
     via 192.168.78.8/GigabitEthernet 1/0, cost 65645
     via 192.168.78.9/GigabitEthernet 1/0, cost 65645
20.0.4.0/24 (inter) area 0
     via 192.168.78.8/GigabitEthernet 1/0, cost 65645
     via 192.168.78.9/GigabitEthernet 1/0, cost 65645
20.0.5.0/24 (inter) area 0
     via 192.168.78.8/GigabitEthernet 1/0, cost 65645
     via 192.168.78.9/GigabitEthernet 1/0, cost 65645
20.0.6.0/24 (inter) area 0
     via 192.168.78.8/GigabitEthernet 1/0, cost 65645
     via 192.168.78.9/GigabitEthernet 1/0, cost 65645
192.168.78.0/24 (intra)(D) area 0
     via 192.168.78.41/GigabitEthernet 1/0*, cost 65535
192.168.79.0/24 (intra) area 0
     via 192.168.78.4/GigabitEthernet 1/0, cost 65537
192.168.82.0/24 (intra) area 0
     via 192.168.78.4/GigabitEthernet 1/0, cost 65536
```

Related Commands

Command	Description
router ospf	Enables the OSPF routing process.

show ip ospf rspf route

To display OSPF reverse shortest path first (RSPF) from a specific router(s), use the s**how ip ospf rspf route** command in EXEC configuration mode.

show ip ospf rspf route [*router_id*]

Syntax Description

router_id	(Optional) Router ID.

Command Defaults

If no router ID is specified, displays OSPF RSPF information for all router IDs.

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command shows cached RSPF routing information because of previous proximity request. This command requires a Proximity Engine license.

Examples

The following is sample output from the **show ip ospf rspf route** command:

```
ServiceRouter# show ip ospf rspf route

Advertising Router  SPF Version  Cache Hit       Age
172.20.168.41          2292         1        00:00:04

ServiceRouter#
```

Table 3-56 describes the significant fields included in the display above

Table 3-56 Significant fields included in output of the show ip ospf rspf router command

Field	Description
Advertising Router	Rspf is computed based on this router.
SPF version	SPF version.
Cache Hit	Same proximity request received (Cache hit + 1) times before has been cache expired.
Age	Age of cached result.

The following example shows the spf cost of each route from router 172.20.168.41:

```
ServiceRouter# show ip ospf rspf route 172.20.168.41

OSPF Process ID p1 context default, Routing Table
  (D) denotes route is directly attached    (R) denotes route is in RIB
192.168.78.0/24 area 0, spf cost 0
192.168.79.0/24 area 0, spf cost 3
192.168.82.0/24 area 0, spf cost 1
193.0.50.0/24 area 0, spf cost 10
193.0.51.0/24 area 0, spf cost 30
```

```
193.0.52.0/24 area 0, spf cost 30
193.0.53.0/24 area 0, spf cost 30
193.0.54.0/24 area 0, spf cost 30
193.0.55.0/24 area 0, spf cost 30
193.0.56.0/24 area 0, spf cost 30
193.0.57.0/24 area 0, spf cost 30
193.0.58.0/24 area 0, spf cost 30
193.0.59.0/24 area 0, spf cost 30
193.0.60.0/24 area 0, spf cost 30

ServiceRouter#
```

Related Commands

Command	Description
router ospf	Enables the OSPF routing process.

show ip ospf traffic

To display OSPF traffic statistics, use the **show ip ospf traffic** command in user EXEC configuration mode.

show ip ospf traffic

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command requires a Proximity Engine license.

Examples

The following is sample output from the **show ip ospf traffic** command:

```
ServiceRouter# show ip ospf traffic

Packet Counter:
 OSPF Process ID p1 context default, Packet Counters (cleared 00:04:33 ago)
  Total: 324 in, 160 out
  LSU transmissions: first 1, rxmit 0, for req 0
  Flooding packets output throttled (IP/tokens): 0 (0/0)
  Ignored LSAs: 0, LSAs dropped during SPF: 0
  LSAs dropped during graceful restart: 0
  Errors: drops in        0, drops out       0, errors in       0,
          errors out      0, hellos in       0, dbds in         0,
          lsreq in        0, lsu in          0, lsacks in       0,
          unknown in      0, unknown out     0, no ospf         0,
          bad version     0, bad crc         0, dup rid         0,
          dup src         0, invalid src     0, invalid dst     0,
          no nbr          0, passive         0, wrong area      0,
          pkt length      0, nbr changed rid/ip addr            0
          bad auth        0

           hellos       dbds     lsreqs       lsus       acks
   In:         84          0          0        118        122
  Out:         31        101          0          1         27

ServiceRouter#
```

Table 3-57 describes the significant fields included in the display above.

Table 3-57 Significant fields included in output of the show ip ospf traffic

Field	Description
Packet Counter	When packet counter last cleared.
Total	Total number of packets in and out from OSPF process.

Table 3-57 Significant fields included in output of the show ip ospf traffic (continued)

Field	Description
Errors	Number of packets have error and dropped because of different reasons.
In	Total count (after last **clear ip ospf traffic**) of the different types of OSPF packets that OSPF process received.
Out	Total count (after last **clear ip ospf traffic**) of the different types of OSPF packets that OSPF process sent.

Related Commands

Command	Description
router ospf	Enables the OSPF routing process.

show ip proximity algorithm

To display the proximity algorithm options currently in use by this Proximity Engine, use the **show ip proximity algorithm** command in user EXEC configuration mode.

show ip proximity algorithm

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

When BGP is configured as the routing protocol, the output from **show ip proximity algorithm** has information on the following:

- Whether the community-based proximity option (location-community) is enabled
- Whether the proximity redirect option is enabled
- Whether the BGP best-path (AS hops) based proximity option is enabled

These threes options are enabled with the **proximity algorithm bgp** command. For information on these options, see the proximity algorithm bgp command.

Examples

The following example shows sample output from the **show ip proximity algorithm** command.

```
ServiceRouter> show ip proximity algorithm

Proximity algorithm: bgp community

ServiceRouter#
```

Related Commands

Command	Description
proximity algorithm bgp	Enables a BGP proximity algorithm option for the Proximity Engine.
proximity engine enable	Enables the Proximity Engine.

show ip proximity servers

To display the interface addresses and hostnames of the Proximity Servers currently in use by this Proximity Engine, use the **show ip proximity servers** command in user EXEC configuration mode.

show ip proximity servers

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command shows other proximity servers and their interface addresses for use in redirection. The DHT ring must be enabled between these proximity servers using the **router srp** command for the DHT ring to be formed. These servers are used for redirection only if the **proximity algorithm bgp redirect** command is enabled.

Examples

The following example shows sample output from the **show ip proximity servers** command.

```
ServiceRouter# show ip proximity servers
Proximity servers:
Hostname: Hostname not found
IP0: 3.1.4.14
IP1: 192.168.82.10
Hostname: Hostname not found
IP0: 3.1.4.12
IP1: 192.168.82.199
Hostname: SN-CDSM
IP0: 192.168.86.77
IP1: 1.100.8.190
ServiceRouter#
```

Related Commands

Command	Description
router srp	Enters SRP configuration mode.
proximity algorithm bgp redirect	Specifies the BGP AS-based redirection on the Proximity Engine.
proximity engine enable	Enables the Proximity Engine.

show ip rib clients

To display details of all the routing protocol instances that are clients of the RIB, use the **show ip rib clients** command in user EXEC configuration mode.

show ip rib clients

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command is used to display detailed information about all routing protocol instances that have registered with RIB.

Examples

The following example shows sample output from the **show ip rib clients** command. The output shows three routing protocol instances that have registered with RIB, along with the results of various counters in RIB.

```
ServiceRouter# show ip rib clients

Displaying information for all clients:CLIENT: direct
 epid: 352       MTS SAP: -1        MRU cache hits/misses:        3/1
 Routing Instances:
  route context "default" table "default"
 Messages received:
  Register          : 1      Add-one-route     : 3      Denotify-request  : 1
 Messages sent:

CLIENT: isis-abc
 epid: 19498     MTS SAP: 1666      MRU cache hits/misses:  1137375/1
 Routing Instances:
  route context “default” table “default”
 Messages received:
  Register          : 1      Add-route         : 52647  Delete-route      : 48872
  Notify-request    : 1
 Messages sent:
  Add-route-ack     : 52647  Delete-route-ack  : 48872

CLIENT: isis-abc-te
 epid: 19498     MTS SAP: 1666      MRU cache hits/misses:        0/0
 Messages received:
  Register          : 1
 Messages sent:
```

Related Commands

Command	Description
proximity engine enable	Enables the Proximity Engine.

show ip rib memory

To display the memory usage information of the RIB, use the **show ip rib memory** command in user EXEC configuration mode.

show ip rib memory

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command is used to display detailed information about the memory usage of the RIB (for example, shared memory information and memory used by routes).

Examples

The following example shows sample output from the **show ip rib memory** command:

```
ServiceRouter# show ip rib memory
Shared memory information for /topos_shm_urib,
Current-Size         HWM    Maximum-Size
     3897168     3897168       131072000
allocated:7   alloc errs:0

URIB slab block statistics:
                  alloc fail   cumm alloc   cumm freed   high-water
urib routes                0            5            0            5
urib nibs                  0            1            0            1
urib rte nibs              0          330          325            5
urib tib nibs              0            1            0            1
urib next hops             0          330          325            5
urib chlst elms            0            5            0            5
urib nhlfes                0            0            0            0
crib nodes                 0            0            0            0
crib routes                0            0            0            0
crib uroutes               0            0            0            0
crib next hops             0            0            0            0

URIB slab statistics:
                   allocated   cumm alloc   cumm freed   high-water
urib routes             8538         8538            0         8538
urib nibs                  2            2            0            2
urib rte nibs           8515       550792       542277         8538
urib tib nibs              2            2            0            2
urib next hops          8515       550792       542277         8538
urib chlst elms         8538         8538            0         8538
urib nhlfes                0            0            0            0
crib nodes                 0            0            0            0
crib routes                0            0            0            0
crib uroutes               0            0            0            0
crib next hops             0            0            0            0
```

Related Commands

Command	Description
proximity engine enable	Enables the Proximity Engine.

show ip rib recursive-next-hop

To display IP recursive next-hop information from the RIB, use the **show ip rib recursive-next-hop** command in user EXEC configuration mode.

show ip rib ip recursive-next-hop [*ip_addr*]

Syntax Description

ip_addr	IP address for which recursive next-hop information is displayed.

Command Defaults

In no *ip_addr* argument is specified, **show ip rib recursive-next-hop** displays information for all recursive next-hops for this Proximity Engine.

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command is used to display IP recursive next-hop information from the RIB.

Examples

The following example shows sample output from the **show ip rib recursive-next-hop** command.

```
ServiceRouter# show ip rib recursive-next-hop

IP Recursive Next-Hop Table

192.168.79.3/32, uptime: 3d22h, bgp-301
192.168.82.1/32, uptime: 3d22h, bgp-301

ServiceRouter> show ip rib recursive-next-hop 192.168.82.1

IP Recursive Next-Hop Table

192.168.82.1/32, uptime: 3d22h, bgp-301

ServiceRouter#
```

In the output, bgp-301 is the number of the BGP Autonomous System containing the recursive next hop.

Related Commands

Command	Description
proximity engine enable	Enables the Proximity Engine.

show ip rib route

To display IP RIB route information, use the **show ip rib route** command in user EXEC configuration mode.

show ip rib route [*ip_address* | **bgp** | **direct** | **isis** | **ospf** | **static** | **summary**]

Syntax Description

ip_address	(Optional) Specifies an IP address for the RIB route.
bgp	(Optional) Specifies the BGP route.
direct	(Optional) Specifies a direct/connected route.
isis	(Optional) Specifies an ISO IS-IS route.
ospf	(Optional) Specifies an OSPF route.
static	(Optional) Specifies static routes.
summary	(Optional) Displays route counts.

Command Defaults

In no *ip_address* argument is specified, **show ip rib route** displays information for all routes for this Proximity Engine.

Command Modes

User EXEC configuration mode.

Examples

The following example shows sample output from the **show ip rib route** command:

```
ServiceRouter# show ip rib route
IP Urib Route Table:
     '*' denotes best ucast next-hop     '**' denotes best mcast next-hop
' [ x/y ] ' denotes [ preference/metric ]

1.1.1.1/32, 1 ucast next-hops, 0 mcast next-hops
    *via 203.0.0.1, GigabitEthernet 2/0, [ 115/20 ] , 04:34:54, isis-p1, L2 2.2.2.2/32, 1
ucast next-hops, 0 mcast next-hops
    *via 203.0.0.1, GigabitEthernet 2/0, [ 115/30 ] , 04:34:54, isis-p1, L2 2.8.1.0/24, 1
ucast next-hops, 0 mcast next-hops, attached
    *via 2.8.1.8, GigabitEthernet 1/0, [ 0/0 ] , 04:35:13, direct 12.0.0.0/8, 1 ucast
next-hops, 0 mcast next-hops
    *via 203.0.0.1, GigabitEthernet 2/0, [ 115/20 ] , 04:34:54, isis-p1, L2 20.0.0.0/16, 1
ucast next-hops, 0 mcast next-hops
    *via 203.0.0.1, GigabitEthernet 2/0, [ 200/0 ] , 04:34:53, bgp-209, internal, tag 209
       extended route information: AS Hops 0, BGP peer AS 209 101.0.0.0/8, 1 ucast
next-hops, 0 mcast next-hops
    *via 203.0.0.1, GigabitEthernet 2/0, [ 200/0 ] , 04:35:03, bgp-209, internal, tag
65209
       extended route information: AS Hops 1, BGP peer AS 209 102.0.0.0/8, 1 ucast
next-hops, 0 mcast next-hops
    *via 203.0.0.1, GigabitEthernet 2/0, [ 200/0 ] , 04:34:53, bgp-209, internal, tag
65209
       extended route information: AS Hops 1, BGP peer AS 209 103.0.0.0/8, 1 ucast
next-hops, 0 mcast next-hops
    *via 203.0.0.1, GigabitEthernet 2/0, [ 200/0 ] , 04:34:53, bgp-209, internal, tag
65209
```

```
       extended route information: AS Hops 1, BGP peer AS 209 201.0.0.0/8, 1 ucast
next-hops, 0 mcast next-hops
    *via 203.0.0.1, GigabitEthernet 2/0, [ 200/0 ] , 04:35:03, bgp-209, internal, tag 209
       extended route information: AS Hops 0, BGP peer AS 209 202.0.0.0/8, 1 ucast
next-hops, 0 mcast next-hops
    *via 203.0.0.1, GigabitEthernet 2/0, [ 200/0 ] , 04:34:53, bgp-209, internal, tag 209
       extended route information: AS Hops 0, BGP peer AS 209 203.0.0.0/8, 1 ucast
next-hops, 0 mcast next-hops, attached
    *via 203.0.0.205, GigabitEthernet 2/0, [ 0/0 ] , 04:35:13, direct 204.0.0.0/8, 1 ucast
next-hops, 0 mcast next-hops
    *via 203.0.0.1, GigabitEthernet 2/0, [ 115/30 ] , 04:34:54, isis-p1, L2 205.0.0.0/8, 1
ucast next-hops, 0 mcast next-hops
    *via 203.0.0.1, GigabitEthernet 2/0, [ 115/20 ] , 04:34:54, isis-p1, L2
ServiceRouter#
```

The following example shows how to display the static route configuration in URIB:

```
ServiceRouter# show ip rib route static
IP Urib Route Table:
    '*' denotes best ucast next-hop     '**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]

10.1.1.0/24, 1 ucast next-hops, 0 mcast next-hops
   *via GigabitEthernet 2/0, [1/0], 00:26:07, static
10.1.2.0/24, 1 ucast next-hops, 0 mcast next-hops
   *via GigabitEthernet 2/0, [1/0], 00:26:07, static
10.1.3.0/24, 1 ucast next-hops, 0 mcast next-hops
   *via GigabitEthernet 2/0, [1/0], 00:26:07, static
10.1.4.0/24, 1 ucast next-hops, 0 mcast next-hops
   *via GigabitEthernet 2/0, [1/0], 00:26:07, static
```

Related Commands

Command	Description
ip rib route	Configures unicast static routes for the Proximity Engine.
proximity engine enable	Enables the Proximity Engine.
show ip static route	Displays IP static route information.

show ip rib unresolved-next-hop

To display unresolved next-hop information from the RIB, use the **show ip rib unresolved-next-hop** command in user EXEC configuration mode.

show ip rib unresolved-next-hop [*ip_address*]

Syntax Description

ip_address	IP address for which recursive next-hop information is displayed.

Command Defaults

In no *ip_address* argument is specified, **show ip rib recursive-next-hop** displays information for all unresolved next-hops for this Proximity Engine.

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command is used to display unresolved next-hop information from the RIB. It is normal to have zero unresolved next-hops. When incoming packets contain a next-hop address that cannot be resolved (that is, cannot be found during the route lookup), the count of unresolved next-hops increases.

Examples

The following example shows sample output from the **show ip rib unresolved-next-hop** command.

```
ServiceRouter# show ip rib unresolved-next-hop

Information about unresolved next-hops for context "default"
Proximity Engine
Number of unresolved nexthops: 0

ServiceRouter#
```

Related Commands

Command	Description
proximity engine enable	Enables the Proximity Engine.

show ip routes

To display the IP routing table, use the **show ip routes** command in EXEC configuration mode.

show ip routes

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The **show ip routes** command displays the policy routing tables. The main routing table is always displayed first, and if any policy routing tables have been instantiated, they are also displayed after the main table.

Examples

The **show ip routes** command displays the IP routing table that shows actual routes in the system.

Table 3-58 describes the fields shown in the **show ip routes** display.

Table 3-58 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.

The following example shows sample output from the **show ip routes** command:

```
ServiceRouter# sh ip routes
Destination      Gateway          Netmask
---------------- ---------------- ----------------
202.0.0.22       203.0.0.1        255.255.255.255
20.0.40.1        2.8.1.204        255.255.255.255
12.0.0.2         203.0.0.1        255.255.255.255
20.0.60.1        2.8.1.206        255.255.255.255
13.0.0.3         203.0.0.1        255.255.255.255
2.2.2.2          203.0.0.1        255.255.255.255
204.0.0.2        203.0.0.1        255.255.255.255
20.0.50.1        2.8.1.205        255.255.255.255
13.0.0.1         203.0.0.1        255.255.255.255
12.0.0.1         203.0.0.1        255.255.255.255
20.0.10.1        2.8.1.201        255.255.255.255
20.0.70.1        2.8.1.207        255.255.255.255
201.0.0.12       203.0.0.1        255.255.255.255
20.0.30.1        2.8.1.203        255.255.255.255
20.0.20.1        2.8.1.202        255.255.255.255
20.0.80.1        2.8.1.208        255.255.255.255
```

```
2.8.1.0          0.0.0.0          255.255.255.0
20.0.0.0         2.8.1.201        255.0.0.0
172.0.0.0        2.8.1.1          255.0.0.0
10.0.0.0         2.8.1.1          255.0.0.0
203.0.0.0        0.0.0.0          255.0.0.0
0.0.0.0          2.8.1.1          0.0.0.0
```

Related Commands

Command	Description
ip	Changes initial network device configuration settings.

show ip static route

To display IP static route information, use the **show ip static route** command in user EXEC configuration mode.

show ip static route

Syntax Description

This command has no keywords or arguments.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Examples

The following example shows sample output from the **show ip rib route** command:

```
ServiceRouter# show ip static route
IPv4 Unicast Static Routes:
  10.1.1.0/24, configured nh: 0.0.0.0/32
    real nh: 0.0.0.0, iod: 8 [1/0]
  10.1.2.0/24, configured nh: 0.0.0.0/32
    real nh: 0.0.0.0, iod: 8 [1/0]
  10.1.3.0/24, configured nh: 0.0.0.0/32
    real nh: 0.0.0.0, iod: 8 [1/0]
  10.1.4.0/24, configured nh: 0.0.0.0/32
    real nh: 0.0.0.0, iod: 8 [1/0]
  10.1.5.0/24, configured nh: 0.0.0.0/32
    real nh: 0.0.0.0, iod: 8 [1/0]
  10.1.6.0/24, configured nh: 0.0.0.0/32
    real nh: 0.0.0.0, iod: 8 [1/0]
```

Related Commandsl

Command	Description
ip rib route	Configures unicast static routes for the Proximity Engine.
show ip rib route	Displays IP RIB route information.

show ipv6

To display IPv6 information, use the **show ipv6** command in user EXEC configuration mode.

show ipv6

Syntax Description

access-list	Displays IPv6 access list information.
standard_ip_acl_num	Standard IPv6 access-list number. The range is from 1 to 99.
extended_ip_acl_num	Extended IPv6 access-list number. The range is from 100 to 199.
access-list name	Access-list name (max 30 characters).
routes	Displays the IPv6 routing table.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Examples

The following example shows sample output from the **show ipv6 access-list** command:

```
ServiceRouter# show ipv6 access-list
Space available:
    48 access lists
   498 access list conditions

Standard IPv6 access list 1
   1 deny fec0:0:3:5::1/128
     (implicit deny any: 0 matches)
   total invocations: 0
Extended IPv6 access list test
   1 permit icmpv6 any any echo
     (implicit fragment permit: 0 matches)
     (implicit deny ip any any: 0 matches)
   total invocations: 0

Interface access list references:
  None Configured

Application access list references:
  No applications registered.
```

The following example shows sample output from the **show ipv6 routes** command:

```
ServiceRouter# show ipv6 routes
Destination                              Next Hop
---------------------------------------- ----------------------------------
Destination                              Next
3ffe:1200:4260:f::/64                    ::
fe80::/64                                ::
fec0:0:3:3::/64                          ::
ff00::/8                                 ::
::/0                                     fec0:0:3:3::1
::/0                                     fe80::218:74ff:fe17:a8c0
ServiceRouter#
```

Note On other **show** commands that relate to the IPv6 addresses, the output fields were designed to work with the longest possible IPv4 address, which has 15 characters; IPv6 addresses can be up to 39 characters long. When the command output displays an IPv6 address, a long IPv6 address can overflow into neighboring fields causing the output to be difficult to read.

Related Commandsl

Command	Description
clear ipv6	Clears IPv6 ACL counters.
ipv6	Specifies the default gateway's IPv6 address.
traceroute6	Traces the route to a remote IPv6-enabled host.

show isis adjacency

To display IS-IS adjacencies, use the **show isis adjacency** command in user EXEC configuration mode.

show isis adjacency [**detail**]

Syntax Description

detail	(Optional) Displays neighbor IP addresses and active topologies.

Command Modes

User EXEC configuration mode.

Command Defaults

By default, this command displays a summarized report on IS-IS adjacency.

Usage Guidelines

This command requires a Proximity Engine license.

Examples

The following is sample output from the **show isis adjacency** command with and without the parameter keyword **detail**:

```
ServiceRouter# show isis adjacency detail

IS-IS adjacency database:
System ID       SNPA            Level  State  Hold Time  Interface
0200.c0a8.5401  0000.a1e8.e019  1      UP     00:00:32   GigabitEthernet 3/0
  Up/Down transitions: 3, Last transition: 18:45:08 ago
  Circuit Type: 1-2
  IPv4 Address: 192.168.84.1
  IPv6 Address: 0::
  Circuit ID: 7301-7-core.01, Priority: 64

7301-7-core     001d.a1e9.c41b  1      UP     00:00:08   GigabitEthernet 3/0
  Up/Down transitions: 1, Last transition: 18:45:52 ago
  Circuit Type: 1-2
  IPv4 Address: 192.168.84.7
  IPv6 Address: 0::
  Circuit ID: 7301-7-core.01, Priority: 64

7301-7-core     001d.a1e9.c41b  2      UP     00:00:07   GigabitEthernet 3/0
  Up/Down transitions: 1, Last transition: 18:37:20 ago
  Circuit Type: 1-2
  IPv4 Address: 192.168.84.7
  IPv6 Address: 0::
Circuit ID: 7301-7-core.01, Priority: 64

ServiceRouter#

ServiceRouter# show isis adjacency

IS-IS adjacency database:
System ID       SNPA            Level  State  Hold Time  Interface
0200.c0a8.5401  0000.a1e8.e019  1      UP     00:00:29   GigabitEthernet 3/0
7301-7-core     001d.a1e9.c41b  1      UP     00:00:08   GigabitEthernet 3/0
7301-7-core     001d.a1e9.c41b  2      UP     00:00:10   GigabitEthernet 3/0
```

Related Commands

Command	Description
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

show isis clns route

To display one or all the destinations to which the router knows how to route CLNS packets, use the **show isis clns route** command in user EXEC configuration mode.

show isis clns route *nsap*

Syntax Description

nsap	CLNS Network Service Access Point (NSAP) address.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

The **show isis clns route** command shows the IS-IS Level 2 routing table and static and Intermediate System-to-Intermediate System Interior Gateway Routing Protocol (ISO-IGRP) learned prefix routes. This table stores IS-IS area addresses and prefix routes. This command requires a Proximity Engine license.

Examples

The following is sample output from the **show clns route** command when the *nsap* argument is not used:

```
ServiceRouter# show isis clns route

IS-IS Level-1 IS routing table
7301-5-Core.00, Instance 0x00000145
   *via 7301-7-core, GigabitEthernet 3/0, metric 20
7301-7-core.00, Instance 0x00000145
   *via 7301-7-core, GigabitEthernet 3/0, metric 10
7301-7-core.02, Instance 0x00000145
   *via 7301-7-core, GigabitEthernet 3/0, metric 20
0200.c0a8.5401.00, Instance 0x00000145
   *via 0200.c0a8.5401, GigabitEthernet 3/0, metric 10
0200.cf00.0002.00, Instance 0x00000145
   *via 0200.c0a8.5401, GigabitEthernet 3/0, metric 20
0200.cf00.0002.01, Instance 0x00000145
   *via 0200.c0a8.5401, GigabitEthernet 3/0, metric 20
0200.cf00.2802.00, Instance 0x00000145
   *via 0200.c0a8.5401, GigabitEthernet 3/0, metric 30
0200.cf00.2802.01, Instance 0x00000145
   *via 0200.c0a8.5401, GigabitEthernet 3/0, metric 30
0200.cf00.5002.00, Instance 0x00000145
   *via 0200.c0a8.5401, GigabitEthernet 3/0, metric 40
0200.cf00.5002.01, Instance 0x00000145
-- More --
```

Related Commands

Command	Description
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

show isis database

To display the IS-IS link-state database, use the **show isis database** command in user EXEC configuration mode.

show isis database [[*LSP_ID*] [**detail**] | **advertise** | **private** | **summary**]

Syntax Description

LSP_ID	(Optional) LSP ID in the form of xxxx.xxxx.xxxx.xxxx or name.
detail	(Optional) Displays detailed IS-IS information. When specified, the contents of each link-state packet (LSP) are displayed. Otherwise, a summary display is provided.
advertise	(Optional) Displays advertise detail information.
private	(Optional) Displays private information.
summary	(Optional) Displays summary IS-IS information.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

Each option for this command can be entered in an arbitrary string within the same command entry. For example, the following are both valid command specifications and provide the same output: **show isis database detail l2** and **show isis database l2 detail**. This command requires a Proximity Engine license.

Examples

The following is sample output from the **show isis database** command when it is issued with no keywords or arguments:

```
ServiceRouter# show isis database summary

IS-IS LSP database:
IS-IS Level-1 Link State Database
  LSP : 3

IS-IS Level-2 Link State Database
  LSP : 3

ServiceRouter#
```

The following is sample output from the **show isis database** command when it is issued with the **private** keyword:

```
ServiceRouter# show isis database private

IS-IS LSP database:
IS-IS Level-1 Link State Database
  LSPID                 Seq Number   Checksum  Lifetime   A/P/O/T
  DD10-CDE205-2.00-00 * 0x00000004   0x7D13    992        0/0/1/3
    Instance      :  0x00000004
    Digest Offset : 0
    Area Address  :  49.0000
```

```
    NLPID         :  0xCC
    Router ID     :  3.1.5.3
    IP Address    :  3.1.5.3
    Hostname      :  DD10-CDE205-2      Length : 13
    Extended IS   :  DD10-CDE205-2.01   Metric : 10
    Extended IP   :         3.1.5.0/24  Metric : 10          (U)
    Extended IP   :        26.0.0.0/8   Metric : 10          (U)
  DD10-CDE205-2.01-00 * 0x00000001   0x8ABC    992        0/0/0/3
    Instance      :  0x00000001
    Digest Offset : 0
    Extended IS   :  DD10-7301-6.00     Metric : 0
    Extended IS   :  DD10-CDE205-2.00   Metric : 0
  DD10-7301-6.00-00     0x00000003   0x206E    988        0/0/0/3
    Instance      :  0x00000000
    Digest Offset : 0
    Area Address  :  49.0000
    NLPID         :  0xCC
    Hostname      :  DD10-7301-6        Length : 11
    IP Address    :  62.0.0.6
    IP Internal   :        26.0.0.0/8   Metric : 10  (I,U)
    IP Internal   :        62.0.0.0/8   Metric : 10  (I,U)
    IS Neighbor   :  DD10-CDE205-2.01   Metric : 10  (I)
IS-IS Level-2 Link State Database
  LSPID                 Seq Number   Checksum  Lifetime   A/P/O/T
  DD10-CDE205-2.00-00 * 0x00000004   0x7D13    994        0/0/1/3
    Instance      :  0x00000004
    Digest Offset : 0
    Area Address  :  49.0000
    NLPID         :  0xCC
    Router ID     :  3.1.5.3
    IP Address    :  3.1.5.3
    Hostname      :  DD10-CDE205-2      Length : 13
    Extended IS   :  DD10-CDE205-2.01   Metric : 10
    Extended IP   :         3.1.5.0/24  Metric : 10          (U)
    Extended IP   :        26.0.0.0/8   Metric : 10          (U)
  DD10-CDE205-2.01-00 * 0x00000001   0x8ABC    994        0/0/0/3
    Instance      :  0x00000001
    Digest Offset : 0
    Extended IS   :  DD10-7301-6.00     Metric : 0
    Extended IS   :  DD10-CDE205-2.00   Metric : 0
  DD10-7301-6.00-00     0x00000003   0x2668    990        0/0/0/3
    Instance      :  0x00000000
    Digest Offset : 0
    Area Address  :  49.0000
    NLPID         :  0xCC
    Hostname      :  DD10-7301-6        Length : 11
    IP Address    :  62.0.0.6
    IS Neighbor   :  DD10-CDE205-2.01   Metric : 10  (I)
    IP Internal   :        26.0.0.0/8   Metric : 10  (I,U)
    IP Internal   :        62.0.0.0/8   Metric : 10  (I,U)

ServiceRouter#
```

The following is sample output from the **show isis database** command when it is issued with an *LSP_ID* specified:

```
ServiceRouter# sh isis database DD10-CDE205-2.00-00

IS-IS LSP database:
IS-IS Level-1 Link State Database
  LSPID                 Seq Number   Checksum  Lifetime   A/P/O/T
  DD10-CDE205-2.00-00 * 0x00000004   0x7D13    968        0/0/1/3
IS-IS Level-2 Link State Database
  LSPID                 Seq Number   Checksum  Lifetime   A/P/O/T
```

```
  DD10-CDE205-2.00-00 * 0x00000004   0x7D13    970        0/0/1/3

ServiceRouter#
```

The following is sample output from the **show isis database** command when it is issued with the **advertise** keyword:

```
ServiceRouter# show isis database advertise

IS-IS LSP database:
IS-IS Level-1 Link State Database
  LSPID                 Seq Number   Checksum  Lifetime   A/P/O/T
  DD10-CDE205-2.00-00 * 0x00000004   0x7D13    1016       0/0/1/3
    Max: 1446  Used:  104  Free: 1342
    Type:   1, Max:  42, Used:  42, Free:   0
    Type: 129, Max:   1, Used:   1, Free:   0
    Type: 134, Max:   4, Used:   4, Free:   0
      Router ID: 3.1.5.3
    Type:  22, Max: 255, Used:  11, Free: 244
      Extended IS NBR: DD10-CDE205-2.01 (UP)
    Type: 135, Max: 255, Used:  14, Free: 241
      Extended IP Prefix:         3.1.5.0/24  Metric: 10
      Extended IP Prefix:        26.0.0.0/8   Metric: 10
    Type: 137, Max: 255, Used:  13, Free: 242
      Hostname: DD10-CDE205-2  Length: 13
  DD10-CDE205-2.01-00 * 0x00000001   0x8ABC    1016       0/0/0/3
    Max: 1446  Used:   24  Free: 1422
    Type:  22, Max: 255, Used:  22, Free: 233
      Extended IS NBR: DD10-7301-6.00 (UP)
      Extended IS NBR: DD10-CDE205-2.00 (UP)
  DD10-7301-6.00-00     0x00000003   0x206E    1012       0/0/0/3
    Max:    0  Used:    0  Free:    0
IS-IS Level-2 Link State Database
  LSPID                 Seq Number   Checksum  Lifetime   A/P/O/T
  DD10-CDE205-2.00-00 * 0x00000004   0x7D13    1018       0/0/1/3
    Max: 1446  Used:  104  Free: 1342
    Type:   1, Max:  42, Used:  42, Free:   0
    Type: 129, Max:   1, Used:   1, Free:   0
    Type: 134, Max:   4, Used:   4, Free:   0
      Router ID: 3.1.5.3
    Type:  22, Max: 255, Used:  11, Free: 244
      Extended IS NBR: DD10-CDE205-2.01 (UP)
    Type: 135, Max: 255, Used:  14, Free: 241
      Extended IP Prefix:         3.1.5.0/24  Metric: 10
      Extended IP Prefix:        26.0.0.0/8   Metric: 10
    Type: 137, Max: 255, Used:  13, Free: 242
      Hostname: DD10-CDE205-2  Length: 13
  DD10-CDE205-2.01-00 * 0x00000001   0x8ABC    1018       0/0/0/3
    Max: 1446  Used:   24  Free: 1422
    Type:  22, Max: 255, Used:  22, Free: 233
      Extended IS NBR: DD10-7301-6.00 (UP)
      Extended IS NBR: DD10-CDE205-2.00 (UP)
  DD10-7301-6.00-00     0x00000003   0x2668    1014       0/0/0/3
    Max:    0  Used:    0  Free:    0

ServiceRouter#
```

The following is sample output from the **show isis database** command when it is issued with the **detail** keyword:

Note The Proximity Engine becomes a passive listener when the overload bit is present. This is set by default in the LSP originated by the Proximity Engine.

```
ServiceRouter# show isis database detail

IS-IS LSP database:
IS-IS Level-1 Link State Database
  LSPID                 Seq Number   Checksum  Lifetime   A/P/O/T
  DD10-CDE205-2.00-00 * 0x00000004   0x7D13    1007       0/0/1/3
    Area Address  :  49.0000
    NLPID         :  0xCC
    Router ID     :  3.1.5.3
    IP Address    :  3.1.5.3
    Hostname      :  DD10-CDE205-2      Length : 13
    Extended IS   :  DD10-CDE205-2.01   Metric : 10
    Extended IP   :         3.1.5.0/24  Metric : 10          (U)
    Extended IP   :        26.0.0.0/8   Metric : 10          (U)
  DD10-CDE205-2.01-00 * 0x00000001   0x8ABC    1007       0/0/0/3
    Extended IS   :  DD10-7301-6.00     Metric : 0
    Extended IS   :  DD10-CDE205-2.00   Metric : 0
  DD10-7301-6.00-00     0x00000003   0x206E    1002       0/0/0/3
    Area Address  :  49.0000
    NLPID         :  0xCC
    Hostname      :  DD10-7301-6        Length : 11
    IP Address    :  62.0.0.6
    IP Internal   :        26.0.0.0/8   Metric : 10  (I,U)
    IP Internal   :        62.0.0.0/8   Metric : 10  (I,U)
    IS Neighbor   :  DD10-CDE205-2.01   Metric : 10  (I)
IS-IS Level-2 Link State Database
  LSPID                 Seq Number   Checksum  Lifetime   A/P/O/T
  DD10-CDE205-2.00-00 * 0x00000004   0x7D13    1008       0/0/1/3
    Area Address  :  49.0000
    NLPID         :  0xCC
    Router ID     :  3.1.5.3
    IP Address    :  3.1.5.3
    Hostname      :  DD10-CDE205-2      Length : 13
    Extended IS   :  DD10-CDE205-2.01   Metric : 10
    Extended IP   :         3.1.5.0/24  Metric : 10          (U)
    Extended IP   :        26.0.0.0/8   Metric : 10          (U)
  DD10-CDE205-2.01-00 * 0x00000001   0x8ABC    1008       0/0/0/3
    Extended IS   :  DD10-7301-6.00     Metric : 0
    Extended IS   :  DD10-CDE205-2.00   Metric : 0
  DD10-7301-6.00-00     0x00000003   0x2668    1004       0/0/0/3
    Area Address  :  49.0000
    NLPID         :  0xCC
    Hostname      :  DD10-7301-6        Length : 11
    IP Address    :  62.0.0.6
    IS Neighbor   :  DD10-CDE205-2.01   Metric : 10  (I)
    IP Internal   :        26.0.0.0/8   Metric : 10  (I,U)
    IP Internal   :        62.0.0.0/8   Metric : 10  (I,U)
ServiceRouter#
```

Related Commands

Command	Description
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

show isis hostname-table

To display the router-name-to-system-ID mapping table entries for an IS-IS router, use the **show isis hostname-table** command in user EXEC configuration mode.

show isis hostname-table

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

In the IS-IS routing domain, the system ID is used to represent each router. The system ID is part of the network entity title (NET) that is configured for each IS-IS router. For example, a router with a configured NET of 49.0001.0023.0003.000a.00 has a system ID of 0023.0003.000a.
Router-name-to-system-ID mapping is difficult for network administrators to remember during maintenance and troubleshooting on the routers. Entering the **show isis hostname-table** command displays the entries in the router-name-to-system-ID mapping table. This command requires a Proximity Engine license.

Examples

Entering the **show isis hostname-table** command displays the dynamic host mapping table, which displays the router-name-to-system-ID mapping table entries. The * symbol next to the System ID signifies that this is the router-name-to-system-ID mapping information for the local router.

```
ServiceRouter# show isis hostname-table

IS-IS dynamic hostname table:
  Level  System ID       Dynamic hostname
  1      0200.c0a8.0a05  7301-5-Core
  1      0200.c0a8.0a07  7301-7-core
  1      1111.1111.1111* sn-sj83
  2      1234.1234.1234  sn-sj86
  2      1234.1242.1234  7301-2-IS-IS

ServiceRouter#
```

Related Commands

Command	Description
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

show isis interface

To display information about the IS-IS interfaces, use the **show isis interface** command in user EXEC configuration mode.

show isis interface *interface_name*

Syntax Description

interface_name	Interface name.

Command Defaults

Displays all IS-IS interfaces.

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command requires a Proximity Engine license.

Examples

The following is sample output from the **show isis interface** command with interface name set to be GigabitEthernet 1/0 and without an interface name, respectively:

```
ServiceRouter# show isis interface GigabitEthernet 1/0

GigabitEthernet 1/0, Interface status: protocol-down/link-down/admin-down
  IP address: 0.0.0.0, IP subnet: 0.0.0.0/0
  IPv6 routing is disabled
  IS-IS interface operation state : Down/Ready
  Index: 0x0002, Local Circuit ID: 0x02, Circuit Type: 1-2
  Passive level: level-1-2
  LSP interval: 33 ms
  Level      Metric   CSNP  Next CSNP  Hello   Multi   Next IIH
  1              10     10  Never         10   3       Never
  2              10     10  Never         10   3       Never
  Level  Adjs   Ups    Pri  Circuit ID         Since
  1         0     0     64  0000.0000.0000.02  never
  2         0     0     64  0000.0000.0000.02  never

ServiceRouter#

ServiceRouter# show isis interface

GigabitEthernet 1/0, Interface status: protocol-up/link-up/admin-up
  IP address: 172.20.168.83, IP subnet: 172.20.168.0/24
  IPv6 routing is disabled
  Index: 0x0001, Local Circuit ID: 0x01, Circuit Type: 1-2
  Passive level: level-1-2
  LSP interval: 33 ms
  Level      Metric   CSNP  Next CSNP  Hello   Multi   Next IIH
  1              10     10  Never         10   3       Never
  2              10     10  Never         10   3       Never
  Level  Adjs   Ups    Pri  Circuit ID         Since
  1         0     0     64  sn-sj83.01         never
  2         0     0     64  sn-sj83.01         never
```

```
GigabitEthernet 1/0, Interface status: protocol-down/link-down/admin-down
  IP address: 0.0.0.0, IP subnet: 0.0.0.0/0
  IPv6 routing is disabled
  IS-IS interface operation state : Down/Ready
  Index: 0x0002, Local Circuit ID: 0x02, Circuit Type: 1-2
  Passive level: level-1-2
  LSP interval: 33 ms
  Level      Metric   CSNP  Next CSNP  Hello   Multi   Next IIH
  1              10     10  Never         10   3       Never
  2              10     10  Never         10   3       Never
  Level  Adjs   Ups    Pri  Circuit ID         Since
  1         0     0     64  0000.0000.0000.02  never
  2         0     0     64  0000.0000.0000.02  never

GigabitEthernet 2/0, Interface status: protocol-down/link-down/admin-down
  IP address: 0.0.0.0, IP subnet: 0.0.0.0/0
  IPv6 routing is disabled
  IS-IS interface operation state : Down/Ready
  Index: 0x0003, Local Circuit ID: 0x03, Circuit Type: 1-2
  Passive level: level-1-2
  LSP interval: 33 ms
  Level      Metric   CSNP  Next CSNP  Hello   Multi   Next IIH
  1              10     10  Never         10   3       Never
  2              10     10  Never         10   3       Never
  Level  Adjs   Ups    Pri  Circuit ID         Since
  1         0     0     64  0000.0000.0000.03  never
  2         0     0     64  0000.0000.0000.03  never

GigabitEthernet 3/0, Interface status: protocol-up/link-up/admin-up
  IP address: 192.168.84.83, IP subnet: 192.168.84.0/24
  IPv6 routing is disabled
  Index: 0x0004, Local Circuit ID: 0x04, Circuit Type: 1-2
  LSP interval: 33 ms
  Level      Metric   CSNP  Next CSNP  Hello   Multi   Next IIH
  1              10     10  Never         10   3       00:00:08
  2              10     10  Never         10   3       00:00:05
  Level  Adjs   Ups    Pri  Circuit ID         Since
  1         2     2     64  7301-7-core.01     18:55:47
  2         1     1     64  7301-7-core.01     18:47:15

GigabitEthernet 4/0, Interface status: protocol-up/link-up/admin-up
  IP address: 192.168.78.83, IP subnet: 192.168.78.0/24
  IPv6 routing is disabled
  Index: 0x0005, Local Circuit ID: 0x05, Circuit Type: 1-2
  Passive level: level-1-2
  LSP interval: 33 ms
  Level      Metric   CSNP  Next CSNP  Hello   Multi   Next IIH
  1              10     10  Never         10   3       Never
  2              10     10  Never         10   3       Never
  Level  Adjs   Ups    Pri  Circuit ID         Since
  1         0     0     64  sn-sj83.05         never
  2         0     0     64  sn-sj83.05         never

GigabitEthernet 5/0, Interface status: protocol-down/link-down/admin-down
  IP address: 0.0.0.0, IP subnet: 0.0.0.0/0
  IPv6 routing is disabled
  IS-IS interface operation state : Down/Ready
  Index: 0x0006, Local Circuit ID: 0x06, Circuit Type: 1-2
  Passive level: level-1-2
  LSP interval: 33 ms
  Level      Metric   CSNP  Next CSNP  Hello   Multi   Next IIH
  1              10     10  Never         10   3       Never
  2              10     10  Never         10   3       Never
  Level  Adjs   Ups    Pri  Circuit ID         Since
```

```
  1         0     0     64  0000.0000.0000.06  never
  2         0     0     64  0000.0000.0000.06  never

GigabitEthernet 6/0, Interface status: protocol-down/link-down/admin-down
  IP address: 0.0.0.0, IP subnet: 0.0.0.0/0
  IPv6 routing is disabled
  IS-IS interface operation state : Down/Ready
  Index: 0x0007, Local Circuit ID: 0x07, Circuit Type: 1-2
  Passive level: level-1-2
  LSP interval: 33 ms
  Level      Metric   CSNP  Next CSNP  Hello   Multi   Next IIH
  1              10     10  Never         10   3       Never
  2              10     10  Never         10   3       Never
  Level  Adjs   Ups    Pri  Circuit ID         Since
  1         0     0     64  0000.0000.0000.07  never
  2         0     0     64  0000.0000.0000.07  never

GigabitEthernet 7/0, Interface status: protocol-down/link-down/admin-down
  IP address: 0.0.0.0, IP subnet: 0.0.0.0/0
  IPv6 routing is disabled
  IS-IS interface operation state : Down/Ready
  Index: 0x0008, Local Circuit ID: 0x08, Circuit Type: 1-2
  Passive level: level-1-2
  LSP interval: 33 ms
  Level      Metric   CSNP  Next CSNP  Hello   Multi   Next IIH
  1              10     10  Never         10   3       Never
  2              10     10  Never         10   3       Never
  Level  Adjs   Ups    Pri  Circuit ID         Since
  1         0     0     64  0000.0000.0000.08  never
  2         0     0     64  0000.0000.0000.08  never

ServiceRouter#
```

Related Commands

Command	Description
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

show isis ip route

To display the Intermediate IS-IS RSPF route for IS-IS learned routes, use the **show isis ip route** command in user EXEC configuration mode.

show isis ip route [*IP* | **detail** | **summary**]

Syntax Description

IP	(Optional) IP address in the form of *xxx.xxx.xxx.xxx*.
detail	(Optional) Displays detailed IS-IS route information. When specified, the contents of each link-state packet (LSP) are displayed. Otherwise, a summary display for a given IP address is provided.
summary	(Optional) Displays summary IS-IS route information.

Command Defaults

Displays all IS-IS route information.

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command requires a Proximity Engine license.

Examples

The following is sample output from the **show isis route** command with various parameters:

```
ServiceRouter# show isis ip route detail

IS-IS IPv4 routing table

5.5.5.5/32, L2
   *via 192.168.84.7, GigabitEthernet 3/0, metric 20, L2 (I,U)
        Instance 0x0000D831
        LSPID 1234.1242.1234.00-00
12.1.1.1/32, L2
   *via 192.168.84.7, GigabitEthernet 3/0, metric 20, L2 (I,U)
        Instance 0x0000D831
        LSPID 1234.1242.1234.00-00
13.1.1.1/32, L2
   *via 192.168.84.7, GigabitEthernet 3/0, metric 20, L2 (I,U)
        Instance 0x0000D831
        LSPID 1234.1242.1234.00-00
14.1.1.1/32, L2
   *via 192.168.84.7, GigabitEthernet 3/0, metric 20, L2 (I,U)
        Instance 0x0000D831
        LSPID 1234.1242.1234.00-00
22.22.22.22/32, L2
   *via 192.168.84.7, GigabitEthernet 3/0, metric 20, L2 (I,U)
        Instance 0x0000D831
        LSPID 1234.1242.1234.00-00
40.1.1.0/24, L2
   *via 192.168.84.7, GigabitEthernet 3/0, metric 20, L2 (I,U)
 -- More --

ServiceRouter# show isis ip route summary
```

```
IS-IS IPv4 routing table

Total number of best routes  : 8517
Total number of paths        : 12523
Total number of best paths   : 8517
Total number of backup paths : 4006

Best routes per level
  L1         total    : 4006
             direct   : 3
             normal   : 4003
  L2         total    : 4511
             normal   : 4511

Best paths per level
  L1         total    : 4006
             direct   : 3
             normal   : 4003
  L2         total    : 4511
             normal   : 4511

Backup paths per level
  L2         total    : 4006
             direct   : 3
             normal   : 4003

Number of best routes per mask-length
  /24 : 8511    /32 : 6

ServiceRouter#

ServiceRouter# show isis ip route 40.1.1.0

IS-IS IPv4 routing table

40.1.1.0/24, L2
   *via 192.168.84.7, GigabitEthernet 3/0, metric 20, L2 (I,U)

ServiceRouter#

ServiceRouter# show isis ip route 40.1.1.0 detail

IS-IS IPv4 routing table

40.1.1.0/24, L2
   *via 192.168.84.7, GigabitEthernet 3/0, metric 20, L2 (I,U)
        Instance 0x0000D880
        LSPID 1234.1242.1234.00-00

ServiceRouter#
```

Related Commands

Command	Description
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

show isis ip rspf route

To display the Intermediate IS-IS RSPF route for IS-IS learned routes, use the **show isis ip rspf** command in user EXEC configuration mode.

show isis ip rspf route [*LSP_ID*]

Syntax Description

LSP_ID	(Optional) LSP ID in the form of *xxxx.xxxx.xxxx.xxxx* or name.

Command Defaults

If no LSP ID is specified, displays IS-IS RSPF information for all LSP IDs.

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command is used to display the IS-IS RSPF routing information. Output is only displayed for this command when a new proximity request has been received. To clear IS-IS RSPF routing information, use the **clear isis ip rspf route** command. This command requires a Proximity Engine license.

Examples

The following is sample output from the **show isis rspf route** command:

```
ServiceRouter# show isis ip rspf route

LSP ID                 SPF Time  Cache Hit  Level      Age Max range
0200.c0a8.0a01.00-00   01:45:41     0          1       01:43:23 10

ServiceRouter#

ServiceRouter# show isis ip rspf route 0200.c0a8.0a07.00-00

IS-IS IPv4 routing table

172.20.168.0/24, L1
   metric 20, L1
192.168.78.0/24, L1
   metric 20, L1
192.168.79.0/24, L1
   metric 20, L1
192.168.84.0/24, L1
   metric 10, L1
192.168.89.0/24, L1
   metric 10, L1
192.168.90.0/24, L1
   metric 10, L1
207.0.0.0/24, L1
   metric 20, L1
207.0.1.0/24, L1
   metric 30, L1
-- More --

ServiceRouter#
```

Related Commands

Command	Description
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

show isis memory

To display memory usage information for an IS-IS instance, use the **show isis memory** command in user EXEC configuration mode.

show isis memory

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command requires a Proximity Engine license.

Examples

The following is sample output from the **show isis memory** command:

```
ServiceRouter# show isis memory

Shared memory information for /topos-shm-isis-abc,
Current-Size         HWM    Maximum-Size
     2005392     2005392         4194304
IS-IS memory usage:
Type             Size      Count        HWM       Slab   Overhead      Total
Interface        2632          9          9         16      18600      42288
Adjacency         184         35         35         64       5512      11952
LSP DB            320        665        665        704      13136     225936
LSP TLV            48         10         10         64       2768       3248
LSP Retx           72          0          0          0        128        128
Next Hop           24      13130      21970      22528     226736     541856
RT HIX             32          0          0          0        128        128
SPF Adj           104          3          3         64       6520       6832
SPF RT             28      20553      20557      21504      27764     603248
Redist RT          44          3          3       1024      45100      45232
RI                 72          6          6       1024      73472      73904
SPF RT             40          0          1          0        128        128
Redist RT          56          0          0          0        128        128
RI                 56          0          0          0        128        128
Total:                                                    420248    1555136

ServiceRouter#
```

Related Commands

Command	Description
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

show isis process

To display summary information about an IS-IS instance, use the **show isis process** command in user EXEC configuration mode.

show isis process

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command requires a Proximity Engine license.

Examples

The following is sample output from the **show isis process** command:

```
ServiceRouter# show isis process

IS-IS process : abc
  System ID : 1111.1111.1111  IS-Type : L1-L2
  SAP : 1666  Queue Handle : 1666
  Metric-style : advertise(narrow, wide), accept(narrow, wide)
  Area address(es) :
    49.0005
  Process is up and running
  VRF ID: 1
  Stale routes during non-graceful controlled restart
  Interfaces supported by IS-IS :
    GigabitEthernet 0/0
    GigabitEthernet 1/0
    GigabitEthernet 2/0
    GigabitEthernet 3/0
    GigabitEthernet 4/0
    GigabitEthernet 5/0
    GigabitEthernet 6/0
    GigabitEthernet 7/0
  Address family IPv4 unicast :
    Number of interface : 8
    Distance : 115
  Address family IPv6 unicast :
    Number of interface : 0
    Distance : 115
```

Related Commands

Command	Description
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

show isis rrm

To display IS-IS Received Routing Message (RRM) information, use the **show isis rrm** command in user EXEC configuration mode.

show isis rrm ***int****erface_name*

Syntax Description

interface-name	Interface name

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command requires a Proximity Engine license.

Examples

The following is sample output from the **show isis rrm** command that shows rrm information for all interfaces:

```
ServiceRouter# show isis rrm GigabitEthernet 1/0

IS-IS RRM information for interface GigabitEthernet 1/0:
  No retransmission on non-P2P interface
ServiceRouter# show isis rrm GigabitEthernet 1/0
IS-IS RRM information for interface GigabitEthernet 1/0:
  No retransmission on non-P2P interface

ServiceRouter#

ServiceRouter# show isis rrm GigabitEthernet 2/0

IS-IS RRM information for interface GigabitEthernet 2/0:
  No retransmission on non-P2P interface
ServiceRouter# show isis rrm GigabitEthernet 3/0
IS-IS RRM information for interface GigabitEthernet 3/0:
  No retransmission on non-P2P interface

ServiceRouter#
```

Related Commands

Command	Description
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

show isis spf-log

To display how often and why the router has run a full shortest path first (SPF) calculation, use the **show isis spf-log** command in user EXEC configuration mode.

show isis spf-log [**detail**]

Syntax Description

detail	(Optional) Displays detailed information about the SPF calculation.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command requires a Proximity Engine license.

Examples

The following is sample output from **show isis spf-log** and **show isis spf-log detail** commands, respectively:

```
ServiceRouter# show isis spf-log

IS-IS SPF information:
Total number of SPF calculations: 55836

Log entry (current/max): 20/20
Ago       Level  Reason                                          Count  Total
00:02:49  2      Updated LSP 7301-5-Core.00-0f                       1  0.011510
00:02:49  2      Updated LSP 7301-5-Core.00-10                       1  0.011956
00:02:49  2      Updated LSP 7301-5-Core.00-11                       1  0.011469
00:02:49  2      Updated LSP 7301-5-Core.00-12                       1  0.011503
00:02:49  2      Updated LSP 7301-5-Core.00-13                       1  0.011473
00:02:49  2      Updated LSP 7301-5-Core.00-14                       1  0.011522
00:02:49  2      Updated LSP 7301-5-Core.00-15                       1  0.011514
00:02:49  2      Updated LSP 7301-5-Core.00-16                       1  0.011516
00:02:49  2      Updated LSP 7301-5-Core.00-17                       1  0.011499
00:02:49  2      Updated LSP 7301-5-Core.00-18                       1  0.011530
00:02:49  2      Updated LSP 7301-5-Core.00-19                       1  0.011476
00:02:49  2      Updated LSP 7301-5-Core.00-1a                       1  0.011560
00:02:49  2      Updated LSP 7301-5-Core.00-1b                       1  0.011510
00:02:49  2      Updated LSP 7301-5-Core.00-1c                       1  0.011710
00:02:49  2      Updated LSP 7301-5-Core.00-1d                       1  0.011514
00:02:49  2      Updated LSP 7301-5-Core.00-1e                       1  0.011512
00:02:49  2      Updated LSP 7301-5-Core.00-1f                       1  0.011934
00:02:49  2      Updated LSP 7301-5-Core.00-20                       1  0.011525
00:02:49  2      Updated LSP 7301-5-Core.00-21                       1  0.012232
00:02:49  2      Purged LSP 7301-5-Core.01-00                        1  0.011647

ServiceRouter#

ServiceRouter# show isis spf-log detail

IS-IS SPF information:
```

```
Total number of SPF calculations: 55836

Log entry (current/max): 20/20
Log entry: 01, Ago: 00:03:59, Date: Tue Jan 06 17:34:05 1970
  Level  Instance    Init      SPF       IS Update  URIB Update  Total
  2      0x0000D8C4  0.000019  0.008100  0.000133   0.003255     0.011510
  Level  Node Count   Changed  Reason
  2         8     1         0  Updated LSP 7301-5-Core.00-0f

Log entry: 02, Ago: 00:03:59, Date: Tue Jan 06 17:34:05 1970
  Level  Instance    Init      SPF       IS Update  URIB Update  Total
  2      0x0000D8C5  0.000016  0.008552  0.000129   0.003256     0.011956
  Level  Node Count   Changed  Reason
  2         8     1         0  Updated LSP 7301-5-Core.00-10

Log entry: 03, Ago: 00:03:58, Date: Tue Jan 06 17:34:05 1970
  Level  Instance    Init      SPF       IS Update  URIB Update  Total
  2      0x0000D8C6  0.000016  0.008079  0.000127   0.003243     0.011469
  Level  Node Count   Changed  Reason
  2         8     1         0  Updated LSP 7301-5-Core.00-11

Log entry: 04, Ago: 00:03:58, Date: Tue Jan 06 17:34:05 1970
  Level  Instance    Init      SPF       IS Update  URIB Update  Total
  2      0x0000D8C7  0.000015  0.008097  0.000129   0.003258     0.011503
  Level  Node Count   Changed  Reason
  2         8     1         0  Updated LSP 7301-5-Core.00-12

Log entry: 05, Ago: 00:03:58, Date: Tue Jan 06 17:34:05 1970
  Level  Instance    Init      SPF       IS Update  URIB Update  Total
  2      0x0000D8C8  0.000017  0.008088  0.000129   0.003236     0.011473
  Level  Node Count   Changed  Reason
  2         8     1         0  Updated LSP 7301-5-Core.00-13

Log entry: 06, Ago: 00:03:58, Date: Tue Jan 06 17:34:05 1970
  Level  Instance    Init      SPF       IS Update  URIB Update  Total
  2      0x0000D8C9  0.000019  0.008113  0.000130   0.003257     0.011522
  Level  Node Count   Changed  Reason
  2         8     1         0  Updated LSP 7301-5-Core.00-14

ServiceRouter#
```

Related Commands

Command	Description
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

show isis srm

To display Send Routing Message (SRM) information for an IS-IS, use the **show isis srm** command in privileged EXEC configuration mode.

show isis srm *interface_name*

Syntax Description

interface-name	Interface name.

Command Defaults

None

Command Modes

Privileged EXEC configuration mode.

Usage Guidelines

This command requires a Proximity Engine license.

Examples

The following example shows how to display sample output from the **show isis srm** command. It shows the srm information on interface GigabitEthernet 1/0:

```
ServiceRouter# show isis srm GigabitEthernet 1/0

IS-IS SRP information for interface GigabitEthernet 1/0:
IS-IS Level-1 Link State Database
Interface is not eligible for flooding LSP
Interface is not on stopped SRM list
LSP interval: 33ms, Next LSP: Never
LSPID                 Seq Number   Checksum  Lifetime   A/P/O/T

IS-IS Level-2 Link State Database
  IS-IS Level-1 Link State Database
Interface is not eligible for flooding LSP
Interface is not on stopped SRM list
LSP interval: 33ms, Next LSP: Never
LSPID                 Seq Number   Checksum  Lifetime   A/P/O/T

ServiceRouter#
```

Related Commands

Command	Description
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

show isis ssn

To display Send Sequence Number (SSN) information for an IS-IS, use the **show isis ssn** command in user EXEC configuration mode.

show isis ssn *interface_name*

Syntax Description

interface-name	Interface name.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command requires a Proximity Engine license.

Examples

The following is sample output from the **show isis ssn** command that shows the ssn information on interface GigabitEthernet 1/0.

```
ServiceRouter# show isis ssn GigabitEthernet 1/0

IS-IS SSN information for interface GigabitEthernet 1/0:
IS-IS Level-1 Link State Database
  Interface is not eligible for sending PSNP
  Next PSNP: Never
  LSPID                 Seq Number   Checksum  Lifetime   A/P/O/T
IS-IS Level-2 Link State Database
  Interface is not eligible for sending PSNP
  Next PSNP: Never
  LSPID                 Seq Number   Checksum  Lifetime   A/P/O/T

ServiceRouter#
```

Related Commands

Command	Description
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

show key chain

To display the key chains in the system, use the **show key chain** command in user EXEC configuration mode.

show key chain [**decrypt** | *name*]

Syntax Description

decrypt	(Optional) Displays key chain information.
name	(Optional) Key chain name.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

This command requires a Proximity Engine license.

Examples

The following is sample output from the **show key chain** command:

```
ServiceRouter# show key chain
show key chain
Key-Chain lsp
  Key 1 -- text <encrypted-string>
    accept lifetime (00:00:00 Jan 01 1970) - (always valid) [valid now]
    send lifetime (00:00:00 Jan 01 1970) - (always valid) [valid now]

ServiceRouter#
```

Related Commands

Command	Description
key	Creates a key chain and enter into key chain configuration submode.
key chain	Creates a key chain and enter into key chain configuration submode.
key-string	Creates a key string to be used for authentication.

show lacp

To display LACP information, use the **show lacp** command in EXEC configuration mode.

show lacp {**counters**| **internal**}

Syntax Description

counters	Displays LACP traffic information.
internal	Displays LACP link status information.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

You must first turn on LACP by entering the **lacp** command in Interface configuration mode before you can display the LACP statistics.

In the **show lacp counters** command, the LACP control packet is sent or received every 30 seconds. If one of the interfaces within the port channel goes down, then the counter value does not further increment for that interface.

Examples

The following example shows how to display the LACP statistics:

```
ServiceEngine# show lacp counters
Interface PortChannel 1 (4 physical interface(s)):
Protocol: none

Interface PortChannel 2 (4 physical interface(s)):
                          lacpdu             marker     marker response
Port                  send       receive    send  receive send receive error
-----------------------------------------------------
GigabitEthernet  7/0         16         16      0      0      0      0      0
GigabitEthernet  8/0         16         15      0      0      0      0      0
GigabitEthernet  9/0         16         15      0      0      0      0      0
GigabitEthernet 10/0         17         15      0      0      0      0      0

Interface PortChannel 3 (0 physical interface(s)):
Protocol: none

Interface PortChannel 4 (0 physical interface(s)):
Protocol: none
```

The following example shows how to display the link status for the port channel:

```
ServiceEngine# show lacp internal
Interface PortChannel 1 (4 physical interface(s)):
Protocol: LACP
Mode:     src-dst-port
Port                    Admin-State Link-State     LACP-State     Aggregate id
-------------------------------------------------------------------------------
GigabitEthernet  3/0           up         up         bndl              21
GigabitEthernet  4/0           up         up         bndl              21
```

```
GigabitEthernet  5/0           up         up         bndl              21
GigabitEthernet  6/0           up         up         bndl              21

ServiceEngine# show interface portChannel 1 lacp
Interface PortChannel 1 (4 physical interface(s)):
Protocol: LACP
Mode:     src-dst-port
Port                    Admin-State Link-State     LACP-State     Aggregate id
------------------------------------------------------------------------------
GigabitEthernet  3/0           up         up         bndl              21
GigabitEthernet  4/0           up         up         bndl              21
GigabitEthernet  5/0           up         up         bndl              21
GigabitEthernet  6/0           up         up         bndl              21
```

Related Commands

Command	Description
lacp	Turns on Link Aggregation Control Protocol (LACP).
show interface portchannel 1 lacp	Displays the link status for the port channel.

show logging

To display the system message log configuration, use the **show logging** command in EXEC configuration mode.

show logging

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

EXEC configuration mode.

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 the SE device.

Examples

The following example shows how to display 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

Command	Description
clear	Clears the HTTP object cache, the hardware interface, statistics, archive working transaction logs, and other settings.
logging	Configures system logging.

show movie-streamer

To display the Movie Streamer configuration, use the **show movie-streamer** command in EXEC configuration mode.

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.

Command Defaults

None

Command Modes

EXEC configuration mode.

Examples

The following example shows the Movie Streamer configuration:

```
ServiceEngine# show movie-streamer
Movie Streamer version cde220-5.0.3
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

Command	Description
movie-streamer	Enables and configures the Movie Streamer server.
show statistics movie-streamer	Displays statistics for the Movie Streamer.

show multicast

To display whether or not the multicast sender and receiver are enabled, use the **show multicast** command in EXEC configuration mode.

show multicast

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

This command is only available on Cisco Internet Streamer CDS Release 3.1.1.

Examples

The following example shows how to display the multicast:

```
ServiceEngine# show multicast
multicast sender not  enabled
multicast receiver  enabled
```

Related Commands

Command	Description
multicast (Global configuration)	Configures multicast options.
multicast (EXEC configuration)	Generate multicast packets and tests connectivity through multicast routers.

show ntp

To display the Network Time Protocol (NTP) parameters, use the **show ntp** command in EXEC configuration mode.

show ntp status

Syntax Description

status	Displays the NTP status.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 3-59 describes the fields shown in the **show ntp status** display.

Table 3-59 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

Command	Description
clock	Sets or clears clock functions or updates the calendar.
ntp	Configures the NTP server and allows the system clock to be synchronized by a time server.

show processes

To display CPU or memory processes, use the **show processes** command in EXEC configuration mode.

show processes [**cpu** | **debug** *pid* | **memory** | **system** [**delay** *delay_num* | **count** *count_num*]]

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.
pid	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. The range is from 1 to 60.
delay_num	Displays delays between updates, in seconds.
count	(Optional) Specifies the number of updates that are displayed. The range is from 1 to 100.
count_num	Displays the number of updates displayed.

Command Defaults

None

Command Modes

EXEC configuration mode.

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:

- List of all processes in wide format.
- Two tables listing the processes that use 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 s**how process** command with keywords **system** and especially **debug,** unless it is absolutely necessary.

Table 3-60 describes the fields shown in the **show processes** displays.

Table 3-60 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** command in EXEC configuration mode.

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.
id	Unique number identifying the program.
program-name	(Optional) Displays detailed program information for the specified program name.
name	(Optional) Name of the program.

Command Defaults

None

Command Modes

EXEC configuration mode.

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 the program starts and ends.

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 prepositioned 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 is 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
  - Prepositioned 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 Content Acquirer 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 Content Acquirer 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 network, make sure that there are no external proxy servers physically located between your Internet Streamer SEs and your Content Acquirer 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 Content Acquirer 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 is 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 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 before the live event, we recommend that you configure multiple schedules, one for each trial. We also recommend that you start the encoder before 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 prepositioned 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

The **show programs** command supports encoder failover. The output of the command looks like the following:

Note In the output of the **show programs program-name xxx** command, if the program is a unicast only program, the Priming Status displays.

```
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
Priming Status        :
       Primed            : No
       Current Status    : N/A
       Restarts          : 0

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

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 Content Acquirer and non-Content Acquirer output is consistent. Also, if the user executes the **show statistics wmt streamstat** command from the Content Acquirer, 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.

Note It is not possible to monitor non-primed streams because they are played directly from the origin server. Primed streams can be monitored because they are buffered on the SE.

Table 3-61 describes the fields shown in the **show programs program-name** and **program-id** display.

Table 3-61 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 radius-server

To display RADIUS information, use the **show radius-server** command in EXEC configuration mode.

show radius-server

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 3-62 describes the fields shown in the **show radius-server** display.

Table 3-62 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 3-62 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

Command	Description
radius-server	Configures RADIUS authentication parameters.

show rcp

To display Remote Copy Program (RCP) information, use the **show rcp** command in EXEC configuration mode.

show rcp

Syntax Description

This command has no keywords or arguments.

Command Defaults

None

Command Modes

EXEC configuration mode.

Examples

The following example shows how to display RCP information:

```
ServiceEngine# show rcp
rcp service configurations:
rcp             enable
```

Related Commands

Command	Description
rcp	Enables the RCP.

show rtsp

To display the Real-Time Streaming Protocol (RTSP) configurations, use the **show rtsp** command in EXEC configuration mode.

show rtsp [**gateway**]

Syntax Description

gateway	(Optional) Displays the RTSP gateway configuration.

Command Defaults

None

Command Modes

EXEC configuration mode.

Examples

The following example display the output of the **show rtsp gateway** command in EXEC configuration mode:

```
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

Command	Description
rtsp	Configure the RTSP-related parameters.

show rule

To display rules configuration information, use the **show rule** command in EXEC configuration mode.

show rule {**action** {**all** [**protocol** {**http** | **rtmp** | **rtsp**}] | **allow** [**protocol** {**http** | **rtmp** | **rtsp**}] | **block** [**protocol** {**http** | **rtmp** | **rtsp**}] | **generate-url-signature** [**protocol** {**http** | **rtmp** | **rtsp**}] | **no-cache** [**protocol** {**http** | **rtmp** | **rtsp**}] | **redirect** [**protocol** {**http** | **rtmp** | **rtsp**}] | **refresh** [**protocol** {**http** | **rtmp** | **rtsp**}] | **rewrite** [**protocol** {**http** | **rtmp** | **rtsp**}] | **validate-url-signature** [**protocol** {**http** | **rtmp** | **rtsp**}]} | **all** | **pattern-list** {*pattern_num* *pattern_type* | **all**}}

Syntax Description

action	Displays all the rules with the same action types.
all	Displays all the action rules.
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.
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.
pattern_num	Pattern number. The range is from 1 to 512.
pattern_type	Pattern type (see Table 3-63).
all	Displays rules with all pattern lists.

Command Defaults

None

Command Modes

EXEC configuration mode.

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 2-310. Table 3-63 shows the permitted pattern types and describes each pattern type.

Note The **rule action redirect** command does not display the pattern-list header field.

Table 3-63 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 shows how to display 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

Command	Description
clear	Clears the HTTP object cache, the hardware interface, statistics, archive working transaction logs, and other settings.
rule	Sets the rules by which the SE filters HTTP, HTTPS, and RTSP traffic.

show running-config

To display the current running configuration information on the terminal, use the **show running-config** command in EXEC configuration mode.

show running-config

Syntax Description

This command has no keywords or arguments.

Command Defaults

None

Command Modes

EXEC configuration mode.

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 shows how to display the current running configuration information:

```
ServiceEngine# show running-config
! CDS version 2.6.0
!
device mode service-engine
!
!
hostname EE8-2G2-5
!
!
authsvr location-server primary 4.0.1.3 7000
!
!
clock timezone PDT -7 0
!
!
ip domain-name telstra.com
!
exec-timeout 0
!
!
!
!
!
interface PortChannel 1
 ip address 188.0.82.8 255.255.255.0
 exit
interface PortChannel 2
 ip address 188.87.0.5 255.255.0.0
 exit
```

```
!
interface GigabitEthernet 1/0
 channel-group 1
 exit
interface GigabitEthernet 2/0
 channel-group 1
 exit
interface GigabitEthernet 3/0
 channel-group 2
 exit
interface GigabitEthernet 4/0
 channel-group 2
 exit
interface GigabitEthernet 5/0
 channel-group 2
 exit
interface GigabitEthernet 6/0
 channel-group 2
 exit
interface GigabitEthernet 7/0
 channel-group 2
 exit
interface GigabitEthernet 8/0
 channel-group 2
 exit
interface GigabitEthernet 9/0
 channel-group 2
 exit
interface GigabitEthernet 10/0
 channel-group 2
 exit
!
streaming-interface PortChannel 2
!
!
ip default-gateway 188.0.82.1
ip default-gateway 188.87.0.1
!
!
port-channel load-balance round-robin
primary-interface PortChannel 2
!
transaction-logs enable
transaction-logs archive max-file-size 2000000
transaction-logs archive max-file-number 50
transaction-logs archive interval 300
transaction-logs export enable
transaction-logs export interval 5
transaction-logs export sftp-server 188.0.84.5 root **** /var/ftp/pub/
upload
transaction-logs format custom "%J"
!
!
!
!
!
ip name-server 188.0.84.7
!
ip route 10.74.61.0 255.255.255.0 188.87.0.1
ip route 171.70.77.0 255.255.255.0 188.87.0.1
ip route 188.85.0.3 255.255.255.255 188.87.0.1
ip route 188.0.86.3 255.255.255.255 188.0.82.1
ip route 188.85.0.4 255.255.255.255 188.87.0.1
ip route 225.1.1.12 255.255.255.255 188.87.0.1
```

```
ip route 239.1.1.12 255.255.255.255 188.87.0.1
ip route 239.1.1.14 255.255.255.255 188.87.0.1
ip route 224.0.0.22 255.255.255.255 188.87.0.1
!
!
!
ntp server 171.68.10.150
ntp server 171.68.10.80
!
!
!
!
!
!
!
!
!
!
rule enable
!
!
!
!
!
movie-streamer enable
movie-streamer max-concurrent-sessions 10000
movie-streamer advanced client idle-timeout 0
movie-streamer advanced client rtp-timeout 0
bitrate movie-streamer outgoing 6000000
bitrate movie-streamer incoming 6000000
!
rtsp advanced max-request-rate 1000
wmt max-concurrent-sessions 14000
wmt cache min-ttl 1
wmt cache max-ttl days 3
wmt advanced client idle-timeout 300
wmt advanced server inactivity-timeout 300
wmt transaction-logs format extended wms-90
!
username admin password 1 $5$bVz2jc/k$QYvCAKrBmq3YqM5IklvuGrXQACMelfON
dq3/siTpqV8
username admin privilege 15
!
snmp-server enable traps config
snmp-server enable traps service-engine disk-fail
snmp-server enable traps alarm raise-critical
snmp-server enable traps alarm clear-critical
snmp-server enable traps alarm raise-major
snmp-server enable traps alarm clear-major
snmp-server enable traps alarm raise-minor
snmp-server enable traps alarm clear-minor
snmp-server enable traps entity
snmp-server enable traps snmp cold-start
snmp-server host 188.0.84.6 telstra v2c
snmp-server group telstra v2c read telstra notify telstra
snmp-server community telstra
!
!
!
tacacs key ****
tacacs password ascii
tacacs host 188.0.84.5 primary
!
!
```

```
aaa authentication login local secondary
aaa authentication login tacacs+ primary
aaa authorization exec local secondary
aaa authorization exec tacacs+ primary
!
ftp enable
!
telnet enable
!
!
!
!
!
!
!
cdsm ip 188.0.86.3
cms enable
!
cms database maintenance regular schedule every-day at 04:00
cms database maintenance full schedule Sun  at 04:00
!
kernel kdb
disk error-handling reload
!
banner enable
!
bandwidth wmt outgoing 6000000 default
bandwidth wmt outgoing 6000000 max-bandwidth
bandwidth wmt incoming 6000000 default
bandwidth wmt incoming 6000000 max-bandwidth
bandwidth movie-streamer outgoing 6000000 default
bandwidth movie-streamer outgoing 6000000 max-bandwidth
bandwidth movie-streamer incoming 6000000 default
bandwidth movie-streamer incoming 6000000 max-bandwidth
!
url-signature key-id-owner  1 key-id-number  1 key ****
url-signature key-id-owner  2 key-id-number  2 key ****
!
!
!
!
!
!
!
!
contentmgr disk-bucket-fail-threshold 1
!
! End of CDS configuration
ServiceEngine#
```

Related Commands

Command	Description
configure	Enters Global configuration mode.
copy	Copies the configuration or image data from a source to a destination.

show service-router

To display the Service Router configuration, use the **show service-router** command in EXEC configuration mode.

On the SE:

show service-router {**keepalive-interval** | **service-monitor**}

On the SR:

show service-router {**access-policy** | **content-based-routing** | **forwarding** [**content-origin** *content_origin*] | **lastresort** [**domain** *name*] | **load** {**all** | **sename** *sename*} | **location-based-routing** | **memory** | **proximity-based-routing** {**cache ip** *ip_address*} | **redirect-burst-control** | **redirect-mode** | **routes** [**content-origin** *content_origin* **ip-address** *ip_address*] | **service-monitor** | **services** {**all** | **sename** *se_name*} | **subscribe domain** | **summary** [**content-origin** *content_origin*]}

On the CDSM:

show service-router service-monitor

Syntax Description

access-policy	Configures the service-router access-policy.
content-based-routing	Displays the content-based routing configuration.
forwarding	Displays the content origin forwarding tables.
content-origin	(Optional) Displays information for one content origin.
content_origin	Content origin FQDN[1].
lastresort	Displays the domain and alternate domain configured.
domain	(Optional) Displays information for one domain.
name	Domain name.
load	Displays the load and threshold reached status.
all	Displays for all SEs.
sename	Displays for one SE.
se_name	SE name.
location-based-routing	Displays the location-based routing configurations.
memory	Displays details on malloc-related memory usage for the SR process.
proximity-based-routing	Displays the proximity-based routing configurations.
cache	(Optional) Displays proximity-based routing cache information.
ip	Displays one IP address or subnet.
ip_address	Client IP address or subnet of the proximity cache information to be displayed.
redirect-burst-control	Displays the redirect burst control configurations.
redirect-mode	Displays the redirect-mode configurations.
routes	Displays the content origin routing tables.

service-monitor	Displays the service monitor configuration.
services	Displays the services status.
subscribe	Displays the subscribe list.
domain	Displays the domain names.
summary	Displays the content origin routing table summary statistics.
keepalive-interval	Displays the keepalive interval.

1. FQDN = fully qualified domain name

Command Defaults

content-based-routing: disabled

Command Modes

EXEC configuration mode.

Usage Guidelines

This command allows users to check the Service Router-releated configuration. Through this command, users can view the configured features of an SR, such as location-based routing and content-based routing.

The **show service-router content-based-routing** command displays the content aware routing configuration for every content-origin. This command displays whether the universal content based routing is enabled or disabled, the content redundant copy number, and whether the content based routing has been disabled for any particular domain.

Note The Load percentage displayed in the Average Device Load field when the **show service-router service-monitor** command is executed on the SE is the maximum of the average disk load/average CPU load given both CPU and disk monitoring are enabled on the SE.

The memory usage is calculated in the **show service-router service-monitor** command as follows:

Total used memory = total memory - (total free memory + total buffer memory + total cache memory) + total pinned memory. The percentage of total used memory = (total used memory)/total memory.

The total memory, total free memory, total buffer memory, and total cache memory are obtained from /proc/meminfo. The total pinned memory is obtained from /proc/ukse/ukse_prefetch_details.

The **show service-router content-origin <content-origin> ip-address <client-ip>** command is only used to check which SE the request is routed to based on the network entries and metrics configured in the coverage zone file. It does not take into account the service status of the SEs because there is no protocol or filename in the input. Also, it does not take into account matches from location based routing and proximity based routing.

The **show service-router content-origin <content-origin>** output shows an SE as overloaded only if the device load has exceeded thresholds. The SE does not show as overloaded because there might be other Protocol Engines in the SE that are still able to serve requests.

Examples

The following example shows how to display SR routing statistics:

```
ServiceRouter# show statistics service-router all | begin "SR Routing Statistics"
----- SR Routing Statistics -----
    Network Redirects         :                 0
```

```
    Proximity Redirects       :                 2
    Geo Location Redirects    :                 0
    Zero Network Redirects    :                 0
    Last Resort Redirects     :                 0
----- SR Proximity Routing Statistics -----
    Cache Hits                :                 1
    Cache Misses              :                 1
    Errors                    :                 0
```

The following example shows how to display the content aware routing configuration for every content-origin:

```
ServiceRouter# show service-router content-based-routing
Content based routing is enabled globally
Content redundant copy 1
Content based routing is disabled for vod.cds.com
Content based routing is disabled for kse.mem
Content based routing is disabled for kse.vod.cds.com
```

The following example shows how to display the proximity routing information on an SR:

```
ServiceRouter# sh service-router proximity-based-routing
Proximity based routing is enabled
Proximity cache timeout 600 seconds
service-router proximity-based-routing proximity-server 127.0.0.1
```

The following example shows how to display the proximity routing cache information on an SR:

```
ServiceRouter# show service-router proximity-based-routing cache ip 171.XX.XXX.XXX

----- Proximity cache information for 171.XX.XXX.XXX -----
Cached proximity information on Fri Jul 30 05:19:50 2010

   SE Name: XX-CDE220-Fiber
   Rating : 3758096385

   SE Name: XX-CDE250-CE-2
   Rating : 3758096385

   SE Name: XXXX-SR
   Rating : 3758096385

   SE Name: XXX-CDE220-1
   Rating : 3758096385

   SE Name: XXX-CDE250-2
   Rating : 3758096385

   SE Name: XX-CDE420-1
   Rating : 3758096385

   SE Name: XXX-CDE420-1
   Rating : 3758096385
```

The following example shows how to display 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         : 90%
FMS         : 90%
MS          : 90%
NIC         : 90%
BURST COUNT : 1
DISK        : 80%
DISKFAILCNT : 1

Sample periods configured:
--------------------------
CPU  : 1 (secs)
MEM  : 1 (secs)
KMEM : 1 (secs)
WMT  : 1 (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  : 2
FMS  : 2
NIC  : 2
DISK : 2

Device Status
-------------

CPU
Current load          : 35%
Average load          : 35%
Threshold             : Not reached

DISK
Current load          : 20%
Average load          : 20%
Threshold             : Not reached
Status                : Operational

MEM
Average Used Memory   : 10%
Threshold             : Not reached

KMEM
Average Kernel Memory : 1%
Threshold             : Not reached

NIC
Interface             : PortChannel 1/0
Average BW In         : 9%
Average BW Out        : 9%
Threshold             : Not reached

Average Device load   : 35%

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 shows how to display the Service Router information on the CDSM:

```
CDSM# show service-router service-monitor
Alarm types configured:
-------------------------

AUGMENTATION ALARM : Disabled

Monitor types configured:
-------------------------
CPU,MEM,KMEM,DISK

Threshold values configured:
---------------------------
CPU         : 80%
MEM         : 80%
KMEM        : 50%
DISK        : 80%
DISKFAILCNT : 75%
AUGMENTATION: 80%

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

Device Status
-------------

CPU
Current load          : 1%
Average load          : 1%
Threshold             : Not reached

DISK
Current load              : 1%
Average load              : 0%
Load Threshold            : Not reached
```

```
Disk Fail Cnt Threshold    : Not reached

MEM
Average Used Memory   : 6%
Threshold             : Not reached

KMEM
Average Kernel Memory : 0%
Threshold             : Not reached


Average Device load   : 1%

CDSM#
```

The following example shows how to display the domains to which the SR is subscribed:

```
ServiceRouter# show service-router subscribe domain
Domains subscribed:
    test1.com
    test5.com
    test4.com
    test3.com
```

Related Commands

Command	Description
service-router	Configures service routing.
clear service-router	Clears the proximity-based routing proximity cache.

show services

To display services-related information, use the **show services** command in EXEC configuration mode.

show services {**ports** [*port_num*] | **summary**}

Syntax Description

ports	Displays services by port number.
port_num	(Optional) Displays up to eight port numbers. The port number range is from 1 to 65535.
summary	Displays the services summary.

Command Defaults

None

Command Modes

EXEC configuration mode.

Examples

The following example shows how to display 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 shows how to display 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
             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** command in EXEC configuration mode.

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.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

This command provides information on various SNMP variables and statistics on SNMP operations.

Table 3-64 describes the fields shown in the **snmp alarm-history** display.

Table 3-64 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 3-65 to map module names to module IDs.
Category	Traps sent by an CDS device contain numeric category IDs. See Table 3-66 to map category names to category IDs.
Descr	Description of the Internet Streamer CDS software alarm and the application that generated the alarm.

Table 3-65 describes the mapping of module names to module IDs.

Table 3-65 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 3-66 describes the mapping of category names to category IDs.

Table 3-66 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 3-67 describes the fields shown in the **show snmp stats** display.

Table 3-67 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.

Table 3-67 show snmp stats Field Descriptions (continued)

Field	Description
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.
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 3-68 describes the fields shown in the **show snmp engineID** display.

Table 3-68 show snmp engineID Field Descriptions

Field	Description
Local SNMP Engine ID	String that identifies the copy of SNMP on the local device.

Table 3-69 describes the fields shown in the **show snmp group** display.

Table 3-69 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 3-70 describes the fields shown in the **show snmp user** display.

Table 3-70 show snmp user Field Descriptions

Field	Description
User name	String identifying the name of the SNMP user.
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

Command	Description
snmp-server community	Configures the community access string to permit access to the SNMP[1].
snmp-server contact	Sets the system server contact (sysContact) string.
snmp-server enable traps	Enables the SE to send SNMP traps.
snmp-server group	Defines a user security model group.
snmp-server host	Specifies the recipient of a host SNMP trap operation.
snmp-server location	Sets the SNMP system location string.
snmp-server notify inform	Configures the SNMP notify inform request.
snmp-server user	Defines a user who can access the SNMP server.
snmp-server view	Defines a SNMP V2 MIB view.

1. SNMP = Simple Network Management Protocol

show srp database

To display the descriptor-related information saved in the descriptor database, use the **show srp database** command in privileged EXEC configuration mode.

show srp database [*key* | **active** | **brief** | **content** | **expired** | **group** | **statistics** | **maincontent** *target_string* | **record** *key target_string* | **service** | **size** *low high* | **subid** *key target_string* | **update** *start end*]

Syntax Description

key	(Optional) DHT key in hexadecimal format that identifies a descriptor to be fetched from the descriptor database,
active	(Optional) Displays the database active entries.
brief	(Optional) Displays brief information for each descriptor in the database, including DHT key, Type, Entity Type, Size, and initial part of the Element Data in Element 0 of the descriptor.
content	(Optional) Filters the descriptor database to display content-type descriptors only.
expired	(Optional) Displays the database expired entries.
group	(Optional) Filters the descriptor database to display group-type (multicast group) descriptors only.
maincontent *target_string*	(Optional) Filters the descriptor database to display descriptors whose Element data field in the main element (Element 0) contains *target_string*.
record *key target_string*	(Optional) In a given descriptor identified by *key*, finds elements whose resource record contains *target_string*.
service	(Optional) Filters the descriptor database to display service-type descriptors only.
size *low high*	(Optional) Filters the descriptor database to display descriptors whose size (in bytes) is no larger than *high* and no smaller than *low*.
statistics	(Optional) Displays the total number of entries in the database.
subid *key target_string*	(Optional) In a given descriptor identified by *key*, finds elements whose sub ID (Element ID) contains the *target_string*.
update *start end*	(Optional) Filters the descriptor database to display descriptors that were updated no earlier than *start* and no later than *end*. Format for *start* and *end* is: *month_date_hour*:*minute*:*second_year*. For example: Sep_8_08:54:55_2007.

Command Defaults

None

Command Modes

Privileged EXEC configuration mode.

Usage Guidelines

This command displays information saved in the descriptor database and filters the data based on the argument that is specified. Without specifying any key or argument, it displays a summary of the descriptor database, which contains the DHT key and size for each descriptor and the total number of active descriptors in the database.

By providing the DHT key in hexadecimal format or various filtering arguments, **show srp database** filters through the descriptor database or a particular descriptor to obtain the desired information. Keys with less than 64 hexadecimal characters are appended with zeroes.

In filtering arguments that have a target string, the specified string is case sensitive.

Examples

The following examples show the output **show srp database** displays with and without a DHT key and the optional filtering arguments that specify how to query the database to obtain desired information. All the examples are based on querying the same descriptor database.

The following example is sample output from the **show srp database** command when it is issued with no keywords or arguments.

```
ServiceRouter# show srp database

DHT KEY                                                                 : SIZE
0a1405495f14dfc1d6fd10b93d957903456166d3b7b883b9047fb89cbecb5157: 1054
1230000000000000000000000000000000000000000000000000000000000000000000: DELETED
15136e3cfb5c3de3c4258d5c16c1bbabc5ddb538b51b32bdc1ebbd9bcb75b6d7: 838
2340000000000000000000000000000000000000000000000000000000000000000000: 168
3392b8bfe67c12c326aa346bdff1e83ac6286e397ce0013f8c4a33fc4dc5abda: 1065
352a5e7e0e3dd9b78ab18fdb4408191f8418439b3ffef79f9b0698b8a73c16bc: 853
39da9f8b45b6a186fdfdb6eec44ab71e7510c1de7b1b049df7c971696cb398a0: 1074
4e346a0c197a6e1e69650badd1687557dc4d9b80789407a9b452eda761f1056e: 1056
4f9400b0372d934d5819f3e88f4ad5be2177e96b79ee34aca49722e2db9ff300: 1102
7770000000000000000000000000000000000000000000000000000000000000000000: 129
7890000000000000000000000000000000000000000000000000000000000000000000: 109
8880000000000000000000000000000000000000000000000000000000000000000000: 167
8d3e7478a3685decd322f891ea5a09a6b264097ab166d5b7bedd5ad9715f1401: 1048
9990000000000000000000000000000000000000000000000000000000000000000000: 183
a6c4ef5b73c5b5621567946e7691b3d1123f9a3cf8b28ce29a075bfa41cb21ad: 1068
c1898f9a8b69c3912f0fe8fecac30818fab24385fa8a1d37a8ffd193cf3eeebc: 324
c53126d4113799d7f300c6accf526423756efa5e007fc3cc16fe45a9c8c06ee3: 881
ca1329d38687cdd5f8ab7aabe4333ee7883a6a28f7e8b03e11d58bb3f4c39988: 1057
cbb037edbe196fbf8d0f5bfa6e629ff1242483f5f5450719748189cf9d7b1fa4: 1086
e50dc5cca2b736d00c41506b754c7bd331ab38826a4df396f6343a81e5631832: 843
e8ca53dbcf748505194a10c9b6fa1549f309345f19b4d4df920be79d5e986471: 1083
f47ec4f84068b9fda926f4767d2219f4faeabbbb0738312f70917504a0c8c9b9: 863

Total                         21 active item(s) in the database

ServiceRouter#
```

The preceding example shows that there are 22 entries in the database, of which 21 are active ones. If a descriptor is active (has not been deleted), then its size is displayed. Otherwise, DELETED is displayed in the SIZE field of the descriptor. If the descriptor database is empty, the following output is displayed:

```
ServiceRouter# show srp database

DHT   KEY                                                         : SIZE
Total                                  0 active item(s) in the database

ServiceRouter#
```

The following is sample output from the **show srp database** *key* command where the DHT key is 234:

```
ServiceRouter# show srp database 234

Getting database entry for
234

Entity key:
234000000000000000000000000000000000000000000000000000000000000000
Entity rec type:          101     Entity total length: 168
Entity type:         5783093e     Entity flags:        0
--------------- Element 0        (main)-----------------
Element ID: main
  Element total len          45   ID len:      0
  Delete Time: 47af31d505d8fb77
  Flags  8
  Last Update: Sun Feb 10 17:18:34 2008 (47af31ea077ac2e7)
  Expiration : Tue Mar 11 17:18:34 2008 (47d6beea077a0000)
  Element data len:           5
  Element data:
test
--------------- Element 1        (comp)-----------------
Element ID: "123"(313233)
  Element total len          51   ID len:      3
  Last Update: Sun Feb 10 17:24:40 2008 (47af335826c5288f)
  Expiration : Sun Feb 10 17:29:40 2008 (47af348426c50000)
  Element data len:           8
  Element data:

testing

ServiceRouter#
```

In the preceding example, the output is detailed information saved for the descriptor 234:

- Descriptor 234 has a record type 101.
- Its entity type is 5783093e, which means this descriptor (234) is a service-type descriptor.
- Its total length is 168 bytes.
- It has zero Entity flags. Entity flags are not currently used.
- It has two elements:
  - Element ID main is for the descriptor itself. The descriptor's name is test.
  - Element ID 123 is for a resource (testing) that has been added to the descriptor.

The following is sample output from **show srp database** *key* command where the DHT key is 123. In this example, the entity specified by the key has been deleted.:

```
ServiceRouter# show srp database 123

Getting database entry for
123
Entity key:
123000000000000000000000000000000000000000000000000000000000000000
Entity was DELETED on (47b1fabdd076fba7) Tue Feb 12 19:59:57 2008

ServiceRouter#
```

The following is abbreviated sample output from the **show srp database** command when it is issued with the optional argument **brief**:

```
ServiceRouter# show srp database brief

Key: 0a1405495f14dfc1d6fd10b93d957903456166d3b7b883b9047fb89cbecb5157
 Type: Regular  Entity Type: Service     Size:     1054
 Body: <Service xmlns="urn:topos:descriptor:xml
Key: 0a1405495f14dfc1d6fd10b93d957903456166d3b7b883b9047fb89cbecb5157
 Type: Regular  Entity Type: Service     Size:     1054
 Body: <Service xmlns="urn:topos:descriptor:xml

... Output omitted

Key: 777000000000000000000000000000000000000000000000000000000000000000000000
 Type: Mcast Cmd        Entity Type: Group       Size:      129
 Body: ..................test.
Key: 789000000000000000000000000000000000000000000000000000000000000000000000
 Type: Regular  Entity Type: Group       Size:      109
 Body: test.
Key: 888000000000000000000000000000000000000000000000000000000000000000000000
 Type: Regular  Entity Type: Unknown(0)  Size:      167
 Body: test

... Output omitted

Total                        21 active item(s) in the database

ServiceRouter#
```

In the preceding example, **show srp database brief** displays brief information for each descriptor in the database, including DHT key, Type, Entity Type, Size, and Body (the initial part of the Element Data in Element 0 of the descriptor). The Body contains different information, depending on the type of the descriptor displayed.

- By default, Body contains the first 40 printable characters of the main element data.
- If the descriptor is a service type descriptor, Body contains the service name information.

The following is sample output from the **show srp database** command when it is issued with the filtering argument **content**. There are no content-type descriptors in the database:

```
ServiceRouter# show srp database content

Total      0 content type descriptor(s) in the database

ServiceRouter#
```

The following is sample output from the **show srp database** command when it is issued with the filtering argument **service**. There are 16 service-type descriptors in the database:

```
ServiceRouter# show srp database service

0a1405495f14dfc1d6fd10b93d957903456166d3b7b883b9047fb89cbecb5157: Size: 1054
15136e3cfb5c3de3c4258d5c16c1bbabc5ddb538b51b32bdc1ebbd9bcb75b6d7: Size: 838
234000000000000000000000000000000000000000000000000000000000000000000000: Size: 168
3392b8bfe67c12c326aa346bdff1e83ac6286e397ce0013f8c4a33fc4dc5abda: Size: 1065
352a5e7e0e3dd9b78ab18fdb4408191f8418439b3ffef79f9b0698b8a73c16bc: Size: 853
39da9f8b45b6a186fdfdb6eec44ab71e7510c1de7b1b049df7c971696cb398a0: Size: 1074
4e346a0c197a6e1e69650badd1687557dc4d9b80789407a9b452eda761f1056e: Size: 1056
4f9400b0372d934d5819f3e88f4ad5be2177e96b79ee34aca49722e2db9ff300: Size: 1102
8d3e7478a3685decd322f891ea5a09a6b264097ab166d5b7bedd5ad9715f1401: Size: 1048
a6c4ef5b73c5b5621567946e7691b3d1123f9a3cf8b28ce29a075bfa41cb21ad: Size: 1068
c53126d4113799d7f300c6accf526423756efa5e007fc3cc16fe45a9c8c06ee3: Size: 881
```

```
ca1329d38687cdd5f8ab7aabe4333ee7883a6a28f7e8b03e11d58bb3f4c39988: Size: 1057
cbb037edbe196fbf8d0f5bfa6e629ff1242483f5f5450719748189cf9d7b1fa4: Size: 1086
e50dc5cca2b736d00c41506b754c7bd331ab38826a4df396f6343a81e5631832: Size: 843
e8ca53dbcf748505194a10c9b6fa1549f309345f19b4d4df920be79d5e986471: Size: 1083
f47ec4f84068b9fda926f4767d2219f4faeabbbb0738312f70917504a0c8c9b9: Size: 863
 Total     16 service type descriptor(s) in the database

ServiceRouter#
```

The following is sample output from the **show srp database** command when it is issued with the filtering argument **group**. There are three group-type descriptors in the database:

```
ServiceRouter# show srp database group

77700000000000000000000000000000000000000000000000000000000000000000: Size: 393
99900000000000000000000000000000000000000000000000000000000000000000: Size: 307
c1898f9a8b69c3912f0fe8fecac30818fab24385fa8a1d37a8ffd193cf3eeebc: Size: 124
 Total      3 group type descriptor(s) in the database

ServiceRouter#
```

The following is sample output from the **show srp database** command when it is issued with the option **statistics**. The output indicates how many descriptors (including deleted ones) exist in the descriptor database:

```
ServiceRouter# show srp database statistics

  Total number of descriptors = 22

ServiceRouter#
```

The following is sample output from the **show srp database** command when it is issued with the filtering argument **maincontent** and the target string **service**. The sample output indicates that there are 15 descriptors in the database whose main content (that is, the Element Data field of Element 0) contains the target string service:

```
ServiceRouter# show srp database maincontent service

0a1405495f14dfc1d6fd10b93d957903456166d3b7b883b9047fb89cbecb5157: Type: 101
  Rec Type: 5783093e Size: 1054
15136e3cfb5c3de3c4258d5c16c1bbabc5ddb538b51b32bdc1ebbd9bcb75b6d7: Type: 101
  Rec Type: 5783093e Size: 838
3392b8bfe67c12c326aa346bdff1e83ac6286e397ce0013f8c4a33fc4dc5abda: Type: 101
  Rec Type: 5783093e Size: 1065
352a5e7e0e3dd9b78ab18fdb4408191f8418439b3ffef79f9b0698b8a73c16bc: Type: 101
  Rec Type: 5783093e Size: 853
39da9f8b45b6a186fdfdb6eec44ab71e7510c1de7b1b049df7c971696cb398a0: Type: 101
  Rec Type: 5783093e Size: 1074
4e346a0c197a6e1e69650badd1687557dc4d9b80789407a9b452eda761f1056e: Type: 101
  Rec Type: 5783093e Size: 1056
4f9400b0372d934d5819f3e88f4ad5be2177e96b79ee34aca49722e2db9ff300: Type: 101
  Rec Type: 5783093e Size: 1102
8d3e7478a3685decd322f891ea5a09a6b264097ab166d5b7bedd5ad9715f1401: Type: 101
  Rec Type: 5783093e Size: 1048
a6c4ef5b73c5b5621567946e7691b3d1123f9a3cf8b28ce29a075bfa41cb21ad: Type: 101
  Rec Type: 5783093e Size: 1068
c53126d4113799d7f300c6accf526423756efa5e007fc3cc16fe45a9c8c06ee3: Type: 101
  Rec Type: 5783093e Size: 881
ca1329d38687cdd5f8ab7aabe4333ee7883a6a28f7e8b03e11d58bb3f4c39988: Type: 101
  Rec Type: 5783093e Size: 1057
cbb037edbe196fbf8d0f5bfa6e629ff1242483f5f5450719748189cf9d7b1fa4: Type: 101
  Rec Type: 5783093e Size: 1086
e50dc5cca2b736d00c41506b754c7bd331ab38826a4df396f6343a81e5631832: Type: 101
```

```
  Rec Type: 5783093e Size: 843
e8ca53dbcf748505194a10c9b6fa1549f309345f19b4d4df920be79d5e986471: Type: 101
  Rec Type: 5783093e Size: 1083
f47ec4f84068b9fda926f4767d2219f4faeabbbb0738312f70917504a0c8c9b9: Type: 101
  Rec Type: 5783093e Size: 863

Total 15 item(s) in the database whose main content contains
'service'

ServiceRouter#
```

The following is sample output from the **show srp database** command when it is issued with the filtering argument **record** to search in a descriptor specified by the key 999 to locate records containing the target string **test**. The examples are in the following order:

- Descriptor for a record where the target string is found.
- Descriptor for a record where the entity has been deleted.
- Descriptor for a record where the target string is not found.

```
ServiceRouter# show srp database record 999 test

Entity key:
999000000000000000000000000000000000000000000000000000000000000000000000
Entity rec type:          101     Entity total length: 183
Entity type:         22222222     Entity flags:        0
--------------- Element 1        (comp)-------4----------
Element ID: "123"(313233)
  Element total len          47   ID len:      3
  Last Update: Tue Feb 12 02:07:38 2008 (47b0ff6ae5e0497b)
  Expiration : Thu Mar 13 02:07:38 2008 (47d88c6ae5e00000)
  Element data len:           4
  Element data:
test

ServiceRouter# show srp database record 123 test
Entity key:
123000000000000000000000000000000000000000000000000000000000000000000000
Entity was DELETED on (47b1fabdd076fba7) Tue Feb 12 19:59:57 2008

ServiceRouter# show srp database record 777 test
Entity key:
777000000000000000000000000000000000000000000000000000000000000000000000
Entity rec type:          102     Entity total length: 129
Entity type:         22222222     Entity flags:        0
There is no resource record containing test

ServiceRouter#
```

The following is sample output from the **show srp database** command when it is issued with the filtering argument **size** to select descriptors whose size is in the given range. This example shows that, for the active descriptors, there are five descriptors whose size is larger than 100 bytes and smaller than 300 bytes:

```
ServiceRouter# show srp database size 100 300

234000000000000000000000000000000000000000000000000000000000000000000000: Type: 101
  Rec Type: 5783093e Size: 168
777000000000000000000000000000000000000000000000000000000000000000000000: Type: 102
  Rec Type: 22222222 Size: 129
789000000000000000000000000000000000000000000000000000000000000000000000: Type: 101
  Rec Type: 22222222 Size: 109
888000000000000000000000000000000000000000000000000000000000000000000000: Type: 101
```

```
  Rec Type:        0 Size: 167
999000000000000000000000000000000000000000000000000000000000000000000000: Type: 101
  Rec Type: 22222222 Size: 183

Total     5 item(s) in the database whose size is between 100 and 300

ServiceRouter#
```

The following example is sample output from the **show srp database** command when it is issued with the filtering argument **subid** to search for elements in a given descriptor whose Element ID contains the given target string. In this example, the search is in the descriptor whose key is 999 and for elements whose sub ID (Element ID) is 123. The output indicates one element, Element 1, with the specified Element ID 123.

```
ServiceRouter# show srp database subid 999 123

Entity key:
999000000000000000000000000000000000000000000000000000000000000000000000
Entity rec type:          101     Entity total length: 183
Entity type:         22222222     Entity flags:        0
--------------- Element 1        (comp)-----------------
Element ID: "123"(313233)
  Element total len          47   ID len:      3
  Last Update: Tue Feb 12 02:07:38 2008 (47b0ff6ae5e0497b)
  Expiration : Thu Mar 13 02:07:38 2008 (47d88c6ae5e00000)
  Element data len:           4
  Element data:
test

ServiceRouter#
```

The following example is sample output from the **show srp database** command when it is issued with the filtering argument **update** to select descriptors that have been updated in the specified time range. The command uses the Last Update field of Element 0 to determine when the descriptor has been updated. The sample output indicates that four descriptors have been updated in the specific time range.

```
ServiceRouter# show srp database update Feb_11_02:07:38_2008 Feb_12_02:07:38_2009

777000000000000000000000000000000000000000000000000000000000000000000000: Type: 102
  Rec Type: 22222222 Size: 129
888000000000000000000000000000000000000000000000000000000000000000000000: Type: 101
  Rec Type:        0 Size: 167
999000000000000000000000000000000000000000000000000000000000000000000000: Type: 101
  Rec Type: 22222222 Size: 183
c1898f9a8b69c3912f0fe8fecac30818fab24385fa8a1d37a8ffd193cf3eeebc: Type: 102
  Rec Type: 22222222 Size: 324

Total 4 active item(s) in the database updated in the specified time duration

ServiceRouter#
```

Related Commands

Command	Description
clear srp descriptor	Deletes a single descriptor or all descriptors in the descriptor database.
show srp multicast database	Displays multicast database information for an SRP process

show srp leafset

To display SRP leafset information, use the **show srp leafset** command in privileged EXEC configuration mode.

show srp leafset

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

Privileged EXEC configuration mode.

Usage Guidelines

This command displays leafset information for the current Proximity Engine (the local node). The current Proximity Engine must be part of a properly configured DHT network for leafset information about network members to be displayed.

Examples

The following example shows the output from **show srp leafset** when the current Proximity Engine is a standalone node and not a member of a DHT network:

```
ServiceRouter# show srp leafset

Codes: T - local node, L - leafset, P - primary, S - secondary, B - backup
       I - Intransitive, W - wrapped

Leafset count: total 5, left 2, right 2

T    d2fc632c53c9ff1de8683e265386b09502791aedd65f28025fe7f64ad8cab2d9
    via sn-sj87 [ 172.20.168.87 ] :9000

ServiceRouter#
```

Table 3-71 describes the codes that **show srp leafset** uses in its output.

Table 3-71 Designations for Leafset Nodes

Code	Leafset Node Designation
T—local node	Proximity Engine where **show srp leafset** is issued.
L—leafset	Member of the leafset.
P—primary	Primary routing entry.
S—secondary	Secondary routing entry.
B—backup	Backup routing entry.
I—Intransitive	Intransitive routing entry.
W—wrapped	Wrapped routing entry.

The following example shows the output from **show srp leafset** command when the current Proximity Engine is a member of a DHT network consisting of seven nodes: the local node in the middle, three nodes on the left, and three nodes on the right.

```
ServiceRouter# show srp leafset

Codes: T - local node, L - leafset, P - primary, S - secondary, B - backup
       I - Intransitive, W - wrapped
Leafset count: total 7, left 3, right 3
WPL  0e33b4fc00ea5e32b7323c2a712cc226fe4990430df6ac9a05d2a87ab67c9fae
    via sn-sj43 [ 172.20.168.43, 192.168.20.10, 192.168.86.10 ] :9000,
1.772254 ms, 00:00:08
PL   b5ca21563f5b938e46e2cb8f33a148ae00a1f6666f2a5eb735b7ed90c012c882
    via sn-sj82 [ 172.20.168.82, 192.168.82.82, 192.168.86.82 ] :9000,
0.392633 ms, 00:00:08
PL   c89908f53cc3ab6bc6065fd545341e9868cab7dcf852eaa346dd470011fcff1d
    via sn-sj89 [ 172.20.168.89 ] :9000, 0.352768 ms, 00:00:08
T    e966a1daec3ef3f1a81fec0e46338ae66eb7d154341e3a20fef0c5d2e8a0aabf
    via sn-sj87 [ 172.20.168.87 ] :9000
PL   0e33b4fc00ea5e32b7323c2a712cc226fe4990430df6ac9a05d2a87ab67c9fae
    via sn-sj43 [ 172.20.168.43, 192.168.20.10, 192.168.86.10 ] :9000,
1.772254 ms, 00:00:08
WPL  b5ca21563f5b938e46e2cb8f33a148ae00a1f6666f2a5eb735b7ed90c012c882
    via sn-sj82 [ 172.20.168.82, 192.168.82.82, 192.168.86.82 ] :9000,
0.392633 ms, 00:00:08
WPL  c89908f53cc3ab6bc6065fd545341e9868cab7dcf852eaa346dd470011fcff1d
    via sn-sj89 [ 172.20.168.89 ] :9000, 0.352768 ms, 00:00:08

ServiceRouter#
```

Related Commands

Command	Description
bootstrap-node	Configures a bootstrap node IP address.
domain	Sets the domain ID for the SRP.

show srp memory

To display SRP memory usage information, use the **show srp memory** command in privileged EXEC configuration mode.

show srp memory

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

Privileged EXEC configuration mode.

Usage Guidelines

This command displays SRP memory usage information.

Examples

The following example shows the output from **show srp memory** command:

```
ServiceRouter# show srp memory

SRP memory usage:
Type             Size      Count        HWM       Slab   Overhead      Total
Packet          65536          2          0          0          0     131072
Operation         192         92          0          0          0      18566
Sync              120          0          0          0          0          0
Pending           104          0          0          0          0          0
Mcast Pend         40          0          0          0          0          0
Proximity         104          0          0          0          0          0
To IPPC           208          0          0          0          0          0
Neighbor          384          2          2        128      48560      49328
Neighbor EP       134          0          0          0        128        128
Timer CTX          16         16         16         64        944       1200
Packet Addr        32          0          2          0        128        128
Subscriber        240          2          2         64      15056      15536
Seq Req            88          0          0          0        128        128
WorkQ              32          0          0          0        128        128
Total:                                                     65072     216214

ServiceRouter#
```

Related Commands

Command	Description
show srp process	Displays the basic configurations for SRP.

show srp multicast database

To display multicast database information for an SRP process, use the **show srp multicast database** command in privileged EXEC configuration mode.

show srp multicast database [*group_id* | **brief** | **statistics**]

Syntax Description

group_id	DHT key in hexadecimal format that identifies a group descriptor to be fetched from the multicast database.
brief	Displays brief information for each group descriptor in the database, including the DHT key, Type, Entity Type, Size, and the initial part of the Element Data in Element 0 of the descriptor.
statistics	Displays the number of entries (including deleted entries) in the multicast database.

Command Defaults

None

Command Modes

Privileged EXEC configuration mode.

Usage Guidelines

This command is used to display information saved in the multicast database. Without specifying any key or argument, **show srp multicast database** displays a summary of the multicast database. The summary contains the DHT key and size for each descriptor and the total number of active group descriptors in the database. By providing the DHT key in hexadecimal format or various filtering arguments, you can filter through the multicast database or a particular group descriptor to obtain desired information.

Examples

The following example is sample output from the **show srp multicast database** command when it is issued with no keywords or arguments:

```
ServiceRouter# show srp multicast database

DHT KEY                                                                 : SIZE
12300000000000000000000000000000000000000000000000000000000000000000: 1003
44440000000000000000000000000000000000000000000000000000000000000000: 522
77700000000000000000000000000000000000000000000000000000000000000000: 523
99900000000000000000000000000000000000000000000000000000000000000000: 307
c1898f9a8b69c3912f0fe8fecac30818fab24385fa8a1d37a8ffd193cf3eeebc: 124
Total                        5 active item(s) in the database

ServiceRouter#
```

The preceding example shows that there are five active entries in the database. If a descriptor is active (has not been deleted), its size is displayed. If a descriptor has been deleted, DELETED is displayed in the SIZE field of the descriptor. If the descriptor database is empty, the following output is displayed:

```
ServiceRouter# show srp multicast database
```

```
DHT KEY                                                              : SIZE
Total                        0 active item(s) in the database

ServiceRouter#
```

The following is sample output from the **show srp multicast database** command when it is issued with the optional argument *group_id.* In this example, the DHT key for *group_id* is 4444:

```
ServiceRouter# show srp multicast database 4444

Getting database entry for
4444
Entity key:
4444000000000000000000000000000000000000000000000000000000000000
Entity rec type:          103     Entity total length: 522
Entity type:         22222222     Entity flags:        0
--------------- Element 0        (main)-----------------
Element ID: main
  Element total len          65   ID len:      0
  Delete Time: 0000000000000000
  Flags  0
  Last Update: Tue Feb 12 21:47:20 2008 (47b213e8ec98be67)
  Expiration : Thu Mar 13 21:47:20 2008 (47d9a0e8ec980000)
  Element data len:          25
  Element data:
    Content Acquirerquence number: 0
    Data: test
--------------- Element 1        (mcast)-----------------
Element ID: "....U.......(# .."(95160500550106090000000028230000)
  Element total len         123   ID len:      16
  Last Update: Tue Feb 12 21:48:14 2008 (47b2141e24526623)
  Expiration : Thu Mar 13 21:48:14 2008 (47d9a11e24520000)
  Element data len:          67
  Element data:
    Content Acquirerquence number: 1
    Sender ID: d2fc632c53c9ff1de8683e265386b09502791aedd65f28025fe7f64ad8cab2d9
    Data: hello1
--------------- Element 2        (mcast)-----------------
Element ID: "....r@......(# .."(9916050072401b1f0000000028230000)
  Element total len         123   ID len:      16
  Last Update: Tue Feb 12 21:48:18 2008 (47b214227ce17ea3)
  Expiration : Thu Mar 13 21:48:18 2008 (47d9a1227ce10000)
  Element data len:          67
  Element data:
    Content Acquirerquence number: 2
    Sender ID: d2fc632c53c9ff1de8683e265386b09502791aedd65f28025fe7f64ad8cab2d9
    Data: hello2
--------------- Element 3        (mcast)-----------------
Element ID: ".............(# .."(b0160500ae9e151c0000000028230000)
  Element total len         123   ID len:      16
  Last Update: Tue Feb 12 21:48:41 2008 (47b21439709c703b)
  Expiration : Thu Mar 13 21:48:41 2008 (47d9a139709c0000)
  Element data len:          67
  Element data:
    Content Acquirerquence number: 3
    Sender ID: d2fc632c53c9ff1de8683e265386b09502791aedd65f28025fe7f64ad8cab2d9
Data: hello3

ServiceRouter#
```

In the preceding example, the output is detailed information saved for the multicast group 4444 including the following:

- Multicast group 4444 has a record type 103.
- Its Entity Type is 22222222, which means this is a group-type descriptor.
- Its total length is 522 bytes.
- It has zero Entity Flags. Entity flags are not currently used.
- It has four elements:
  - Element 0 is the main element whose Element Data field saves group topic information instead of messages received by this group.
  - Other elements are created for saving messages received by the group.

Related Commands

Command	Description
clear srp group messages	Deletes all locally stored messages sent to a multicast group in the service routing layer.

show srp neighbor

To display SRP neighbor information, use the **show srp neighbor** command in privileged EXEC configuration mode.

show srp neighbor [**detail** | **down**]

Syntax Description

detail	Displays detailed information for each neighbor.
down	Displays the information of down neighbor entries.

Command Defaults

None

Command Modes

Privileged EXEC configuration mode.

Usage Guidelines

This command displays SRP neighbor information. The current Proximity Engine must be part of a properly configured DHT network for neighbor information about current network members to be displayed.

If the keyword **down** is specified, **show srp neighbor** displays down neighbors. These are Proximity Engines that are members of a DHT network the local Proximity Engine previously belonged to.

Examples

In the following example, assume a standalone Proximity Engine sn-sj87, and a two-node network consisting of Proximity Engine sn-sj81 and Proximity Engine sn-sj85. The **show srp neighbor** command is run from sn-sj87 before it is connected to the two-node network:

```
ServiceRouter# show srp neighbor

Codes: T - local node, L - leafset, P - primary, S - secondary, B - backup
       I - Intransitive, D - delay, H - hold time

Number of neighbors in the database: 0
```

In the preceding example, sn-sj87 does not have any neighbor in the database.

In the following example, after sn-sj87 is added to the network, **show srp neighbor** is issued again. From the following output, we can see that sn-sj87 has two neighbors, sn-sj81 and sn-sj85:

```
ServiceRouter# show srp neighbor

Codes: T - local node, L - leafset, P - primary, S - secondary, B - backup
       I - Intransitive, D - delay, H - hold time

Number of neighbors in the database: 2

PL  8886822171add71887d54107c266d814b605eaa0d5cc9b54b9160a137f4355d1
    via sn-sj81 [ 172.20.168.81 ] :9000, D=0.339605 ms,
    H=00:00:07
PL  9f752f56f347ca8fcc40a4e09b645f9b4c9b71c73401083f4c04920b30215b0a
via sn-sj85 [ 172.20.168.85, 192.168.20.85, 192.168.86.85 ] :9000,
D=0.379999 ms, H=00:00:09
```

To see details of these two neighbors, issue the **show srp neighbor detail** command:

```
ServiceRouter# show srp neighbor detail

Codes: T - local node, L - leafset, P - primary, S - secondary, B - backup
       I - Intransitive
       D - delay, H - hold time, U - up time
       S_SEQ - send seq no., R_SEQ - receive seq. no.
       S_SID - send session id, R_SID - receive session id,
       R_Q - Receive Queue, T_Q - Transmit Queue.
Number of neighbors in the database: 2
PL  8886822171add71887d54107c266d814b605eaa0d5cc9b54b9160a137f4355d1
    via sn-sj81 [ 172.20.168.81 ] :9000, D=0.302328 ms,
    H=00:00:08, U=02:15:53, S_SEQ=1, R_SEQ=0, S_SID=148214958, R_SID=0
PL  9f752f56f347ca8fcc40a4e09b645f9b4c9b71c73401083f4c04920b30215b0a
via sn-sj85 [ 172.20.168.85, 192.168.20.85, 192.168.86.85 ] :9000,
D=0.379999 ms, H=00:00:10, U=01:45:42, S_SEQ=0, R_SEQ=0,
S_SID=2134859630, R_SID=0
```

The following example illustrates the usage of **show srp neighbor down**. Assume that a four-node network consists of Proximity Engines sn-sj43, sn-sj88, sn-sj44, and sn-sj87. From sn-sj87, the **show srp neighbor down** command can be used to confirm this, as shown by the following output:

```
ServiceRouter# show srp neighbor

Codes: T - local node, L - leafset, P - primary, S - secondary, B - backup
       I - Intransitive, D - delay, H - hold time
Number of neighbors in the database: 3
PLI 0e33b4fc00ea5e32b7323c2a712cc226fe4990430df6ac9a05d2a87ab67c9fae
    via sn-sj43 [ 192.168.86.43 ] :9000, D=0.439602 ms,
   H=00:00:03
PL  2a2db308fd3dc172940a7902a4db7c16c98c3a32e1b048005bce1e832b6d056f
    via sn-sj88 [ 192.168.86.88 ] :9000, D=0.405537 ms,
   H=0.553618
PL  9a28755bba0228c7ac3d1be20d21a7a57c532eed9d5ffc5e1da2a9841e2e77a8
    via sn-sj44 [ 192.168.86.44 ] :9000, D=0.398474 ms,
   H=00:00:01

ServiceRouter# show srp neighbor down

Number of down neighbors in the database: 0
Next down neighbor write offset: 0
```

For the next example, assume that the domain ID for the local node (sn-sj87) is reconfigured so that it is detached from the network. The following output from **show srp neighbor down** now shows that all three neighbors are down:

```
ServiceRouter# show srp neighbor down
Number of down neighbors in the database: 3
Next down neighbor write offset: 3

9a28755bba0228c7ac3d1be20d21a7a57c532eed9d5ffc5e1da2a9841e2e77a8
   via sn-sj44 [ 192.168.86.44 ] :9000, 0.000 ms, no-timer
0e33b4fc00ea5e32b7323c2a712cc226fe4990430df6ac9a05d2a87ab67c9fae
   via sn-sj43 [ 192.168.86.43 ] :9000, 0.000 ms, no-timer
2a2db308fd3dc172940a7902a4db7c16c98c3a32e1b048005bce1e832b6d056f
   via sn-sj88 [ 192.168.86.88 ] :9000, 0.000 ms, no-timer
```

Related Commands

Command	Description
bootstrap-node	Configures a bootstrap node IP address.
domain	Sets the domain ID for an SRP.

show srp process

To display the basic configurations for SRP, use the **show srp process** command in privileged EXEC configuration mode.

show srp process

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

Privileged EXEC configuration mode.

Usage Guidelines

This command displays SRP process information.

Examples

The following example shows sample output from **show srp process** when it is run from Proximity Engine sn-sj87.

```
ServiceRouter# show srp process

Process:
  Domain: 0
  Node Id: d2fc632c53c9ff1de8683e265386b09502791aedd65f28025fe7f64ad8cab2d9
  Host name: sn-sj87
  Port: 9000
  Interfaces running SRP:
     *GigabitEthernet 1/0
  Bootstrap host name: 172.20.168.85, address: 172.20.168.85, port: 9000
  Database Mirroring: Disabled
  # of storages requested for mirroring: 2
  # of storages used for mirroring     : 1

ServiceRouter#
```

Related Commands

Command	Description
show srp memory	Displays SRP memory usage information.

show srp replica-set

To display the replica set information for a Proximity Engine, use the **show srp replica-set** command in privileged EXEC configuration mode.

show srp replica-set

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

Privileged EXEC configuration mode.

Usage Guidelines

This command displays SRP replica set information.

To use this command to show a replica set, a network needs to be formed by properly configuring a bootstrap node and domain ID.

Examples

The following examples show sample output from **show srp replica-set**. For the first example, assume a standalone Proximity Engine sn-sj87 and a two-node network consisting of Proximity Engine sn-sj81 and Proximity Engine sn-sj85. The **show srp replica-set** command is issued from sn-sj87 before it is connected to the two-node network:

```
ServiceRouter# show srp replica-set

Codes: T - local node, L - leafset, P - primary, S - secondary, B - backup
       I - intransitive, R - Replicate Set, A - active

key(part)         address              type  state
-------------------------------------------------

308fe23f...       EE7-CDE205-8:9000    PL    Active
5c71ac1e...       EE7-CDE205-10:9000   PL    Active
feb5784c...->     SN-CDSM:9000         local None
ServiceRouter#
```

Related Commands

Command	Description
show srp leafset	Displays SRP leafset information,
show srp neighbor	Displays SRP neighbor information

show srp route

To display route information for a Proximity Engine to its neighbor nodes on the same DHT network, use the **show srp route** command in privileged EXEC configuration mode.

show srp route [**backup | statistics**]

Syntax Description

backup	Displays entries, including backup entries.
statistics	Displays statistics information.

Command Defaults

None

Command Modes

Privileged EXEC configuration mode.

Usage Guidelines

This command displays route information for a Proximity Engine to its neighbor nodes on the same DHT network.

To use this command to show route entries, a network needs to be formed by properly configuring a bootstrap node and domain ID.

Examples

The following examples show sample output from **show srp route**. For the first example, assume a standalone Proximity Engine sn-sj87 and a two-node network consisting of Proximity Engine sn-sj81 and Proximity Engine sn-sj85. The **show srp route** command is issued from sn-sj87 before it is connected to the two-node network. The output shows no srp route information, as is expected for a standalone Proximity Engine:

```
ServiceRouter# show srp route

Codes: T - local node, L - leafset, P - primary, S - secondary, B - backup
       I - Intransitive
```

For the following example, assume that Proximity Engine sn-sj87 has joined the two-node network consisting of Proximity Engine sn-sj81 and Proximity Engine sn-sj85. The output shows that sn-sj87 has route information to its two neighbors, sn-sj81 and sn-sj85.

```
ServiceRouter# show srp route

Codes: T - local node, L - leafset, P - primary, S - secondary, B - backup
       I - Intransitive
PL  8/4 via 8886822171add71887d54107c266d814b605eaa0d5cc9b54b9160a137f4355d1
    sn-sj81 [ 172.20.168.81 ] :9000, 0.301080 ms, 00:00:09
PL  9/4 via 9f752f56f347ca8fcc40a4e09b645f9b4c9b71c73401083f4c04920b30215b0a
sn-sj85 [ 172.20.168.85, 192.168.20.85, 192.168.86.85 ] :9000, 0.382097 ms,
00:00:08
```

The **show srp route** command shows only primary routing table entries. In the SRP routing table, there are backup routes as well. To display the backup routes as well as the primary routes, use the command **show srp route backup** command:

```
ServiceRouter# show srp route backup

Codes: T - local node, L - leafset, P - primary, S - secondary, B - backup
       I - Intransitive
PL  8/4 via 8886822171add71887d54107c266d814b605eaa0d5cc9b54b9160a137f4355d1
    sn-sj81 [ 172.20.168.81 ] :9000, 0.301080 ms, 00:00:07
PL  9/4 via 9f752f56f347ca8fcc40a4e09b645f9b4c9b71c73401083f4c04920b30215b0a
sn-sj85 [ 172.20.168.85, 192.168.20.85, 192.168.86.85 ] :9000, 0.382097 ms,
00:00:10

ServiceRouter#
```

Because there is no backup route in this small three-node network, **show srp route backup** displays the same results as **show srp route**. This can be confirmed by issuing the **show srp route statistics** command as shown in the following example. From the following output, we can confirm that are total two routes in the routing table, one appearing in cell 8 row 0 (which is the route via sn-sj81) and the other appearing in cell 9 row 0 (which is the route via sn-sj85).

```
ServiceRouter# show srp route statistics

Total routes: 2
Entries that share my prefix: 0
Last nonempty row: 0

ServiceRouter#
```

Related Commands

Command	Description
show srp leafset	Displays SRP leafset information.
show srp neighbor	Displays SRP neighbor information.
show statistics srp	Displays SRP statistics information.

show srp subscribers

To display SRP multicast group subscriber information, use the **show srp subscribers** command in privileged EXEC configuration mode.

show srp subscribers

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

Privileged EXEC configuration mode.

Usage Guidelines

This command is used to check what multicast groups the Proximity Engine is currently subscribed to. If the Proximity Engine is not subscribed to any groups, there is no output.

Examples

In the following example, assume a standalone Proximity Engine sn-sj87:

1. The **show srp subscribers** command displays output showing that sn-sj87 is subscribed to one group (c1898f9a8b69c3912f0fe8fecac30818fab24385fa8a1d37a8ffd193cf3eeebc).
2. The local Proximity Engine (sn-sj87) subscribes to another existing multicast group (999).
3. The **show srp subscribers** displays output showing that sn-sj87 is subscribed two groups (c1898f9a8b69c3912f0fe8fecac30818fa b24385fa8a1d37a8ffd193cf3eeebc and 999).

```
ServiceRouter# show srp subscribers

c1898f9a8b69c3912f0fe8fecac30818fab24385fa8a1d37a8ffd193cf3eeebc
  Root node: d2fc632c53c9ff1de8683e265386b09502791aedd65f28025fe7f64ad8cab2d9
  Subscriber: 0x6891a0

ServiceRouter# show srp subscribers

999000000000000000000000000000000000000000000000000000000000000000000000
  Root node: 8886822171add71887d54107c266d814b605eaa0d5cc9b54b9160a137f4355d1
  Subscriber: 0x6891a0
c1898f9a8b69c3912f0fe8fecac30818fab24385fa8a1d37a8ffd193cf3eeebc
  Root node: d2fc632c53c9ff1de8683e265386b09502791aedd65f28025fe7f64ad8cab2d9

ServiceRouter#
```

show ssh

To display Secure Shell (SSH) status and configuration information, use the **show ssh** command in EXEC configuration mode.

show ssh

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

EXEC configuration mode.

Related Commands

Command	Description
sshd	Enables the SSH daemon.

show standby

To display standby interface information, use the **show standby** command in EXEC configuration mode.

show standby

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 3-72 describes the fields shown in the **show standby** display.

Table 3-72 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

Command	Description
show interface	Displays the hardware interface information.
show running-config	Displays the current running configuration information on the terminal.
show startup-config	Displays the startup configuration.

show startup-config

To display the startup configuration, use the **show startup-config** command in EXEC configuration mode.

show startup-config

Syntax Description

This command has no keywords or arguments.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Use this command to display the configuration used during an initial bootup, stored in non-volatile random-access memory (NVRAM).

Examples

The following example shows how to display the startup configuration details on the SE:

```
ServiceEngine# show startup-config
! CDS version 2.3.9
!
device mode service-engine
!
!
hostname V2-CDE220-3
!
!
!
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
```

Related Commands

Command	Description
configure	Enters Global configuration mode.
copy	Copies the configuration or image data from a source to a destination.
show running-config	Displays the current running configuration information on the terminal.

show statistics aaa

To display SE access control list statistics, use the **show statistics access-lists 300** command in EXEC configuration mode.

show statistics aaa

Syntax Description

This command has no keywords or arguments.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 3-73 describes the fields shown in the **show statistics aaa** display.

Table 3-73 show statistics aaa Field Descriptions

Field	Description
Authentication and Authorization Statistics	
Number of access requests	The number of authentication and authorization requests issued from this server.
Number of access deny responses	The number of authentication and authorization deny responses received from remote AAA server.
Number of access allow responses	The number of authentication and authorization allow responses received from remote AAA server.
Accounting Statistics	
Number of access requests	The number of accounting requests issued from this server.
Number of access deny responses	The number of accounting deny responses received from remote AAA server.
Number of access allow responses	The number of accounting allow responses received from remote AAA server.

Related Commands

Command	Description
aaa	Specifies accounting, authentication and authorization methods.
show aaa	Displays the accounting, authentication and authorization configuration.

show statistics access-lists 300

To display SE access control list statistics, use the **show statistics access-lists 300** command in EXEC configuration mode.

show statistics access-lists 300

Syntax Description

This command has no keywords or arguments.

Command Defaults

None

Command Modes

EXEC configuration mode.

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.

Table 3-74 describes the fields shown in the **show statistics access-lists 300** display.

Table 3-74 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

Command	Description
clear	Clears the HTTP object cache, the hardware interface, statistics, archive working transaction logs, and other settings.

show statistics acquirer

To display SE acquirer channel statistics, use the **show statistics acquirer** command in EXEC configuration mode.

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.
delivery_service_id	Delivery service ID.
delivery-service-name	Displays acquirer statistics for the specified delivery service name.
delivery_service_name	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.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The **show statistics acquirer** command displays acquirer statistics for all channels for which the SE is the Content Acquirer. 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.

Table 3-75 describes the fields shown in the **show statistics acquirer** display.

Table 3-75 show statistics acquirer Field Descriptions

Field	Description
Statistics For Channel ID: ***channel-id***	
Delivery-service-id	Delivery service identification number.

Table 3-75 show statistics acquirer Field Descriptions (continued)

Field	Description
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.

Table 3-76 describes the fields shown in the **show statistics acquirer contents delivery-service-name** display.

Table 3-76 show statistics acquirer contents delivery-service-name Field Descriptions

Field	Description
Acquired Contents	
Modification Time	Local time the acquirer contents were modified.
Size	Size of the file.
URL	URL of the file.

Examples

The following example shows how to display the acquirer statistics for the Delivery Service name settur-ds:

```
ServiceEngine# show statistics acquirer contents deliver-service-name settur-ds
Querying Database.......

Contents Acquired for the Delivery Service Name :settur-ds
----------------------------------------

Acquired Contents:
----------------------

Modification Time : Fri Aug  1 06:08:26 2008
Size              : 128899758 Bytes
Url               : http://172.XX.XX.XX/300kbs.wmv


Modification Time : Wed May 21 08:58:17 2008
Size              : 174569021 Bytes
Url               : http://172.XX.XX.XX/1mbps.mov


Modification Time : Wed May 11 09:19:17 2011
```

```
Size              : 425468369 Bytes
Url               : http://172.XX.XX.XX/flash_1mbps.mp4


Modification Time : Mon Jun 20 10:15:37 2011
Size              : 22952732 Bytes
Url               : http://172.XX.XX.XX/sample.mpeg
```

Related Commands

Command	Description
acquirer (EXEC)	Starts or stops content acquisition on a specified acquirer delivery service.
clear statistics	Clears all statistical counters from the parameters given.
show acquirer	Displays the acquirer information and progress of content acquisition for a specified channel number or name.

show statistics admission

To display admission control statistics, use the **show statistics admission** command in EXEC configuration mode.

show statistics admission

Syntax Description

This command has no keywords or arguments.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 3-77 describes the fields shown in the **show statistics admission** display.

Table 3-77 show statistics admission

Field	Description
QOS Admission Check	
Bypassed	
Attempts	
Succeeded	
Failed	
Best effort	
Attempts	
Based on congestion	
Succeeded	
Failed	
Too many sessions	
Average too low	
Soft guaranteed	
Attempts	
Succeeded	
Failed	
Disk congestion	

Table 3-77 show statistics admission (continued)

Field	Description
BE would be too low	
Over threshold	
Hard guaranteed	
Attempts	
Succeeded	
Failed	
Hole management	
Bypassed	
Succeeded	
Failed	
fill too close	
Hit data	
with active fill	
request range inside inactive fill	
request range overlaps inactive fill	
Hit hole	
not aligned, 2 fills	
aligned, 1 fill	
too many fills	
too many holes	
fill from start	
active fill	
fill from left	
Disk overload	
Misc errors	

show statistics authsvr

To view the Authentication Server statistics, use the **show statistics authsvr** command in EXEC configuration mode.

show statistics authsvr {**delivery-service-id** *num* {**detail** | **geo** | **ip** | **rules**} | **global**}

Syntax Description

delivery-service-id	Delivery service ID.
num	Displays delivery service statistics (0 to 4294967295).
detail	Displays detail statistics for all authorization types.
geo	Displays geographical authorization statistics.
ip	Displays IP authorization statistics.
rules	Displays rules authorization statistics.
global	Displays Authentication Server global statistics.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The output of the **show statistics authsvr** command displays Rules statistics based on the rules configured through the XML. If Rule_Allow is configured, then the statistics for Rule_Allow must be incremented whether or not any other rule is configured. If the Rule_Allow or Rule_Block is not configured but Rule_UrlRewrite is configured, then the statistics of Rule_UrlRewrite are incremented. Similarly, if the Rule_Block is configured along with Rule_UrlRewrite, then the statistics of Rule_Block and Rule_UrlRewrite are incremented.

When Unknown Server Requests is enabled, a request for an unknown server increments both the Allowed counter and the Unknown Server Allowed counter. When Unknown Server Request is disabled, a request for an unknown server increments both the Blocked counter and the Unknown Server Blocked counter.

The **show statistics authsvr delivery-service-id** command displays statistics for each delivery service and for each rule in the delivery service. All the statistics are based on the Authsvr Rules configured in the XML file for a particular delivery service.

Table 3-78 describes the fields shown in the **show statistics authsvr delivery-service-id detail** display.

Table 3-78 show statistics authsvr delivery-service-id detail Command Field Descriptions

Field	Description
IP Statistics	IP authorization statistics.
Allow	This field increments when Unknown Server Request is enabled.
Block	This field increments when Unknown Server Request is disabled.
Geo Statistics	Geographical authorization statistics.
Allow	This field increments when Unknown Server Request is enabled.
Block	This field increments when Unknown Server Request is disabled.
Rules Statistics	Rules authorization statistics.
Rule Allow	Number of authorization requests applied on Rule Allow.
Rule Block	Number of Rule Block statistics.
Rule Forced Revalidate	Number of Rule Forced Revalidate statistics.
Rule No Cache	Number of Rule No Cache statistics.
Rule SWF File Validate	Number of Rule (FMS) SWF File Validate statistics.
Rule URL Redirect	Number of Rule URL Redirect statistics.
Rule URL Resolve	Number of Rule URL Resolve statistics.
Rule URL Rewrite	Number of Rule URL Rewrite statistics.

Table 3-79 describes the fields shown in the **show statistics authsvr global** display.

Table 3-79 show statistics authsvr global Command Field Descriptions

Field	Description
Allowed	This field increments when Unknown Server Request is enabled.
Blocked	This field increments when Unknown Server Request is disabled.
Unknown Server Allowed	This field increments when Unknown Server Request is enabled.
Unknown Server Blocked	This field increments when Unknown Server Request is disabled.
Errors	This field increments when errors occur.

Examples

The following shows how to display the Authentication Server delivery service ID detail statistics:

```
ServiceEngine# show statistics authsvr delivery-service-id 1 detail

IP Statistics
----------------
    Allow               :  200
    Block               :  10
```

```
Geo Statistics
-------------------
    Allow               :  23
    Block               :  10

Rules Statistics
----------------------
    Rule_Allow          :  134
    Rule_Block          :  23
    Rule_ForcedReValidate:  12
    Rule_NoCache        :  16
    Rule_SwfFileValidate :  5
    Rule_UrlRedirect    :  7
    Rule_UrlResolve     : 10
    Rule_UrlRewrite     :  3
ServiceEngine#
```

The following shows how to display the Authentication Server global statistics:

```
ServiceEngine# show statistics authsvr global

Authserver Statistics
---------------------
Allowed                :                  4329108
Blocked                :                        0
Unknown Server Allowed :                       10
Unknown Server Blocked :                        0
Errors                 :                        0
ServiceEngine#
```

Related Commands

Command	Description
authsvr	Enables and configures the Authorization server.
show authsvr	Displays the status of the Authorization server.

show statistics cdn-select

To view the CDN Selector statistics, use the **show statistics cdn-select** command in EXEC configuration mode.

show statistics cdn-select summary

Syntax Description

summary	Displays summary statistics for the CDN Selector.

Command Defaults

None

Command Modes

EXEC configuration mode.

Examples

The following is sample CDN Selector statistics:

```
ServiceRouter# show statistics cdn-select summary

----- CDN Selector Summary Statistics -----

Requests Received                 :                 0
Requests Redirected (3rd party)   :                 0
Requests Routed (CDS-IS)          :                 0
Requests Not Redirected           :                 0
  CDN Errors                      :                 0

ServiceRouter#
```

Related Commands

Command	Description
cdn-select	Enables the CDN Selector for third-party service selection.
geo-location-server	Redirects requests to different Content Delivery Networks based on the geographic location of the client.
show cdn-select	Displays the status of the CDN Selector.

show statistics cdnfs

To display SE CDS network file system (cdnfs) statistics, use the **show statistics cdnfs** command in EXEC configuration mode.

show statistics cdnfs

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 3-80 describes the **show statistics cdnfs** command fields displayed in the command output.

Table 3-80 show statistics cdnfs Fields

Field	Description
Size of physical file system	Physical disk size of the CDNFS.
Space assigned for cdnfs purposes	Amount of physical disk space on the CDNFS that has been assigned to hold prepositioned objects. The space can be less than the size of the file system.
Number of cdnfs entries	Number of CDNFS objects. **Note** One prepositioned file internally uses two CDNFS entries. The number of CDNFS entries is twice the number of actual files displayed to users.
Space reserved for cdnfs entries	Amount of disk space reserved for existing prepositioned 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 CDNFS for new prepositioned objects.
Physical file system in use	Amount of physical disk space currently in use by the CDNFS.
Physical file system space free	Amount of unused physical disk space in the CDNFS
Physical file system percentage in use	Percentage of physical disk space in use relative to the total disk space available.

Related Commands

Command	Description
cdnfs	Manages the Internet Streamer CDNFS.
clear	Clears the HTTP object cache, the hardware interface, statistics, archive working transaction logs, and other settings.
show cdnfs	Displays CDNFS information.
show disks	Displays the names of the disks currently attached to the SE.

show statistics content-mgr

To display Content Manager statistics, use the **show statistics content-mgr** command in EXEC configuration mode.

show statistics content-mgr

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 3-81 describes the **show statistics content-mgr** command fields displayed in the command output.

Table 3-81 show statistics content-mgr Fields

Field	Description
Add Message Count	Counter to track when new content is added in content manager. The source of content can be either protocol engine or snapshot.
Update Message Count	Counter to track when content is updated in content manager.
Delete Message Count	Counter to track when content is deleted in content manager.
New Content Count	Counter to track when new content is added in content manager from protocol engine. This does not include content added via snapshot.
Slow Scan Cache Count	Count of cached content added to content manager via slow scan
Slow Scan Preposition Count	Count of preposition content added to content manager via slow scan.
Slow Scan Cache Child Count	Count of cached child content (WMT/MS) added to content manager via slow scan.
Last Slow Scan Time	Time at which last slow scan operation was performed.
Snapshot Recovered Count	Counter to track when new content is added to content manager from snapshot. This does not include content added via protocol engine.
Deletion Task Count	Number of deletion tasks in Content Manager.
Evicted Asset Count	Count of assets evicted.
Eviction count Disk Size	Number of evictions occurred due to insufficient disk size.
Last Eviction Time	Last time at which eviction added.
Eviction Protect Add Count	Number of contents added for eviction protection.
Eviction Protect Delete Count	Number of contents removed from eviction protection.

Table 3-81 show statistics content-mgr Fields (continued)

Field	Description
Eviction Protect Skip Count	Number of contents skipped since it is protected by eviction protection.
Deletion Store Size	Count of entries present in deletion store.
Preposition Asset Count	Count of preposition assets.
Cache Asset Count	Count of cache assets.
Preposition Asset Size	Disk size for preposition assets.
Cache Asset Size	Disk size for cache assets.
Total Asset Size	Total size for preposition and cache assets.
Current Memory Usage	Current memory usage of Content Manager process.
Slow Scan In Progress	Is slow scan process running?
Clear-Cache-All Count	Number of times cache was cleared by clear all command.
Deletion In Progress	Is content deletion currently in progress?
Snapshot In Progress	Is Snapshot writer running?
Snapshot Reader up	Is Snapshot reader running?
Priority Queue Size	Number of assets present in priority queue/.
Eviction Protection Size	Number of entries present in eviction protection table.
Eviction Count-Mem Usage	Number of evictions occurred due to less mem usage.
Eviction Count-Content Count	Number of evictions due max content limit reached.
Eviction Protect Max Size	Max size of the eviction protection table since start of content manager.
Last Cache Clear Time	Time at which cache was cleared.
Last Statistics Clear Time	Time at which statistics was cleared.
Last Global Eviction Time	Time at which global eviction happened.

Related Commands-

Command	Description
contentmgr	Configures the Content Manager.
content-mgr disk-info force-reset	Forces the Content Manager to reset the disk share memory information.
show content-mgr	Displays all content management information.

show statistics distribution

To display the statistics of the content distribution components, use the **show statistics distribution** command in EXEC configuration mode.

show statistics distribution {**all** | **errors** {**delivery-service-id** *delivery_service_id* | **delivery-service-name** *delivery_service_name*} | **mcast-data-receiver detail** | **mcast-data-sender** [**delivery-service-id** *delivery_service_id* | **delivery-service-name** *delivery_service_name* | **detail** | **feedback duration {days** *num* **detail** | **hours** *num* **detail** | **minutes** *num* **detail}**] | **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.
delivery_service_id	Delivery service number.
delivery-service-name	Displays statistics about the specified delivery service name.
delivery_service_name	Delivery service name.
mcast-data-receiver	Distribution statistics for Multicast Data Receiver.
detail	(Optional) Detailed statistics.
mcast-data-sender	Distribution statistics for Multicast Data Sender.
feedback	(Optional) Distribution feedback statistics.
duration	(Optional) Feedback statistics for the particular duration.
days	Number of days. The range is from 1 to 365.
num	Days.
hours	Number of hours. The range is from 1 to 24.
num	Hours.
minutes	Number of minutes. The range is from 1 to 60.
num	Minutes.
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.
delivery_service_id	(Optional) Delivery service number.
delivery-service-name	(Optional) Displays statistics about the specified delivery service name.
delivery_service_name	(Optional) Delivery service name.
hot-forwarders	(Optional) Displays the content distribution statistics of hot forwarders.
forwarder_id	(Optional) Identifier for the hot forwarder SE.
forwarder_name	(Optional) Name of the hot forwarder SE.
idle-forwarders	(Optional) Displays the content distribution statistics of idle forwarders.

max_idle_forwarders	(Optional) Maximum number of idle forwarder SEs to be displayed.
unicast-data-sender	(Optional) Displays the content distribution statistics of the unicast data sender.

Command Defaults

The **idle-forwarders** *max_idle_forwarders* default is 3.

Command Modes

EXEC configuration mode.

Usage Guidelines

Note This command is only available on Cisco Internet Streamer CDS Release 3.1.1.

The customer creates a multicast cloud and specifies which SEs are multicast senders, and which are multicast receivers within the cloud. Use the **show statistics distribution mcast-data-sender** or **show statistics distribution mcast-data-receiver** to view multicast statistics.

Note While distributing large content from the sender, the **show statistics distribution mcast-data-sender** takes time to get all the records.

Table 0-1 describes the fields shown in the **show statistics distribution unicast-data-receiver** display.

Table 0-1 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.

Table 0-1 show statistics distribution unicast-data-receiver Field Descriptions (continued)

Field	Description
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.
# 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.

Note This command is only available on Cisco Internet Streamer CDS Release 3.1.1.

Related Commands

Command	Description
clear	Clears the HTTP object cache, the hardware interface, statistics, archive working transaction logs, and other settings.
distribution	Reschedules and refreshes content redistribution for a specified delivery service ID or name
show distribution	Displays the distribution information for a specified delivery service.

show statistics flash-media-streaming

To display the statistics for Flash Media Streaming, use the **show statistics flash-media-streaming** command in EXEC configuration mode.

show statistics flash-media-streaming [**connections | dvrcast | errors | flvcache | livestats | performance | proxy | rules | server | swf | vod**]

Syntax Description

connections	(Optional) Displays Flash Media Streaming connections statistics.
dvrcast	(Optional) Displays Flash Media Streaming dvrcast application statistics. **Note** The **dvrcast** keyword is only available on the 2.4.3 and earlier releases.
errors	(Optional) Displays Flash Media Streaming errors statistics.
flvcache	(Optional) Displays Flash Media Streaming FLV[1] cache statistics.
livestats	(Optional) Displays Flash Media Streaming live application statistics.
performance	(Optional) Displays Flash Media Streaming performance statistics.
proxy	(Optional) Displays Flash Media Streaming proxy application statistics.
rules	(Optional) Displays Flash Media Streaming rules statistics.
server	(Optional) Displays Flash Media Streaming server level statistics.
swf	(Optional) Displays Flash Media Streaming SWF[2] verification statistics.
vod	(Optional) Displays Flash Media Streaming vod application statistics.

1. Flash Video
2. Shockwave Flash

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The **show statistics flash-media-streaming rules** command indicates how many requests rules were allowed, denied, if URL signing was performed, if URL signing failed with different error cases, and if the auth server accepted or rejected the request. Since the auth server rules framework performs all these actions, the values of the rules statistics are calculated by observing auth server replies and return codes.

Examples

The following example shows how to display 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 Connections
Total                :                    0
VOD                  :                    0
LIVE                 :                    0
DVRCast              :                    0
Proxy                :                    0
Max Concurrent       :                    0
Total Connections
Total                :                    0
VOD                  :                    0
LIVE                 :                    0
DVRCast              :                    0
Proxy                :                    0

VOD Streaming
-----
Current Connections  :                    0
Total Connections    :                    0
DownStream Bytes     :                    0
UpStream Bytes       :                    0
DownStream BW        :                    0 Kbps
Preposition Hit      :                    0
External Hit         :                    0
Cache Hit            :                    0
Cache Miss           :                    0
Proxy Case           :                    0
Cache Hit Percentage :                 0.00
Local Disk Reads     :                    0
HTTP Based Reads     :                    0
Bytes From Local Disk:                    0
Bytes Through HTTP   :                    0
Ignore Query String  :                    0
Query String Bypassed:                 0

Live Streaming
-----
Current Connections          :                    0
Total Connections            :                    0
UpStream BW                  :                    0 Kbps
DownStream BW                :                    0 Kbps
UpStream Bytes               :                    0
DownStream Bytes             :                    0
Downstream CDS-IS total conn.:                    0
Ignore Query String          :                    0
Query String Bypassed:                 0

DVRCast Streaming
-----
Current Connections  :                    0
Total Connections    :                    0
UpStream BW          :                    0 Kbps
DownStream BW        :                    0 Kbps
UpStream Bytes       :                    0
DownStream Bytes     :                    0
Ignore Query String  :                    0
Query String Bypassed:                 0

Proxy Streaming
-----
Current Connections  :                    0
Total Connections    :                    0
UpStream BW          :                    0 Kbps
DownStream BW        :                    0 Kbps
UpStream Bytes       :                    0
```

```
DownStream Bytes     :                   0

Rules
-----------
Action Allow               :                   0
Action Block               :                   0
Validate url Sign          :                   0
URL Signing errors:
         Invalid Client    :                   0
         Invalid Signature :                   0
         No signing        :                   0
         Expired URL       :                   0
Auth server validation:
         Auth Server Allow :                   0
         Auth Server Deny  :                   0

SWF Verification :
 --------------------
Requests
         Performed            :                   0
         Failed               :                   0
         Successful           :                   0
         Bypassed             :                   0
         Memory Hash Hit      :                   0
         Memory Hash Calculated:                  0
         Local SWF Hit        :                   0
         Preposition SWF      :                   0
         SWF External Hit     :                   0
         SWF Cache Hit        :                   0
         SWF Cache Miss       :                   0
         SWF Proxy            :                   0
Errors
         SWF Fetch Error      :                   0
         Local SWF Read Error :                   0
         Cached SWF Read Error :                  0
         SWF File not found   :                   0
         SWF Incorrect Depth  :                   0
         SWF Hash Match Fail  :                   0
         SWF Hash Partial     :                   0
         Edge SWF Cache Miss  :                   0
         SWF Response Timeout :                   0
         SWF Client Unsupported:                  0
         SWF Wrong Version    :                   0

Error
-----
Disk Error
         File Open Error           :                  0
         File Read Error           :                  0
         File GetAttributes Error  :                  0
         File Close Error          :                  0

 HTTP Error
         Invalid Error             :                  0
         Server Error              :                  0
         Media Not Found           :                  0
         Media Unauthorize         :                  0
         Invalid Request           :                  0
         Bad Gateway               :                  0
         Service Unavailable       :                  0
         Gateway Timeout           :                  0
         Request Failed            :                  0
         Invalid Response          :                  0
         Too many Redirect         :                  0
```

```
        Invalid Redirect          :                    0
        Invalid Cache Type        :                    0

Server
-----------
Total UpStream BW      :                    0 Kbps
Total DownStream BW    :                    0 Kbps
Total UpStream Bytes   :                    0
Total DownStream Bytes :                    0
Total Server Bytes     :                    0

Performance
-----------
Server Up Time       :                   3 S
Mem Usage            :                   4 %
Max Mem Usage        :                   4 %
Total Messages Dropped:                   0

Num of Active VOD Instances     :                   0
Num of Active Live Instances    :                   0
Num of Active DVRCast Instances :                   0

Flash Video Cache Statistics
-----------
Hits                 :                   0
Misses               :                   0
Released             :                   0
Bytes in cache       :                   0
Bytes in use         :                   0
Disk Usage           :                4096
ServiceEngine#
```

Table 0-2 describes the fields shown in the **show statistics flash-media-streaming** display.

Table 0-2 show statistics flash-media-streaming Field Descriptions

Field	Description
Connections	
Current Connections	
Total	Total number of current active connections to Flash Media Streaming.
VOD	Total number of current active connections to VOD applications to Flash Media Streaming.
Live	Total number of current active connections to Live applications to Flash Media Streaming.
DVRCast	Total number of current active connections to DVRCast applications to Flash Media Streaming.
Proxy	Total number of current active connections to non-VOD, Live or DVR applications to Flash Media Streaming.
Max Current	Max concurrent connections to Flash Media Streaming since it has started.
Total Connections	
Total	Total number of connections to Flash Media Streaming since it has started.

Table 0-2 show statistics flash-media-streaming Field Descriptions (continued)

Field	Description
VOD	Total number of connections to VOD applications to Flash Media Streaming since it has started.
LIVE	Total number of connections to Live applications to Flash Media Streaming since it has started.
DVRCast	Total number of connections to DVRCast applications to Flash Media Streaming since it has started.
Proxy	Total number of connections to non-VOD, Live or DVR applications to Flash Media Streaming since it has started.
VOD Streaming	
Current Connections	Total number of current active connections to VOD applications to Flash Media Streaming.
Total Connections	Total number of connections to VOD applications to Flash Media Streaming since it has started.
DownStream Bytes	Total bytes transferred from server to client by VOD applications of Flash Media Streaming since it has started.
UpStream Bytes	Total bytes transferred from client to server by VOD applications of Flash Media Streaming since it has started.
DownStream BW	Current Bandwidth from server to client by VOD applications of Flash Media Streaming in Kbps.
Preposition Hit	Total requests for prepositioned content by VOD applications of Flash Media Streaming since it has started.
External Hit	Displays NAS Origin Hit count.
Cache Hit	Total requests for cache hit content by VOD applications of Flash Media Streaming since it has started.
Cache Miss	Total cache miss requests by VOD applications of Flash Media Streaming since it has started.
Proxy Case	Total requests for non cached and non prepositioned content by VOD applications of Flash Media Streaming since it has started.
Cache Hit Percentage	Percentage of cache hit requests to total requests.
Local Disk Reads	Number of read calls to local disk by VOD applications.
HTTP Based Reads	Number of read calls to HTTP sockets by VOD applications.
Bytes from Local Disk	Total bytes read through HTTP by VOD applications.
Bytes through HTTP	Total bytes read from local disk by VOD applications.
Live Streaming	
Current Connections	Total number of current active connections to Live applications to Flash Media Streaming.
Total Connections	Total number of connections to Live applications to Flash Media Streaming since it has started.
UpStream BW	Current bandwidth from client to server by Live applications of Flash Media Streaming in Kbps.

Table 0-2 show statistics flash-media-streaming Field Descriptions (continued)

Field	Description
DownStream BW	Current bandwidth from server to client by Live applications of Flash Media Streaming in Kbps.
UpStream Bytes	Total bytes transferred from client to server by Live applications of Flash Media Streaming since it has started.
DownStream Bytes	Total bytes transferred from server to client by Live applications of Flash Media Streaming since it has started.
Downstream CDS-IS Total Connections	Total live connections from CDS-IS devices that are on a lower level in a tree hierarchy.
DVRCast Streaming	
Current Connections	Total number of current active connections to DVRCast applications to Flash Media Streaming.
Total Connections	Total number of connections to DVRCast applications to Flash Media Streaming since it has started.
UpStream BW	Current bandwidth from client to server by DVRCast applications of Flash Media Streaming in Kbps.
DownStream BW	Current bandwidth from server to client by DVRCast applications of Flash Media Streaming in Kbps.
UpStream Bytes	Total bytes transferred from client to server by DVRCast applications of Flash Media Streaming since it has started.
DownStream Bytes	Total bytes transferred from server to client by DVRCast applications of Flash Media Streaming since it has started.
Proxy Streaming	
Current Connections	Total number of current active connections non-VOD, Live or DVR applications to Flash Media Streaming.
Total Connections	Total number of connections non-VOD, Live or DVR applications to Flash Media Streaming since it has started.
UpStream BW	Current bandwidth from client to server by non-VOD, Live or DVR applications of Flash Media Streaming in Kbps.
DownStream BW	Current bandwidth from server to client by non-VOD, Live or DVR applications of Flash Media Streaming in Kbps.
UpStream Bytes	Total bytes transferred from client to server by non-VOD, Live or DVR applications of Flash Media Streaming since it has started.
DownStream Bytes	Total bytes transferred from server to client by non-VOD, Live or DVR applications of Flash Media Streaming since it has started.
Rules	
Action Allow	Total number of requests allowed by configured rules.
Action Block	Total number of requests blocked by configured rules.
Validate URL Sign	Total number of requests for which URL sign validation was performed.
URL Signing errors	
Invalid Client	Total requests where URL signing failed as request was from an invalid client IP address.

Table 0-2 show statistics flash-media-streaming Field Descriptions (continued)

Field	Description
Invalid Signature	Total requests where URL signing failed as request had an invalid signature.
No signing	Total requests where URL signing failed as request was sent without URL signature.
Expired URL	Total requests where URL signing failed as the signature had expired its lifetime.
Auth server validation	
Auth Server Allow	Total number of requests allowed by the authorization server process.
Auth Server Deny	Total number of requests denied by the authorization server process.
SWF Verification	
Requests	
Performed	Total number of requests for which SWF verification was performed.
Failed	Total number of requests for which SWF verification failed.
Successful	Total number of requests for which SWF verification was successful.
Bypassed	Total number of requests for which SWF verification was not performed or bypassed.
Memory Hash Hit	Total number of requests for which SWF signature was already present in internal memory of Flash Media Streaming.
Memory Hash Calculated	Total number of requests for which SWF signature was newly calculated by Flash Media Streaming.
Local SWF Hit	Total number of requests where SWF file was present on /local1 partition of SE.
Preposition SWF	Total number of requests where SWF file was prepositioned on SE.
SWF External Hit	Total number of requests where SWF file was present on a NAS partition.
SWF Cache Hit	Total number of requests where SWF file was cached on local disk.
SWF Cache Miss	Total number of requests where SWF file was dynamically cached on local disk.
SWF Proxy	Total number of requests where SWF file was not prepositioned or cached on disk.
Errors	
SWF Fetch Error	SWF Fetch Error: Error in fetching SWF file from web engine.
Local SWF Read Error	Error reading SWF file from /local1 partition.
Cached SWF Read Error	Error reading cached SWF file.
SWF File not found	SWF file not found on disk.
SWF Incorrect Depth	SWF File could not hash to the requested depth.
SWF Match Fail	Hash produced does not match the client's hash.
SWF Hash Partial	Partial file SWF Hash Match.

Table 0-2 show statistics flash-media-streaming Field Descriptions (continued)

Field	Description
Edge SWF Cache Miss	Edge SWF Hash Cache missed.
SWF Response Timeout	SWF Hash Response Timeout.
SWF Client Unsupported	Client cannot support SWF Hashing.
SWF Wrong Version	Hash is the wrong SWF Verification version.
Error	
Disk Error	
File Open Error	Total errors when trying to open a file by Flash Media Streaming.
File Read Error	Total errors when trying to read a file by Flash Media Streaming.
File GetAttributes Error	Total errors when trying to get file attributes by Flash Media Streaming.
File Close Error	Total errors when trying to close a file by Flash Media Streaming.
HTTP Error	
Invalid Error	Invalid HTTP error code received by Flash Media Streaming.
Server Error	HTTP error code 500 received by Flash Media Streaming.
Media Not Found	HTTP error code 404 received by Flash Media Streaming.
Media Unauthorize	Unauthorized access, HTTP error code 401-407, except 404, received by Flash Media Streaming.
Invalid Request	HTTP error code 400 received by Flash Media Streaming.
Bad Gateway	HTTP error code 502 received by Flash Media Streaming.
Service Unavailable	HTTP error code 503 received by Flash Media Streaming.
Gateway Timeout	HTTP error code 504 received by Flash Media Streaming.
Request Failed	Null reply received by Flash Media Streaming.
Invalid Response	HTTP error code 0 received by Flash Media Streaming.
Too many Redirect	More than allowed number of HTTP redirects received by Flash Media Streaming.
Invalid Redirect	Invalid redirect URL received by Flash Media Streaming.
Invalid Cache Type	Invalid cache type received from web engine by Flash Media Streaming.
Server	
Total UpStream BW	Total instantaneous BW from client to server for Flash Media Streaming.
Total DownStream BW	Total instantaneous BW from server to client for Flash Media Streaming.
Total UpStream Bytes	Total bytes transferred from client to server for Flash Media Streaming.
Total DownStream Bytes	Total bytes transferred from server to client for Flash Media Streaming.
Total Server Bytes	Total bytes served by Flash Media Streaming.
Performance	
Server Up Time	Time since the Flash Media Streaming has been running.

Table 0-2 show statistics flash-media-streaming Field Descriptions (continued)

Field	Description
Mem Usage	Current memory usage of Flash Media Streaming.
Max Mem Usage	Maximum memory usage of Flash Media Streaming.
Total Messages Dropped	Total messages dropped by Flash Media Streaming.
Num of Active VOD Instances	Total active VOD instances.
Num of Active Live Instances	Total active Live instances.
Num of Active DVRCast Instances	Total active DVRCast instances.
Flash Video Cache Statistics	
Hits	Total hits on Flash video cache.
Misses	Total misses on Flash video cache.
Released	Total number of segments released by Flash video cache since Flash Media Streaming has started.
Bytes in cache	Current number of bytes in cache.
Bytes in use	Current number of bytes in cache being used.
Disk Usage	Size of flash video cache on disk.

Related Commands

Command	Description
flash-media-streaming	Enables and configures Flash Media Streaming.
show flash-media-streaming	Displays the Flash Media Streaming information.

show statistics icmp

To display SE Internet Control Message Protocol (ICMP) statistics, use the **show statistics icmp** command in EXEC configuration mode.

show statistics icmp

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

EXEC configuration mode.

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 is delivered or a control message is 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 show a value of 0 in the code field. ICMP uses the queries as shown in Table 0-3.

Table 0-3 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

Table 0-3 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 0-4.

Table 0-4 Errors

Error	Type Field Value
Destination Unreachable	3
Source Quench	4
Redirect	5
Time Exceeded	11
Parameter Problems	12

Table 0-5 describes the fields shown in the **show statistics icmp** display.

Table 0-5 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 0-5 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 because of 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 0-5 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 0-5 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.

Table 0-5 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

Command	Description
clear	Clears the HTTP object cache, the hardware interface, statistics, archive working transaction logs, and other settings.

show statistics ip

To display the IP statistics, use the **show statistics ip** command in user EXEC configuration mode.

On the SE and CDSM:

show statistics ip

On the SR:

show statistics ip {**ospf** | **proximity** {**rib** | **server**}}

Syntax Description

ospf	Displays the different OSPF counters.
proximity	Displays the proximity statistics.
rib	Displays the RIB proximity statistics.
server	Displays the proximity server statistics.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

The **show statistics ip OSPF** command is used to display OSPF counters.

The **show statistics ip proximity** command is used to display proximity statistics that are tracked in the RIB.

Examples

The following is sample output from the **show statistics ip ospf** command:

```
ServiceRouter# show statistics ip ospf

Generic counters:
 OSPF Process ID p1, Event statistics (cleared 06:57:01 ago)
  Router ID changes: 0
  DR elections: 0
  Older LSAs received: 0
  Neighbor state changes: 0
  Neighbor dead postponed: 0
  Neighbor dead interval expirations: 0
  Neighbor bad lsreqs: 0
  Neighbor sequence number mismatches: 0
  SPF computations:  2926 full, 0 summary, 0 external

        LSA Type Generated Refreshed   Flushed  Aged out
          Router         0        14         0         2
         Network         0         0         0         0
     Summary Net         0         0         0         0
    Summary ASBR         0         0         0         0
     AS External         0         0         0         0
     Opaque Link         0         0         0         0
```

```
      Opaque Area          0          0          0          0
        Opaque AS          0          0          0          0

  Following counters can not be reset:

  LSA deletions: 0 pending, 2 hwm, 531 deleted, 0 revived, 12 runs
  Hello queue: 0/200, hwm 2, drops 0
  Flood queue: 0/100, hwm 8, drops 0
  LSDB additions failed: 0

         Buffers:    in use       hwm permanent     alloc      free
       128 bytes          0         4         4     19430     19430
       512 bytes          0         4         4     37061     37061
      1520 bytes          0         3         2      1205      1205
      4500 bytes          0         2         1     20535     20535
            huge          0         0         0         0         0

ServiceRouter#
```

The following is sample output from the **show statistics ip proximity** command.

```
ServiceRouter> show statistics ip proximity

Total number of proximity requests received from applications: 9736
Total number of proximity replies sent to applications:        9736

Proximity msg exchanges between urib and other routing protocols:
                                Sent_Prox_Req     Received_Prox_Resp
isis                                    0                  0

ospf                                 6677               6677

Local proximity requests from applications: 3055

Invalid proximity requests from applications: 0

PSA/PTL non-rankable proximity requests from applications: 4
Failed proximity requests to routing protocols: 0
Failed PSA lookups: 4
Failed PTL lookups: 52493

ServiceRouter>
```

Table 0-6 describes the fields shown in the **show statistics ip** display.

Table 0-6 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 because of 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.

Table 0-6 show statistics ip Field Descriptions (continued)

Field	Description
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 includes 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).
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 send 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 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.

Table 0-6 show statistics ip Field Descriptions (continued)

Field	Description
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 because of fragmentation at this entity.

Related Commands

Command	Description
clear statistics ip	Clears IP statistics counters.
ip	Configures the IP.
show ip routes	Displays the IP routing table.

show statistics isis

To display IS-IS traffic counters, use the **show statistics isis** command in user EXEC configuration mode.

show statistics isis [**GigabitEthernet** *slot/port_num* | **PortChannel** *num*]

Syntax Description

GigabitEthernet	(Optional) Selects a Gigabit Ethernet interface.
slot/port_num	Slot and port number for the selected interface. The slot range is 0 to 14; the port range is 0 to 0. The slot number and port number are separated with a forward slash character (/).
PortChannel	(Optional) Selects the Ethernet Channel of interfaces.
num	Ethernet Channel interface number. The range is from 1 to 4.

Defaults

Not specifying an interface name displays IS-IS traffic statistics for all the IS-IS instances. IS-IS traffic statistics are displayed for all interfaces.

Command Modes

User EXEC configuration mode.

Usage Guidelines

The **show statistics isis** command displays IS-IS traffic counters for the specified interface or all traffic counters if no interface is specified.

Examples

The following is sample output from the **show statistics isis** command that shows all traffic counters for all IS-IS instances:

```
ServiceRouter# show statistics isis

IS-IS statistics:
PDU        Received        Sent  RcvAuthErr OtherRcvErr
LAN-IIH       60182       15965           0           0
P2P-IIH           0           0           0           0
CSNP          73498           0           0           0
PSNP              0          28           0           0

PDU        Received     Flooded  RcvAuthErr OtherRcvErr  ReTransmit
LSP          117526        2922           0           0           0

DIS elections:    24
SPF calculations: 55836
LSPs sourced:     3
LSPs refreshed:   273
LSPs purged:      3183

ServiceRouter#
```

The following is sample output from the **show statistics isis** command that shows all traffic counters for a specific interface:

```
ServiceRouter# show statistics isis GigabitEthernet 1/0

IS-IS statistics for GigabitEthernet 1/0:
PDU        Received        Sent  RcvAuthErr OtherRcvErr
LAN-IIH           0           0           0           0
P2P-IIH           0           0           0           0
CSNP              0           0           0           0
PSNP              0           0           0           0

PDU        Received     Flooded  RcvAuthErr OtherRcvErr  ReTransmit
LSP               0           0           0           0           0

DIS elections:    2

ServiceRouter#
```

show statistics movie-streamer

To display statistics for the Movie Streamer, use the **show statistics movie-streamer** command in EXEC configuration mode.

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.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Execution Order of Rule Actions

The order in which the rule actions are implemented for Windows Media Streaming and Movie Streamer is the order in which they were configured, except for the validate-url-signature action. If the rule pattern associated with the validate-url-signature action is matched, regardless of the configuration order of the rules, the validate-url-signature action is performed before any other action.

1. validate-url-signature
2. block or allow

Note NOTE: The allow and block actions carry the same precedence. The order of implementation depends on the order of configuration between allow and block actions. Other actions always take precedence over allow.

3. redirect (before cache lookup)
4. rewrite (before cache lookup)

Note Windows Media Streaming supports all rule actions. Movie Streamer supports the following rule actions: allow, block, redirect, rewrite, and validate-url-signature.

For the Web Engine and Flash Media Streaming, the Service Rule file must be used if service rules are to be configured. See the *Cisco Internet Streamer CDS 3.2 Software Configuration Guide*.

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


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
Validate URL Signature:         0
```

Related Commands

Command	Description
movie-streamer	Enables and configures the Movie Streamer server.
show movie-streamer	Displays the Movie Streamer configuration.

show statistics netstat

To display SE Internet socket connection statistics, use the **show statistics netstat** command in EXEC configuration mode.

show statistics netstat

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 0-7 describes the fields shown in the **show statistics netstat** display.

Table 0-7 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 radius

To display SE RADIUS authentication statistics, use the **show statistics radius** command in EXEC configuration mode.

show statistics radius

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

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

Command	Description
clear	Clears the HTTP object cache, the hardware interface, statistics, archive working transaction logs, and other settings.
radius-server	Configures the RADIUS authentication.
show radius-server	Displays the RADIUS server information.

show statistics replication

To display delivery service replication status and related statistical data, use the following **show statistics replication** command in EXEC configuration mode.

On the CDSM:

show statistics replication {**content-items** *content_name* **selected-delivery-service** *content_origin_name delivery_service_name* {**all-service-engines** [**refetch**] | **service-engine** *service_engine_name* [**fully-replicated** | **not-fully-replicated** | **refetch**} | **delivery-service** [**selected-delivery-service** *content_origin_name delivery_service_name*| **item** *url* **selected-delivery-service** *content_origin_name delivery_service_name* | **service-engines** **selected-delivery-service** *content_origin_name delivery_service_name* [**refetch** | **service-engine** *service_engine_name*]}

On the SE:

show statistics replication {**content-items** *content_name* **selected-delivery-service** *content_origin_name delivery_service_name* [**fully-replicated** | **not-fully-replicated**] | **delivery-service** [**selected-delivery-service** *content_origin_name delivery_service_name*}

Syntax Description

content-items	Displays the replication status of the specified content items.
content_name	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.
content_origin_name	Content origin name.
delivery_service_name	Delivery service name.
all-service-engines	For all service engines in a delivery service.
refetch	Initiates a request to re-fetch the status.
fully-replicated	Content items that are fully replicated.
not-fully-replicated	Content items that are not fully replicated.
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.
url	URL of the content item.
service-engines	Displays the replication status of the specified SEs.
service-engine	Displays the replication status of the specified service engine.
service_engine_name	Service engine name.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The **show statistics replication delivery-service** command displays the delivery service replication status on the CDSM and the SE.

Table 0-8 describes the fields shown in the **show statistics replication delivery-service** display.

Table 0-8 show statistics replication delivery-service Field Descriptions

Field	Description
Delivery Service	Delivery service name.
State	Overall state of the delivery service. Values are Complete or Failed.
Status	Replication status. Values are Red for failure and Green for success.
User Selected Content Acquirer	Name of the Content Acquirer that has been selected for delivery service.
Current Content Acquirer	Name of the currently acting Content Acquirer 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.
Content Origin	Origin of content.
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 Content Acquirer, states are Acquiring Content, Rechecking Content, or Completed.
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.

The **show statistics replication content-items** command displays the progressive file count status during acquisition and replication.

Table 0-9 describes the fields shown in the **show statistics replication content-items** display.

Table 0-9 show statistics replication content-items Field Descriptions

Field	Description
Content URL	URL of the replicated content.
Status	Indicates if the content was complete.
Size	Size of the file.
Modification Time	Displays the UTC time the content was replicated.

Examples

The following example shows how to display the statistics for the replication delivery service on a CDSM:

```
CDSM# show statistics replication delivery-service selected-delivery-service XXXX-iptv
XXXX-ds1
Delivery Service: XXXX-ds1
State: Completed
Status: Green
User Selected Content Acquirer: XX-nas-se01
Current Content Acquirer: XX-nas-se01
Receiver SEs Completed: 0
Receiver SEs In Progress: 0
Receiver SEs Failed: 0
Receiver SEs Not Responding: 0

Displaying Device Acquisition Replication Status
Device: XX-nas-se01 (SE ID: 111)
Delivery Service: XXXX-ds1 (Delivery Service ID: 222)
Content Origin: XXXX-iptv
Type: Acquirer
State: Completed
Status: Green
Completed: 579
To Do: 0
Failed: 0
Total: 579
Last Report Time: Tue Aug 30 20:05:03 GMT 2011
Disk Quota Used: 270.715 GB
Manifest Last Modified: Tue Aug 30 19:33:32 GMT 2011
Manifest Last Check: Tue Aug 30 20:04:47 GMT 2011
Manifest State: Completed
```

The following example shows how to display the statistics for the replication delivery service on an SE:

```
ServiceEngine# show statistics replication delivery-service selected-delivery-service
XXXX-iptv XXXX-ds1
Displaying Device Acquisition Replication Status
Device: XX-nas-se01 (SE ID: 111)
Delivery Service: XXXX-ds1 (Delivery Service ID: 222)
Content Origin: XXXX-iptv
Type: Acquirer
State: Completed
Status: Green
Completed: 579
To Do: 0
Failed: 0
Total: 579
Last Report Time: Tue Aug 30 20:13:24 GMT 2011
Disk Quota Used: 270.715 GB
Manifest Last Modified: Tue Aug 30 19:33:32 GMT 2011
```

```
Manifest Last Check: Tue Aug 30 20:12:57 GMT 2011
Manifest State: Completed
```

The following example shows how to display the statistics for replication content items on an SE:

```
ServiceEngine# show statistics replication content-items * selected-delivery-service
jerry-iptv dtnas-ds1
Gathering replication status may take some time.... (enter ctrl-c to stop)

There are 579 content items for Delivery Service: 'XXXX-ds1', Content Origin: 'XXXX-iptv'
(Delivery Service ID 111) that match the request.

Content URL: http://14.6.0.2/isilon_prepos/largefile/nastest_4
Status: Complete
Size: 478.318 MB
Modification Time: 00:44:04 03-25-2011


Content URL: http://14.6.0.2/isilon_prepos/largefile/nastest_70
Status: Complete
Size: 478.318 MB
Modification Time: 00:47:15 03-25-2011


Content URL: http://14.6.0.2/isilon_prepos/largefile/nastest_583
Status: Complete
Size: 478.318 MB
Modification Time: 00:56:19 03-25-2011


Content URL: http://14.6.0.2/isilon_prepos/largefile/nastest_464
Status: Complete
Size: 478.318 MB
Modification Time: 01:04:21 03-25-2011

<Output truncated>
```

show statistics service-router

To display Service Router statistics, use the **show statistics service-router** command in EXEC configuration mode.

show statistics service-router {**all** | **content-origin** content_*name* | **dns** | **history** | **keepalive** | **routing** {**geo-location** | **proximity**} | **se** *se_name* | **summary**}

Syntax Description

all	Displays all statistics.
content-origin	Displays content origin specific statistics.
content_name	Content origin name to show.
dns	Displays DNS statistics.
history	Displays statistics history.
keepalive	Displays keepalive statistics.
routing	Displays routing statistics.
geo-location	Displays routing geo location-related statistics.
proximity	Displays routing proximity-related statistics.
se	Displays Service Engine specific statistics.
se_name	Service Engine name to show.
summary	Displays summary statistics.

Command Defaults

None

Command Modes

EXEC configuration mode.

Examples

The following example shows how to display the content origin-specific statistics on the number of requests and redirects:

```
ServiceRouter# show statistics service-router content-origin

----- SR Statistics Of Content Origin -----
domain: sr.ABC.com (Origin Server: ABC.com)
HTTP Requests (normal) :                    0
HTTP Requests (ASX)    :                    0
HTTP Requests (API)    :                    0
RTSP Requests          :                    0
RTMP Requests          :                    0
HTTP 302 Redirects     :                    0
ASX Redirects          :                    0
HTTP API Redirects     :                    0
RTSP Redirects         :                    0
RTMP Redirects         :                    0
Overflow Redirects     :                    0

----- SR Statistics Of Content Origin -----
domain: cdsfms.com (Origin Server: 171.71.50.185, Alternate Domain: 171.71.50.18
5)
```

```
HTTP Requests (normal) :                    0
HTTP Requests (ASX)    :                    0
HTTP Requests (API)    :                    0
RTSP Requests          :                    0
RTMP Requests          :                    0
HTTP 302 Redirects     :                    0
ASX Redirects          :                    0
HTTP API Redirects     :                    0
RTSP Redirects         :                    0
RTMP Redirects         :                    0
Overflow Redirects     :                    0

----- SR Statistics Of Content Origin -----
domain: chunliu.com (Origin Server: 72.163.255.111)
HTTP Requests (normal) :                    0
HTTP Requests (ASX)    :                    0
HTTP Requests (API)    :                    0
RTSP Requests          :                    0
RTMP Requests          :                    0
HTTP 302 Redirects     :                    0
ASX Redirects          :                    0
HTTP API Redirects     :                    0
RTSP Redirects         :                    0
RTMP Redirects         :                    0
Overflow Redirects     :                    0

----- SR Statistics Of Content Origin -----
domain: install3.com (Origin Server: 10.74.115.24)
HTTP Requests (normal) :                    0
HTTP Requests (ASX)    :                    0
HTTP Requests (API)    :                    0
RTSP Requests          :                    0
RTMP Requests          :                    0
HTTP 302 Redirects     :                    0
ASX Redirects          :                    0
HTTP API Redirects     :                    0
RTSP Redirects         :                    0
RTMP Redirects         :                    0
Overflow Redirects     :                    0
V2-CDE220-2#
```

The following example shows how to display the DNS statistics, including the number of DNS queries for each type (Content Origin FQDN, Service Engine aliases), and the response sent (aliases for down Service Engines, unknown domains, failed, dropped).

:

```
ServiceRouter# show statistics service-router dns

----- SR DNS Statistics -----
Total DNS queries             :                 0
    Content Origin FQDNs      :                 0
    Service Engine aliases    :                 0
    Aliases for Down SEs      :                 0
    Unknown domains           :                 0
    PTR queries               :                 0
    Failed                    :                 0
    Dropped                   :                 0

ServiceRouter#
```

The following example shows how to display the statistics history on the number of redirect requests (maximum, minimum, average, last [in the past hour or minute]):

```
ServiceRouter# show statistics service-router history

----- SR Statistics History -----
Type         Minimum   Maximum   Average      Last (in past hour/per minute)
---------- --------- --------- --------- ---------
REQUESTS           0         0         0         0
REDIRECTS          0         0         0         0
```

The following example shows how to display keepalive statistics on the number of keepalives received from Service Engines, unknown source, and number of keepalives dropped:

```
ServiceRouter# show statistics service-router keepalive

----- SR Keepalive Statistics -----
    Dropped                   :                 0
    Service Engine keepalives :                 0
    From unknown source       :                 0

ServiceRouter#
```

The following example shows how to display statistics to show which routing method is used in redirection to SEs:

```
ServiceRouter# show statistics service-router routing

----- SR Routing Statistics -----
    Network Redirects         :                 0
    Proximity Redirects       :                 0
    Geo Location Redirects    :                 4
    Zero Network Redirects    :                 0
    Last Resort Redirects     :                 1

ServiceRouter#
```

The following example shows how to display geo location-related statistics showing the number of cache hits, cache misses and errors.

```
ServiceRouter# show statistics service-router routing geo-location

----- SR Geo Location Routing Statistics -----
    Cache Hits                :                 3
    Cache Misses              :                 2
    Errors                    :                 1

ServiceRouter#
```

The following example shows how to display proximity-related statistics showing the number of cache hits, cache misses and errors.

```
ServiceRouter# show statistics service-router routing proximity

----- SR Proximity Routing Statistics -----
    Cache Hits                :                 2
    Cache Misses              :                 3
    Errors                    :                 2

ServiceRouter#
```

The following example shows how to display Service Engine statistics including liveness of the SE, number of redirects to that particular SE, and the total number of keepalives received from that SE.

```
ServiceRouter# show statistics service-router se

----- Statistics Of SE: V2-CDE220-1 -----
Aliveness               : down
HTTP 302 Redirects      :                  0
ASX Redirects           :                  0
HTTP API Redirects      :                  0
RTSP Redirects          :                  0
RTMP Redirects          :                  0
DNS Redirects           :                  0
Number Of Keepalives    :                  0

----- Statistics Of SE: V2-CDE220-3 -----
Aliveness               : down
HTTP 302 Redirects      :                  0
ASX Redirects           :                  0
HTTP API Redirects      :                  0
RTSP Redirects          :                  0
RTMP Redirects          :                  0
DNS Redirects           :                  0
Number Of Keepalives    :                  0
V2-CDE220-2#
```

The following example shows how to display summary statistics including the number of requests received, requests redirected, requests served, and requests not redirected:

```
ServiceRouter# show statistics service-router summary

----- SR Summary Statistics -----
Requests Received          :                  1
  HTTP Requests (normal)   :                  0
  HTTP Requests (ASX)      :                  0
  HTTP Requests (API)      :                  0
  RTSP Requests            :                  1
  RTMP Requests            :                  0
  DNS Requests             :                  0

Requests Served            :                  0
  HTTP Requests Served     :                  0

Requests Redirected        :                  1
  HTTP 302 Redirects       :                  0
  ASX Redirects            :                  0
  HTTP API Redirects       :                  0
  RTSP redirects           :                  1
  RTMP redirects           :                  0
  DNS redirects            :                  0

Requests Overflowed        :                  0
  HTTP 302 Redirects       :                  0
  ASX Redirects            :                  0
  HTTP API Redirects       :                  0
  RTSP redirects           :                  0
  RTMP redirects           :                  0
  DNS redirects            :                  0

Requests Not Redirected    :                  0
  No SE Covering Client    :                  0
  Unknown Content Origin   :                  0
  Invalid Requests         :                  0
  Session limit exceeded   :                  0
  Bandwidth limit exceeded :                  0

  "Stale SE" Requests      :                  0
```

Related Commands

Command	Description
service-router	Configures service routing.
show service-router	Displays the Service Router configuration.

show statistics services

To display SE services statistics, use the **show statistics services** command in EXEC configuration mode.

show statistics services

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 0-10 describes the fields shown in the **show statistics services** display.

Table 0-10 show statistics services Field Descriptions

Field	Description
Port Statistics	Service-related statistics for each port on the WAAS[1] device.
Port	Port number.
Total Connections	Number of total connections.

1. WAAS = Wide Area Application Service

Related Commands

Command	Description
show services	Displays the services-related information.

show statistics snmp

To display SE Simple Network Management Protocol (SNMP) statistics, use the **show statistics snmp** command in EXEC configuration mode.

show statistics snmp

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 0-11 describes the fields shown in the **show statistics snmp** display.

Table 0-11 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.

Table 0-11 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

Command	Description
show snmp	Displays the SNMP parameters.
snmp-server community	Configures the community access string to permit access to the SNMP.
snmp-server contact	Sets the system server contact string.
snmp-server enable	Enables the SE to send SNMP traps.
snmp-server group	Defines a user security model group.
snmp-server host	Specifies the hosts to receive SNMP traps.
snmp-server location	Sets the SNMP system location string.
snmp-server notify inform	Configures the SNMP notify inform request.
snmp-server user	Defines a user who can access the SNMP engine.

show statistics srp

To display SRP statistics information, use the **show statistics srp** command in Privileged EXEC configuration mode.

show statistics srp

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Privileged EXEC configuration mode.

Usage Guidelines

This command displays SRP statistics information.

Examples

The following example shows sample output from the **show statistics srp** command.

```
ServiceRouter# show statistics srp
                            Sent     Received    Neighbors
Join request                 504          493            0
Join response                493          492            0
LS exchange request         7447         7317            0
LS exchange response        7317         7447            0
Route exchange request      3469         3743            8
Route exchange response     3742         3469            9
Ping request               39570        39405            1
Ping response              39405        39530            0
Lookup request              4610         2920            0
Lookup response             2920         4582            0
Ping traceroute request        0            0            0
Ping traceroute response       0            0            0
Request Retry                  0
Pkt at wrong interface         0
Malform packet                 0
Mismatched domain ID           1

ServiceRouter#
```

In the **show statistics srp** output, the “Pkt at wrong interface” statistic for received packets indicates that packets have arrived at an interface that is not configured as a network-facing interface. For Pkt at wrong interface, the Sent and Neighbors values are always 0.

Related Commands

Command	Description
show srp leafset	Displays SRP leafset information.
show srp neighbor	Displays SRP neighbor information.
show srp route	Displays route information for a Proximity Engine to its neighbor nodes on the same DHT ring.

show statistics tacacs

To display Service Engine TACACS+ authentication and authorization statistics, use the **show statistics tacacs** command in user EXEC configuration mode.

show statistics tacacs

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

User EXEC configuration mode.

Usage Guidelines

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

Command	Description
clear	Clears the HTTP object cache, the hardware interface, statistics, archive working transaction logs, and other settings.
show tacacs	Displays TACACS+ authentication protocol configuration information.
tacacs	Configures TACACS+ server parameters.

show statistics tcp

To display SE Transmission Control Protocol (TCP) statistics, use the **show statistics tcp** command in EXEC configuration mode.

show statistics tcp

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 0-12 describes the fields shown in the **show statistics tcp** display.

Table 0-12 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 because of rate limiting or resource shortage.
Connections established	Number of incoming connections that have been set up.
Connections resets received	Number of RSTs[1] received by the SE.
Connection resets sent	Number of 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 because of 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 0-12 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 SYN^2 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 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 has 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 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.
Packets pruned from receive queue	Number of packets that the TCP drops from the receive queue (usually because of low memory).

Table 0-12 show statistics tcp Field Descriptions (continued)

Field	Description
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 ARPs[3] 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 PAWS[4] 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.
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 because of a resource shortage.

Table 0-12 show statistics tcp Field Descriptions (continued)

Field	Description
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 ACK[5] 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 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 0-12 show statistics tcp Field Descriptions (continued)

Field	Description
TCP SACK reneging	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 FACK[6] 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 SACK[7] 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 D-SACK[8] 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 0-12 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 because of 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 cwnd[9] shrunk because the SE failed to recover from a 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 is only one or two duplicate ACKs before the reordered segment is processed, which then generates 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 0-12 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: • 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. • 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 sent 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 0-12 show statistics tcp Field Descriptions (continued)

Field	Description
TCP DSACK old packets sent	Number of 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.

Table 0-12 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.

1. RST = reset
2. SYN = synchronized
3. ARP = Address Resolution Protocol
4. PAWS = Protection Against Wrapped Sequence
5. ACK = acknowledgment
6. FACK = Forward Acknowledgment
7. SACK = Selective Acknowledgment
8. D-SACK = Duplicate Selective Acknowledgment
9. cwnd = congestion window

Related Commands

Command	Description
clear	Clears the HTTP object cache, the hardware interface, statistics, archive working transaction logs, and other settings.

show statistics transaction-logs

To display SE transaction log export statistics, use the **show statistics transaction-logs** command in EXEC configuration mode.

show statistics transaction-logs

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

To display the transaction log export statistics, you must first configure the FTP server.

Table 0-13 describes the fields shown in the **show statistics transaction-logs** display.

Table 0-13 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.
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

Command	Description
clear	Clears the HTTP object cache, the hardware interface, statistics, archive working transaction logs, and other settings.
show transaction-logging	Displays the transaction log configuration settings and a list of archived transaction log files.
transaction-log force	Forces the archive or export of the transaction log.

show statistics udp

To display SE User Datagram Protocol (UDP) statistics, use the **show statistics udp** command in EXEC configuration mode.

show statistics udp

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 0-14 describes the fields shown in the **show statistics udp** display.

Table 0-14 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 web-engine

To display the Web Engine statistics, use the **show statistics web-engine** command in EXEC configuration mode.

show statistics web-engine [**abr** {**generic-tracking-app** [**file | session | summary**] **| hls-media-app** [**detail | fragment-file | manifest-file | session | summary**] **| smoothhd-media-app** [**detail | fragment-file | manifest-file | meta-file | session | summary**] **| zeri-media-app** [**detail | fragment-file | manifest-file | meta-file | summary**]} **| detail | error summary | key-client | performance | usage**]

Syntax Description

abr	(Optional) Adaptive Bit-Rate streaming statistics.
generic-tracking-app	(Optional) Displays Generic-Tracking-App statistics.
hls-media-app	(Optional) Displays Hls-Media-App statistics.
detail	(Optional) Displays Hls-Media-App Detail Statistics.
fragment-file	(Optional) Displays Hls-Media-App Fragment-File Statistics.
manifest-file	(Optional) Displays Hls-Media-App Manifest-File Statistics.
meta-file	(Optional) Displays Hls-Media-App Meta-File Statistics.
session	(Optional) Displays Session Statistics.
summary	(Optional) Displays Hls-Media-App Summary.
smoothhd-media-app	Displays SmoothHD-Media-App statistics.
detail	Displays the SmoothHD-Media-App Detail Statistics.
fragment-file	Displays the SmoothHD-Media-App Fragment-File Statistics.
manifest-file	Displays the SmoothHD-Media-App Manifest-File Statistics.
meta-file	Displays the SmoothHD-Media-App Meta-File Statistics.
summary	Displays the SmoothHD-Media-App Summary.
zeri-media-app	Displays the Zeri-Media-App statistics.
detail	Displays the Zeri-Media-App Detail Statistics.
fragment-file	Displays the Zeri-Media-App Fragment-File Statistics.
manifest-file	Displays the Zeri-Media-App Manifest-File Statistics.
meta-file	Displays the Zeri-Media-App Meta-File Statistics.
summary	Displays the Zeri-Media-App Summary.
detail	(Optional) Displays detail statistics.
error	(Optional) Displays error statistics.
summary	Displays statistics based on 4xx/5xx response codes.
key-client	(Optional) Displays key client statistics.
performance	(Optional) Displays performance statistics.
usage	(Optional) Displays usage statistics.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The Web Engine must be running to see the statistics. The Web Engine is running by default.

Note A client request to an edge SE triggers a liveness query to the upstream SEs and Content Acquirer. Even after the client connection is closed, the liveness query continues for up to ten minutes. This is to keep the SEs ready with liveness states for subsequent client requests.

Note The **show statistics web-engine detail** command output also displays Web Engine memory usage. This can increase to greater than 2 GB and can stay above 2 GB even after traffic subsides. This is expected behavior and does not indicate a memory leak.

Table 0-15 describes the fields shown in the **show statistics web-engine** display.

Table 0-15 show statistics web-engine Field Descriptions

Field	Description
HTTP Request Info Statistics	
Num Lookups	Number of CAL lookups done.
Preposition Hit	Number of preposition hit requests. This statistic is only incremented at the end of the session life.
External Hit	Displays NAS Origin Hit count.
Cache Hit	Number of requests that resulted in a cache hit. This statistic is only incremented at the end of the session life.
Cache Miss	Number of requests that resulted in a cache miss (the web object was not available in the cache).
Partial Cache Hit	Number of cacheable requests that were partial cache hits. This statistic is only incremented at the end of the session life.
Cache Bypass	Whenever the Web Engine receives either a large file range request or a request type that it cannot cache. This statistics counter increases and the request file is not cached. This statistic is only incremented at the end of the session life.
Live Miss	Session miss for MP3 Live streaming over HTTP.
Live Hit	Session hit for MP3 Live streaming over HTTP.
ASX Meta Response	Incremented when a Windows Media Live Request(.asx) request is processed by the Web Engine.
HTTP Request Type Statistics	
Get Requests	Total Get requests.
Post Requests	Total Post requests.
Head Requests	Total Head requests.
Range Requests Received	Range requests from clients.
Range Requests Sent	Requests sent to OS liveness query.

Table 0-15 show statistics web-engine Field Descriptions (continued)

Field	Description
Revalidation Requests Received	Revalidation requests from clients. This counter is incremented only when an If-Modified-since (IMS) request is received by the Streamer.
Revalidation Requests Sent	Revalidation requests to OS liveness query.
Liveness Query	Liveness query received from the downstream SE. Liveness queries are sent even when there are no client requests and liveness updates are sent every ten minutes, so it is not mandatory to have client request in order to generate a liveness query.
Streaming Redirected Requests	The number of request handed over to WMT.
Local Requests	Requests from other Protocol Engines.
Play Live Requests	WMT Live requests.
Total Outgoing Requests	Total number of unique request that web-engine sent to the upstream.
Origin Server Redirected Requests	Cumulative sum of requests coming to all delivery services on the SE for which this feature is enabled. This number is cleared when the Web Engine is restarted or the **clear statistics all** command is executed.
HTTP Authorization Statistics	
Authorization Allow	Number of authorization requests being allowed.
Authorization No Cache	Number of authorization requests being applied with the No-cache rule.
Authorization Force Revalidate	Number of authorization requests being applied with the Force revalidate rule.
Authorization Deny	Number of authorization requests being denied.
Authorization Rewrite	Number of authorization requests being applied with the rewrite rule.
Authorization GenerateSign	Number of authorization requests being applied with the generate sign rule.
Authorization Redirect	Number of authorization requests being redirected.
Authorization Resolve	Number of authorization requests being applied with the URL-Resolve rule.
WMT (HTTP) Rule Statistics	
Allow	Number of WMT (HTTP) rules being allowed.
Block	Number of WMT (HTTP) rules being blocked.
URL Redirect	Number of URL redirect statistics.
URL Rewrite	Number of URL rewrite statistics.

Table 0-15 show statistics web-engine Field Descriptions (continued)

Field	Description
Validate URL Signature	Total number of requests for which URL sign validation was performed.
No Cache	Number of WMT (HTTP) rules being applied with no cache.
HTTP Error Statistics	
Client Errors	Number of 4xx errors.
Server Errors	Number of 5xx errors.
Bad Requests	Number of HTTP request corruptions.
Error Response Hit	Number of error response cache hits.
Error Response Miss	Number of error response cache misses. With error response caching enabled, the error responses like 404 and 503 could be cached.
HTTP Performance Statistics	
Total Bytes In	Total bytes in. This statistic is only incremented at the end of the session life.
Total Bytes Out	Total bytes out. This statistic is only incremented at the end of the session life.
Total Requests	Total requests since last web-engine statistics cleared time.
Average Request Per Second	Average requests per second. **Note** To get an accurate request per second reading in a given time period, clear the Web Engine statistics first and then generate the **shows statistics web-engine** command.
Average Bytes Per Second	Average number of bytes per second since the last web-engine statistics were cleared.
Web-Engine Detail Statistics	
Active HTTPSession	HTTPSession is unique to the end user connection. This value counts the HTTP request targeted to port 80, regardless of which Protocol Engine handles the request. The sample rate and Real-Time value are calculated at the time the command is executed.
Active DataSource	Sources used to fetch the data. Disk for cache hit; OS for cache miss.
Active HTTPDataFeed	Active connections to the Origin Server or upstream SE's to fetch Data.
Active HTTPData SourceFinder	The number of active DataSourceFinder present. DataSourceFinder is responsible for creating the datasource.
Active HTTPTransact-ion	On a given session, this is the number of active pipeline transactions the Web Engine is currently processing.
Pending HTTPTransact-ion	On a given session, this is the number of pending pipeline transactions the Web Engine has yet to process.
Active ServerXact	HTTP Request currently under process.

Table 0-15 show statistics web-engine Field Descriptions (continued)

Field	Description
Total HTTPConnection	Total outgoing HTTP connection to upstream.
Active HTTPConnection	HTTP connection currently serving request.
Idle Proxy HTTPConnection	Intra-SE connection in the idle queue.
Idle Origin HTTPConnection	Non-Intra-SE/Origin Server connection in the idle queue.
Memory Hit	Number of requested files available in /tmpfs. This statistic is only incremented at the end of the session life.
Cut-Thru Counter	Number of cached files deleted without moving to disk.
Memory Usage	Memory usage of the Web Engine process.
WebEngine Trickle Status	This flag is set when the Web Engine has exceeded thresholds but cannot restart because of outstanding sessions. When the transactions on HTTPSessions complete, it looks at this trickle flag and terminates the connection instead of processing the next request on the connection. This flag is reset to 0 when memory usage is low because the number of sessions has decreased. If the number of sessions goes to 0 and memory usage is still high, the Trickle flag is set and the web-engine restarts.
Outstanding Content Create Requests	Allocates a disk and a file path for a given URL. The protocol engine uses this location to store the downloaded content. The number of outstanding creates reflect the number of such requests to the CAL module that have been submitted but were not completed.
Outstanding Content Lookup Requests	Translates the URL from an end client into a disk path in the case of a cache hit (based on a previous create). In the case of cache miss, it would give the route from where the content can be found. The counter number of outstanding lookups reflects the number of pending requests.
Outstanding Content Delete Requests	Deletes a file created by CAL. The number of outstanding deletes reflects the number of pending delete requests.
Outstanding Content Update Requests	Updates the Content metadata CAL. The number of outstanding updates reflect the number of pending update requests submitted to CAL.
Outstanding Content Popularity Update Requests	Updates the Content Popularity metadata CAL. The number of outstanding updates reflect the number of pending update requests submitted to CAL.

Note The “Total Bytes Out” statistic counts the header length but the “Total Bytes In” statistic does not.

Examples

The following example shows how to display the detailed Web Engine statistics:

```
ServiceEngine# show statistics web-engine abr generic-tracking-app file

Generic Session File Statistics
-----------------------
Preposition Hit               :                   0
Alien Hit                     :                   0
Cache Hit                     :                   0
Cache Miss                    :                   0
Partial Cache Hi              :                   0
Cache Bypass                  :                   0

ServiceEngine# show statistics web-engine abr generic-session-app session

Session Statistics
-----------------------
Active Generic sessions                           :                   0
Sessions Created                                  :                   0
Sessions Created-Internal SessID                  :                   0
Sessions Recreated With Received Cookie           :                   0
Sessions Deleted-Inactive                         :                   0
Requests Failed to Track Internal Error           :                   0
Requests Failed to Track Client IP Invalid        :                   0
Requests Failed to Track SessID Collision         :                   0
Requests Failed to Track                          :                   0
Requests Failed to Track Session in Deletion      :                   0
Start Notifications sent                          :                   0
Start Notification send failed                    :                   0
Stop Notifications sent                           :                   0
Stop Notification send failed                     :                   0
Notification message send aborted due to DNS failure :                0
Requests Internal SessId With Cookie Disabled     :                   0

ServiceEngine# show statistics web-engine abr generic-tracking-app summary

Generic Session Summary Statistics
-----------------------
Preposition Hit               :                   0
External Hit                  :                   0
Cache Hit                     :                   0
Cache Miss                    :                   0

ServiceEngine# show statistics web-engine detail

HTTP Request Info Statistics
-----------------------
Num Lookups                   :                 4212308
Preposition Hit               :                       0
External Hit                  :                       0
Cache Hit                     :                   30109
Cache Miss                    :                 4043651
Partial Cache Hit             :                       0
Cache Bypass                  :                       0
Live Miss                     :                       0
Live Hit                      :                       0
ASX Meta Response             :                       0

HTTP Request Type Statistics
-----------------------
Get Requests                  :                 4215164
Post Requests                 :                       0
Head Requests                 :                       0
Range Requests Received       :                      10
```

```
Range Requests Sent            :                        0
Revalidation Requests Received :                    26921
Revalidation Requests Sent     :                  1003660
Liveness Query                 :                     6832
WMT(http) Redirected Requests  :                        0
Local Requests                 :                        0
Play Live Requests             :                        0
Total Outgoing Requests        :                  4073031

HTTP Authorization Statistics
----------------------
Authorization Allow            :                  4212638
Authorization No Cache         :                        0
Authorization Force Revalidate :                        0
Authorization Deny             :                        0
Authorization Rewrite          :                        0
Authorization GenerateSign     :                        0
Authorization Redirect         :                        0
Authorization Resolve          :                        0

WMT(http) Rule Statistics
----------------------
Allow                          :                        0
Block                          :                        0
Url Redirect                   :                        0
Url Rewrite                    :                        0
Validate Url Signature         :                        0
No Cache                       :                        0

HTTP Error Statistics
----------------------
Client Errors                  :                        0
Server Errors                  :                   877658
Bad Requests                   :                        0
Error Response Miss            :                        0
Error Response Hit             :                        0

HTTP Performance Statistics
----------------------
Total Bytes In                 :             621029676477
Total Bytes Out                :             594801670055
Total Requests                 :                  4215255
Average Requests Per Second    :                    60.61
Average Bytes Per Second       :                8552759.45

Web-Engine Detail Statistics
----------------------
Active HTTPSession             :                       29
Active DataSource              :                      161
Active HTTPDataFeed            :                        0
Active HTTPDataSourceFinder    :                        0
Active HTTPTransaction         :                        1
Pending HTTPTransaction        :                        0
Active ServerXact              :                        0
Total HTTPConnection           :                       12
Active HTTPConnection          :                        0
Idle Proxy HTTPConnection      :                        0
Idle Origin HTTPConnection     :                       12
Memory Hit                     :                      377
Cut-Thru Counter               :                  7390705
Memory Usage                   :               2297475072
WebEngine Trickle Status       :                        0
Outstanding Content Create Requests:                    0
Outstanding Content Lookup Requests:                    0
```

```
Outstanding Content Delete Requests:                        0
Outstanding Content Update Requests:                        0
Outstanding Content Popularity Update Requests:                     0
Statistics was last cleared on Wednesday, 24-Aug-2011 22:18:08 PDT.
ServiceEngine#

The following example shows how to display the statistics for theHLD-Media-App:
ServiceEngine# show statistics web-engine abr hls-media-app

Media Manifest File Statistics
-----------------------
Preposition Hit                                     :                   0
Alien Hit                                           :                   0
Cache Hit                                           :                   0
Cache Miss                                          :                   0
Partial Cache Hit                                   :                   0
Cache Bypass                                        :                   0

Media Fragment File Statistics
-----------------------
Preposition Hit                                     :                   0
Alien Hit                                           :                   0
Cache Hit                                           :                   0
Cache Miss                                          :                   0
Partial Cache Hit                                   :                   0
Cache Bypass                                        :                   0

Media Detail Statistics
----------------------
Active Assets                                       :                   0
Active Manifest Files                               :                   0
Active Media Files                                  :                   0
Request Sent To Default App                         :                   0

Session Statistics
----------------------
Active Media sessions                               :                   0
Sessions Created                                    :                   0
Sessions Created-Internal SessID                    :                   0
Sessions Recreated With Received Cookie             :                   0
Sessions Deleted-Inactive                           :                   0
Sessions Deleted-Internal Error                     :                   0
Sessions Deleted-Expired Request                    :                   0
Sessions Deleted-Session ID Error                   :                   0
Requests Rejected-Client IP Invalid                 :                   0
Requests Rejected-SessID Collision                  :                   0
Requests Rejected-Failed to Track                   :                   0
Inline Key Requests                                 :                   0
Start Notifications sent                            :                   0
Start Notification send failed                      :                   0
Stop Notifications sent                             :                   0
Stop Notification send failed                       :                   0
Notification message send aborted due to DNS failure  :                 0
ServiceEngine#

The following example shows how to display the detailed statistics for the Zeri-Media-App:
ServiceEngine# show statistics web-engine abr zeri-media-app detail

Media Detail Statistics
----------------------
Active DataSource             :                     0
Request Sent To Default App   :                     0
ServiceEngine#
```

```
The following example shows how to display the summary for the Smooth-Media-App:
ServiceEngine# show statistics web-engine abr smoothhd-media-app summary

Media Summary Statistics
------------------------
Preposition Hit                :                          0
External Hit                   :                          0
Cache Hit                      :                          0
Cache Miss                     :                          0
ServiceEngine#
```

Related Commands

Command	Description
show web-engine	Displays the Web Engine information.
web-engine (EXEC)	Configures the Web Engine module.
web-engine (Global configuration)	Configures the Web Engine caching parameters.

show statistics wmt

To display the SE Windows Media Technologies (WMT) statistics, use the **show statistics wmt** command in EXEC configuration mode.

show statistics wmt {**all** | **bytes** {**incoming** | **outgoing**} | **cache** | **errors** | **multicast** | **requests** | **rule** | **savings** | **streamstat** [**incoming** | **live** | **outgoing** | **stream-id** *stream_id*] | **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. The range is from 1 to 999999.
stream_id	WMT stream ID to display.
usage	Displays current usage statistics.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The output of the **show statistics wmt** command includes information about WMT RTSP requests. For example, the output from the **show statistics wmt** command was changed as follows:

- RTSP-related information was added to the **show statistics wmt all** command output.
- Information about RTSPT 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** 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** command to display statistics of all incoming WMT streams, outgoing WMT streams, and streams with the specified ID.

Configuring the HTTP Allow and 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.

Table 0-16 describes the fields shown in the **show statistics wmt all** display.

Table 0-16 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.
Multicast nsc file Request	Number of multicast NSC file requests received. **Note** This field continuously increments for a single request if there are two SE locations in the same subnet. This is not valid and causes both SEs to send data to the same multicast address.
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.
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.
Remote RTSP	Number of remote RTSP bytes saved.
Multicast	Number of multicast bytes saved.

Table 0-16 show statistics wmt all Field Descriptions (continued)

Field	Description
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.
NTLM	
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.
By prepositioned content	Number of bytes saved for prepositioned content.

Table 0-16 show statistics wmt all Field Descriptions (continued)

Field	Description
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.
Concurrent Bandwidth to Remote Servers (Kbps)	Total amount of bandwidth being used (in kilobits per second) for concurrent remote server sessions.

Table 0-16 show statistics wmt all Field Descriptions (continued)

Field	Description
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 Incoming Bytes	Total number of bytes incoming as multicast-out streams.
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.
Cache Validation Statistics	
Fresh Content Requests	
Object Not Found	

Table 0-16 show statistics wmt all Field Descriptions (continued)

Field	Description
Revalidate Requests	
Revalidate Reasons	
Object Expired	
Min TTL Expired	
Max TTL Expired	
MBR Content	
Others	

Related Commands

Command	Description
clear	Clears the HTTP object cache, the hardware interface, statistics, archive working transaction logs, and other settings.
show wmt	Displays WMT bandwidth and proxy mode configuration.
wmt	Configures the WMT.

show tacacs

To display TACACS+ authentication protocol configuration information, use the **show tacacs** command in EXEC configuration mode.

show tacacs

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The **show tacacs** command displays the TACACS+ configuration for the Service Engine.

Table 0-17 describes the fields shown in the **show tacacs** display.

Table 0-17 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 fails 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 PAP[1] is the mechanism for password authentication.

Table 0-17 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.

1. PAP = Password Authentication Protocol

Related Commands

Command	Description
clear	Clears the HTTP object cache, the hardware interface, statistics, archive working transaction logs, and other settings.
show statistics tacacs	Displays the SE TACACS+ authentication and authorization statistics.
tacacs	Configures TACACS+ server parameters.

show tech-support

To view information necessary for the Cisco Technical Assistance Center (TAC) to assist you, use the **show tech-support** command in EXEC configuration mode.

show tech-support [**list-files** *directory_name* [**recursive**] | **page** | **service** {**acquisition-distribution** [**authentication** | **cms** | **flash-media-streaming** | **icap** | **kernel** | **movie-streamer** | **rules** | **web-engine** | **wmt**] | **authentication** [**acquisition-distribution** | **cms** | **flash-media-streaming** | **icap** | **kernel** | **movie-streamer** | **rules** | **web-engine** | **wmt**] | **cms** [**acquisition-distribution** | **authentication** | **flash-media-streaming** | **icap** | **kernel** | **movie-streamer** | **rules** | **web-engine** | **wmt**] | **flash-media-streaming** [**acquisition-distribution** | **authentication** | **cms** | **icap** | **kernel** | **movie-streamer** | **rules** | **web-engine** | **wmt**] | **icap** [**acquisition-distribution** | **authentication** | **cms** | **flash-media-streaming** | **kernel** | **movie-streamer** | **rules** | **web-engine** | **wmt**] | **kernel** [**acquisition-distribution** | **authentication** | **cms** | **flash-media-streaming** | **icap** | **movie-streamer** | **rules** | **web-engine** | **wmt**] | **movie-streamer** [**acquisition-distribution** | **authentication** | **cms** | **flash-media-streaming** | **icap** | **kernel** | **rules** | **web-engine** | **wmt**] | **rules** [**acquisition-distribution** | **authentication** | **cms** | **flash-media-streaming** | **icap** | **kernel** | **movie-streamer** | **web-engine** | **wmt**] | **web-engine** [**acquisition-distribution** | **authentication** | **cms** | **flash-media-streaming** | **icap** | **kernel** | **movie-streamer** | **rules** | **wmt**] | **wmt** [**acquisition-distribution** | **authentication** | **cms** | **flash-media-streaming** | **icap** | **kernel** | **movie-streamer** | **rules** | **web-engine**]}

Syntax Description

list-files	(Optional) Displays the list of files under a directory.
directory_name	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.

Command Defaults

None

Command Modes

EXEC configuration mode.

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 (bdflush)
    6     S   0      0      0 (kupdated)
    7     S   0      0      0 (scsi_eh_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 (snmpced)
 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    611 (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)
 2150    S   0      0      0 (rsvpd)
 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 (dfcontrolsvr)
 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 (snmpced)
 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 (dfcontrolsvr)
 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
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** command in EXEC configuration mode.

show telnet

Syntax Description

This command has no arguments or keywords.

Command Defaults

Enabled.

Command Modes

EXEC configuration mode.

Examples

The following example shows how to display the Telnet service details:

```
ServiceEngine# show telnet
telnet service is enabled
```

Related Commands

Command	Description
exec-timeout	Configures the length of time that an inactive Telnet or SSH session remains open.
telnet enable	Enables the Telnet services.

show transaction-logging

To display the transaction log configuration settings and a list of archived transaction log files, use the **show transaction-logging** command in EXEC configuration mode.

show transaction-logging

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

To display information about the current configuration of transaction logging on an SE, use the **show transaction-logging** command. Transaction log file information is displayed for HTTP and WMT caching proxy transactions and TFTP and ICAP transactions.

Examples

The following example shows how to display 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
```

```
  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 shows how to display 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

Command	Description
clear	Clears the HTTP object cache, the hardware interface, statistics, archive working transaction logs, and other settings.
show statistics transaction-logs	Displays the SE transaction log export statistics.
transaction-log force	Forces the archive or export of the transaction log.

show url-signature

To display the URL signature information, use the **show url-signature** command in EXEC configuration mode.

show url-signature

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

EXEC configuration mode.

Examples

The following example shows how to display 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** command in EXEC configuration mode.

show user {**uid** *num* | **username** *name*}

Syntax Description

uid	Displays the user's identification number.
num	Identification number. The range is from 0 to 65535.
username	Displays the name of user.
name	Name of the user.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 0-18 describes the fields shown in the **show user** display.

Table 0-18 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

Command	Description
clear	Clears the HTTP object cache, the hardware interface, statistics, archive working transaction logs, and other settings.
show users	Displays the specified users.
username	Establishes the username authentication.

show users

To display users, use the **show users** command in EXEC configuration mode.

show users administrative

Syntax Description

administrative	Lists users with administrative privileges.

Command Defaults

None

Command Modes

EXEC configuration mode.

Examples

The following example shows how to display the list of users with administrative privileges:

```
ServiceEngine# show users administrative
           UID USERNAME
           0 admin
```

Related Commands

Command	Description
clear	Clears the HTTP object cache, the hardware interface, statistics, archive working transaction logs, and other settings.
show user	Displays the user identification number and username information for a particular user.
username	Establishes the username authentication.

show version

To display version information about the software, use the **show version** command in EXEC configuration mode.

show version pending

Syntax Description

pending	Displays the version for pending upgraded image.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Table 0-19 describes the fields shown in the **show version** display.

Table 0-19 show version Field Descriptions

Field	Description
Version	CDS software version.
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.

Note If you update the CDS software on an SE, the new version displays in the **show version pending** command output, but it says, "Pending version will take effect after reload." You must reboot the device for the software update to take affect.

Examples

The follow example shows how to display the software version:

```
ServiceEngine# show version
Content Delivery System Software (CDS)
Copyright (c) 1999-2011 by Cisco Systems, Inc.
Content Delivery System Software Release 3.0.0 (build b460 Aug 28 2011)
Version: cde220-2g2-DEVELOPMENT[vcn-build1:/auto/vcn-u1/cdsis_release_builds/cds
is_3.0.0-b460/spcdn]

Compiled 05:55:01 Aug 28 2011 by ipvbuild
Compile Time Options: KQ SS

System was restarted on Mon Aug 29 11:56:58 2011.
The system has been up for 1 day, 23 hours, 32 minutes, 15 seconds.
```

```
ServiceEngine#
```

The following example shows how to display the pending software version:

```
ServiceEngine# show version pending
Pending version is CDS 3.0.0-b360, built on 05:17:52 Jun 19 2011 by ipvbuild
It will take effect after reload
ServiceEngine#
```

Related Commands

Command	Description
show flash	Displays the flash memory version and usage information.

show web-engine

To display the Web Engine information, use the **show web-engine** command in EXEC configuration mode.

show web-engine {**all** | **delivery-service-configuration** | **health**}

Syntax Description

all	Displays all Web Engine-related caching configuration.
delivery-service-configuration	Displays the Delivery Service configuration information.
health	Displays the Web-engine health information.

Command Defaults

None

Command Modes

EXEC configuration mode.

Examples

The following example shows how to display the Web Engine information:

```
ServiceEngine# show web-engine all
HTTP heuristic age-multipliers: 30%

Maximum time to live in days: 61

Minimum time to live in minutes: 60

Web-Engine Revalidation Disabled.

Web-Engine Cache Range Fill Enabled.

ServiceEngine#
```

The following example shows how to display the Web Engine health information:

```
ServiceEngine# show web-engine health

WebEngine - Virtual memory Usage
---------------------------------
Total memory usage                      :           1133268992 bytes [UnderLimit
]
Platform Virtual memory limit           :           3435973836 bytes
Glibc Caching Turn-Off Threshold        :           2061584301 bytes
Glibc memory Caching                    :                   ON

WebEngine - Alarm Status
-------------------------
memory_exceeded                         :                  OFF
max_session_exceeded                    :                  OFF
```

The following example shows how to display the Web Engine Delivery Service configuration:

```
ServiceEngine#

ServiceEngine# show web-engine delivery-service-configuration
```

```
Delivery Service Configuration
-----------------------------------
Delivery Service Id                                  : 355
Delivery Service Rfqdn                               : www.samreval.com
Delivery Service Ofqdn                                  : 7.7.7.7
Delivery Service Type                                   : Vod
Delivery Service BitRate                                : 5000
Delivery Service Max tmpfs File Size                    : 2097152
Delivery Service OutgoingCookie                         :
Delivery Service Dscp                                   : 0
Delivery Service Enable Download                        : Enabled
Delivery Service Enable Streaming Extensions            :
Delivery Service URL Hash Level for Cache Routing       : 0
Delivery Service Enable Error Caching                   : Disabled
Delivery Service Cacheable Error Responses              :
Delivery Service Content Flow Trace                     : Disabled
Delivery Service Filter Trace Flow                      : Disabled
Delivery Service Disable Small File Caching on Disk     : Disabled
Delivery Service Response Read Timeout                 :15 sec
ServiceEngine#
```

Related Commands

Command	Description
web-engine (EXEC)	Configures the Web Engine module.
web-engine (Global configuration)	Configures the Web Engine caching parameters.
show statistics web-engine	Displays the Web Engine statistics.

show wmt

To display Windows Media Technologies (WMT) bandwidth and proxy mode configuration, use the **show wmt** command in EXEC configuration mode.

show wmt [**bandwidth** [**incoming bypass-list**] | **detail** | **diagnostics** {**header-info** {**stream-file** *word* | **nsc-file** *.nsc_filename*} | **network-trace** *filename*} **http allow extension** | **proxy**]

Syntax Description

bandwidth	(Optional) Displays WMT bandwidth settings.
incoming	(Optional) Displays WMT incoming bandwidth settings.
bypass-list	Displays the WMT incoming bandwidth bypass list.
broadcast	(Optional) Displays the WMT broadcast configuration.
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.
word	An .asf, .wma, .wmv URL, or local file.
nsc-file	Displays the .nsc file headers.
.nsc_filename	Name of a local or remote WMT station.
network-trace	Displays WMT diagnostics information.
filename	Name of a local tcpdump file.
http	(Optional) Displays HTTP configurations.
allow	Displays the HTTP filename extensions allowed to be served using WMT.
extension	(Optional) Displays the list of HTTP filename extensions to be served using WMT.
proxy	(Optional) Displays proxy mode configuration.

Command Defaults

None

Command Modes

EXEC configuration mode.

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* command.
- nschead—Examine the .nsc file headers. To access the nschead tool, enter the **show wmt diagnostics header-info nsc-file** *.ncs-filename* 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* 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** 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** 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** 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 shows how to display 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

Command	Description
clear	Clears the HTTP object cache, the hardware interface, statistics, archive working transaction logs, and other settings.
show statistics wmt	Displays the SE WMT statistics.
wmt	Configures the WMT.

shutdown (interface configuration)

To shut down a specific hardware interface, use the **shutdown** command in interface configuration mode. 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.

Command Defaults

None

Command Modes

Interface configuration (config-if) mode.

Usage Guidelines

See the "interface" section on page 2-187 for alternative mechanism.

Examples

The following example shows how to shut down an interface configured on an SE:

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

Related Commands

Command	Description
interface	Configures a Gigabit Ethernet or port channel interface.
show interface	Displays the hardware interface information.
show running-config	Displays the current operating configuration.
show startup-config	Displays the startup configuration.

shutdown (EXEC)

To shut down the Service Engine (SE), Service Router (SR), or Content Delivery System Manager (CDSM), use the **shutdown** command in EXEC configuration mode.

shutdown [**poweroff**]

Syntax Description

poweroff	(Optional) Turns off the power after closing all applications and the operating system.

Command Defaults

None

Command Modes

EXEC configuration mode.

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 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** 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** 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 0-20 describes the shutdown and shutdown power-off operations for SEs.

Table 0-20 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, press the power button once to bring the SE back online.
File system check	Is not performed after you turn the power on again and reboot the SE.	Is not performed after you turn the power on again and reboot the SE.

You can enter the **shutdown** 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** 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.
```

Table 0-21 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.
Multicast 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.
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.

Table 0-21 show statistics wmt all Field Descriptions (continued)

Field	Description
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.
By prepositioned content	Number of bytes saved for prepositioned 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.

Table 0-21 show statistics wmt all Field Descriptions (continued)

Field	Description
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.
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.

Table 0-21 show statistics wmt all Field Descriptions (continued)

Field	Description
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.

```
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** 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

community_string	Community string that acts like a password and permits access to SNMP.
group	(Optional) Specifies the group to which this community name belongs.
group_name	(Optional) Name of the group.
rw	(Optional) Specifies read-write access with this community string.

Command 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 (config) mode.

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

Command	Description
snmp-server view	Defines a Version 2 SNMP (SNMPv2) MIB view.

snmp-server contact

To set the system server contact (sysContact) string, use the **snmp-server contact** command in Global configuration mode. To remove the system contact information, use the **no** form of this command.

snmp-server contact *line*

no snmp-server contact

Syntax Description

line	Identification of the contact person for this managed node.

Command Defaults

No system contact string is set.

Command Modes

Global configuration (config) mode.

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:

```
ServiceEngine(config)# snmp-server contact Dial System Operator at beeper # 27345
```

The following example shows how to reset the system contact string:

```
ServiceEngine(config)# no snmp-server contact
```

Related Commands

Command	Description
show snmp	Displays the SNMP parameters.
snmp-server community	Configures the community access string to permit access to the SNMP.
snmp-server enable traps	Enables the SE to send SNMP traps.
snmp-server group	Defines a user security model group.
snmp-server host	Specifies the hosts to receive SNMP traps.
snmp-server location	Sets the SNMP system location string.
snmp-server notify inform	Configures the SNMP notify inform request.
snmp-server user	Defines a user who can access the SNMP engine.
snmp-server view	Defines a SNMPv2 MIB view.

snmp-server enable traps

To enable the SE to send SNMP traps, use the **snmp-server enable traps** command in Global configuration mode. 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.

Command Defaults

This command is disabled by default. No traps are enabled.

Command Modes

Global configuration (config) mode.

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:

- Severity of the alarm (critical, major, or minor)
- Action (the alarm is raised or cleared)

Cisco Internet Streamer CDS 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.

Note Some SNMP traps are different between v1 and v2 and v3 when configure the trap.

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, 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. To configure the SE to send these SNMP notifications, 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. To enable multiple types of notifications, 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, configure at least one host using the **snmp-server host** command.

For a host to receive a trap, enable both the **snmp-server enable traps** command and the **snmp-server host** command for that host.

In addition, enable SNMP with the **snmp-server community** command.

To disable the sending of the MIB-II SNMP authentication trap, enter the **no snmp-server enable traps snmp authentication** command.

Examples

The following example shows how to enable 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

Command	Description
show snmp	Displays the SNMP parameters.
snmp-server community	Configures the community access string to permit access to the SNMP.
snmp-server contact	Sets the system server contact string.
snmp-server group	Defines a user security model group.
snmp-server host	Specifies the hosts to receive SNMP traps.
snmp-server location	Sets the SNMP system location string.
snmp-server notify inform	Configures the SNMP notify inform request.
snmp-server user	Defines a user who can access the SNMP engine.
snmp-server view	Defines a SNMPv2 MIB view.

snmp-server group

To define a user security model group, use the **snmp-server group** command in Global configuration mode. 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

name	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.
name	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.
name	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.
name	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.

Command Defaults

The default is that no user security model group is defined.

Command Modes

Global configuration (config) mode.

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).

Note Each community is associated with a group. Each group has a view and users are assigned to a group. If the group does not have a view associated with it, then users associated that group cannot access any MIB entry.

The Cisco Internet Streamer CDS 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 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 shows how to configure the SNMP group name, security model, and notify view on the SE:

```
ServiceEngine(config)# snmp-server group acme v1 notify mymib
```

Related Commands

Command	Description
show snmp	Displays the SNMP parameters.
snmp-server community	Configures the community access string to permit access to the SNMP.
snmp-server contact	Sets the system server contact string.
snmp-server enable traps	Enables the SE to send SNMP traps.
snmp-server host	Specifies the hosts to receive SNMP traps.
snmp-server location	Sets the SNMP system location string.
snmp-server notify inform	Configures the SNMP notify inform request.
snmp-server user	Defines a user who can access the SNMP engine.
snmp-server view	Defines a SNMPv2 MIB view.

snmp-server host

To specify the recipient of a host SNMP trap operation, use the **snmp-server host** command in Global configuration mode. 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

hostname	Hostname of the SNMP trap host that is sent in the SNMP trap messages from the SE.
ip_address	IP address of the SNMP trap host that is sent in the SNMP trap messages from the SE.
communitystring	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.)
number	Number of retries for the inform request. The range is from 1 to 10.
timeout	(Optional) Sets the timeout for the inform request The default is 15 seconds.
seconds	Timeout value, in seconds. The range is from 1 to 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.

Command 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

timeout *seconds*: 15

Command Modes

Global configuration (config) mode.

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. Informs 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.

Note When entering the **snmp-server host** command, a valid host name must be provided or you receive an error.

If you do not enter an **snmp-server host** command, no notifications are sent. To configure the SE to send SNMP notifications, enter at least one **snmp-server host** command. To enable multiple hosts, 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 is 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 replaces 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 shows how to remove the host 172.16.2.160 from the SNMP trap recipient list:

```
ServiceEngine(config)# no snmp-server host 172.16.2.160
```

Related Commands

Command	Description
show snmp	Displays the SNMP parameters.
snmp-server community	Configures the community access string to permit access to the SNMP.
snmp-server contact	Sets the system server contact string.
snmp-server enable traps	Enables the SE to send SNMP traps.
snmp-server group	Defines a user security model group.
snmp-server location	Sets the SNMP system location string

snmp-server notify inform	Configures the SNMP notify inform request.
snmp-server user	Defines a user who can access the SNMP engine.
snmp-server view	Defines a SNMPv2 MIB view.

snmp-server location

To set the SNMP system location string, use the **snmp-server location** command in Global configuration mode. To remove the location string, use the **no** form of this command.

snmp-server location *line*

no snmp-server location

Syntax Description

line	String that describes the physical location of this node.

Command Defaults

No system location string is set.

Command Modes

Global configuration (config) mode.

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** command.

Examples

The following example shows how to configure a system location string:

```
ServiceEngine(config)# snmp-server location Building 3/Room 214
```

Related Commands

Command	Description
show snmp	Displays the SNMP parameters.
snmp-server community	Configures the community access string to permit access to the SNMP.
snmp-server contact	Sets the system server contact string.
snmp-server enable traps	Enables the SE to send SNMP traps.
snmp-server group	Defines a user security model group.
snmp-server host	Specifies the hosts to receive SNMP traps.
snmp-server notify inform	Configures the SNMP notify inform request.
snmp-server user	Defines a user who can access the SNMP engine.
snmp-server view	Defines a SNMPv2 MIB view.

snmp-server notify inform

To configure the SNMP notify inform request, use the **snmp-server notify inform** command in Global configuration mode. 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.

Command Defaults

If you do not enter the **snmp-server notify inform** command, the default is an SNMP trap request.

Command Modes

Global configuration (config) mode.

Usage Guidelines

The **snmp-server host** command specifies which hosts receive informs. The **snmp-server enable traps** command globally enables the production mechanism for the specified notifications (traps and informs).

For a host to receive an inform, 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 shows how to configure the SNMP notify inform request on the SE:

```
ServiceEngine(config)# snmp-server notify inform
```

Related Commands

Command	Description
show snmp	Displays the SNMP parameters.
snmp-server community	Configures the community access string to permit access to the SNMP.
snmp-server contact	Sets the system server contact string.
snmp-server enable traps	Enables the SE to send SNMP traps.
snmp-server group	Defines a user security model group.
snmp-server host	Specifies the hosts to receive SNMP traps.
snmp-server location	Sets the SNMP system location string.
snmp-server user	Defines a user who can access the SNMP engine.
snmp-server view	Defines a SNMPv2 MIB view.

snmp-server user

To define a user who can access the SNMP server, use the **snmp-server user** command in Global configuration mode. 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** *octet_string* [**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

name	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.
group	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.
password	HMAC MD5 user authentication password.
priv	(Optional) Configures authentication parameters for the packet.
password	HMAC MD5 user private password. You can enter a maximum of 256 characters.
sha	Configures the HMAC Secure Hash Algorithm (SHA) authentication algorithm.
password	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.
octet_string	Globally unique identifier for a remote SNMP entity (for example, the SNMP network management station) for at least one of the SNMP users.

Command Defaults

None

Command Modes

Global configuration (config) mode.

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, define at least one SNMPv3 user account on the SE for the SE to be accessed through SNMP.
- 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.

Tip 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

Command	Description
show snmp	Displays the SNMP parameters.
snmp-server community	Configures the community access string to permit access to the SNMP.
snmp-server contact	Sets the system server contact string.
snmp-server enable traps	Enables the SE to send SNMP traps.
snmp-server group	Defines a user security model group.
snmp-server host	Specifies the hosts to receive SNMP traps.
snmp-server location	Sets the SNMP system location string.
snmp-server notify inform	Configures the SNMP notify inform request.
snmp-server view	Defines a SNMPv2 MIB view.

snmp-server view

To define a SNMP Version 2 (SNMPv2) MIB view, use the **snmp-server view** command in Global configuration mode. To undefine the MIB view, use the **no** form of this command.

snmp-server view *view_name MIB_family* {**excluded** | **included**}

no snmp-server view *view_name MIB_family* {**excluded** | **included**}

Syntax Description

view_name	Name of this family of view subtrees. You can enter a maximum of 64 characters.
MIB_family	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.

Command Defaults

None

Command Modes

Global configuration (config) mode.

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.

Note When configuring an SNMP View with Excluded, the specified MIB that is excluded is not accessible for the community associated with the group that has that view.

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 shows how to create 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

Command	Description
show snmp	Displays the SNMP parameters.
snmp-server community	Configures the community access string to permit access to the SNMP.
snmp-server contact	Sets the system server contact string.
snmp-server enable traps	Enables the SE to send SNMP traps.
snmp-server group	Defines a user security model group.
snmp-server host	Specifies the hosts to receive SNMP traps.
snmp-server location	Sets the SNMP system location string.
snmp-server notify inform	Configures the SNMP notify inform request.
snmp-server user	Defines a user who can access the SNMP engine.

splunk-uf-monitor

To configure Splunk Universal Forwarder monitoring, use the **splunk-uf-monitor** command in Global configuration mode.

On the SE:

splunk-uf-monitor {**enable** | **host** *hostname or ipaddress* [**port** *port number*] | **type** {**all** | **abr-session** | **flash-media-streaming** | **movie-streamer** | **snapshot-counter** | **web-engine** | **wmt**}}

no splunk-uf-monitor {**enable** | **host** *hostname or ipaddress* [**port** *port number*] | **type** {**all** | **abr-session** | **flash-media-streaming** | **movie-streamer** | **snapshot-counter** | **web-engine** | **wmt**}}

On the SR:

splunk-uf-monitor {**enable** | **host** *hostname or ipaddress* [**port** *port number*] | **type {all** | **snapshot-counter** | **service-router}**}

no splunk-uf-monitor {**enable** | **host** *hostname or ipaddress* [**port** *port number*] | **type {all** | **snapshot-counter** | **service-router}**}

Syntax Description

enable	Enables the Splunk Universal Forwarder.
host	Uploads to the host (maximum of three hosts).
hostname or ipaddress	Host name or IP address of the host.
port	Port to use when connected to a host (default is 9998).
port number	Port number of the host.
type	Configures the log type to be monitored.
all	Monitors all log types.
abr-session	Monitors the ABR session log.
flash-media-streaming	Monitors the Flash Media Streaming log.
movie-streamer	Monitors the Movie Streamer log.
snapshot-counter	Monitors the snapshot-count log.
service-router	Monitors the Service Router log.
web-engine	Monitors the Web Engine log.
wmt	Monitors the WMT log.

Command Defaults

Port: 9998

Command Modes

Global configuration (config) mode.

Usage Guidelines

The **splunk-uf-monitor enable** command enables and disables the Splunk Universal Forwarder monitoring on the SE and SR.

The **splunk-uf-monitor host** *hostname or ipaddress* [**port** *port number*] command configures the Splunk Universal Forwarder host IP address and port number, the port number is optional when it's default port number is 9998 on the SE and SR.

The **splunk-uf-monitor type** {**all** | **abr-session** | **flash-media-streaming** | **movie-streamer** | **snapshot-counter** | **web-engine** | **wmt**} command configures the transaction logs to be monitored by Splunk Universal Forwarder on an SE.

The **splunk-uf-monitor type {all | snapshot-counter | service-route}** command configures the transaction logs to be monitored by the Splunk Universal Forwarder on an SR.

Examples

The following example shows how to enable the Splunk Universal Forwarder and configures the forwarder to monitor all transaction log types:

```
ServiceEngine(config)# splunk-uf-monitor enable
ServiceEngine(config)#

ServiceEngine(config)# splunk-uf-monitor type all
ServiceEngine(config)#
```

The following example shows how to configure the Splunk Universal Forwarder host IP address and port number:

```
ServiceEngine(config)# splunk-uf-monitor host X.X.X.X port 9998
ServiceEngine(config)#
```

Related Commands

Command	Description
transaction-logs	Configure and enable transaction logs.

ss

To dump socket statistics, use the **ss** command in EXEC configuration mode.

ss *line*

Syntax Description

line	ss connection information, -h to get help.

Command Defaults

None

Command Modes

EXEC configuration.

Usage Guidelines

The **ss** utility is used to dump socket statistics. It shows information similar to the **netstat** command and displays more TCP information than other tools.

When specifying the options and filters, you can use the short form of the option (a single dash followed by a character) or the long form of the option (two dashes followed by the whole word). To view the list of options and filters, enter **ss -h** (or **ss --help**) and the list of options and filters are displayed along with descriptions.

```
ServiceEngine# ss -h
Usage: ss [OPTIONS]
       ss [OPTIONS] [FILTER]
   -h, --help           this message
   -V, --version        output version information
   -n, --numeric        does not resolve service names
   -r, --resolve       resolve host names
   -a, --all            display all sockets
   -l, --listening      display listening sockets
   -o, --options       show timer information
   -e, --extended      show detailed socket information
   -m, --memory        show socket memory usage
   -p, --processes      show process using socket
   -i, --info           show internal TCP information
   -s, --summary        show socket usage summary

   -4, --ipv4          display only IP version 4 sockets
   -6, --ipv6          display only IP version 6 sockets
   -0, --packet display PACKET sockets
   -t, --tcp            display only TCP sockets
   -u, --udp            display only UDP sockets
   -d, --dccp           display only DCCP sockets
   -w, --raw            display only RAW sockets
   -x, --unix           display only Unix domain sockets
   -7, --filter display when tcp rqueue threshold meet
   -8, --filter display when tcp wqueue threshold meet
   -9, --filter display when tcp retransmit threshold meet
   -W, --filter display only window scale disable
   -B, --background display output in new format
   -L, --no_loop_back   display without loopback interface
   -S, --basic_output  display basic information
   -f, --family=FAMILY display sockets of type FAMILY
```

```
-A, --query=QUERY
    QUERY := {all | inet | tcp | udp | raw | unix | packet | netlink}[,QUERY]

-F, --filter=FILE   read filter information from FILE
    FILTER := [state TCP-STATE] [EXPRESSION]
```

With the **-A** query option, you list the identifiers (all, inet, tcp, udp, and so on) of the socket tables you want displayed, separated by commas.

With the -F filter option, you can filter by TCP state, or using a boolean expression you can filter by IP addresses and ports.

The default output does not resolve host addresses (IP addresses) and does resolve service names (usually stored in local files). To resolve host addresses, use the **-r** option. To suppress resolution of service names, use the **-n** option.

Examples

The following command shows how to display all TCP sockets:

```
ServiceEngine# ss -t -a
```

The following command shows how to display all UDP sockets:

```
ServiceEngine# ss -u -a
```

The following command shows how to display all established SSH connections and display the timer information:

```
ServiceEngine# ss -o state established '( dport = :ssh or sport = :ssh )'
```

The following command shows how to display all established HTTP connections and display the timer information:

```
ServiceEngine# ss -o state established '( dport = :http or sport = :http )'
```

Related Commands

Command	Description
gulp	Captures lossless gigabit packets and writes them to disk.
netmon	Displays the transmit and receive activity on an interface.
netstatr	Displays the rate of change of netstat statistics.
tcpmon	Searches all TCP connections.

sshd

To enable the Secure Shell (SSH) daemon, use the **sshd** command in Global configuration mode. 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 is 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 is terminated by the SE even after successful login if the grace period expires.
seconds	SSH login grace time value, in seconds. The range is from 1 to 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.

Command Defaults

timeout *seconds*: 300

version: Both SSH Version 1 and 2 are enabled.

Command Modes

Global configuration (config) mode.

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** command in Global configuration mode allows you to enable support for either SSH Version 1 or SSH Version 2. When you enable SSH using the **sshd enable** command in Global configuration mode, 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), 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** command output does not display any sshd configuration. If you have disabled the support for one version of SSH, the **show running-config** 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** command in Global configuration mode 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

Command	Description
show ssh	Displays the SSH status and configuration.

streaming-interface

To configure the streaming interface, use the **streaming-interface** command in Global configuration mode. To remove a streaming interface, use the **no** form of this command.

streaming-interface {**GigabitEthernet** *num* | **PortChannel** *num* | **Standby** *num*}

Syntax Description

GigabitEthernet	Selects a Gigabit Ethernet interface as streaming interface.
num	Gigabit Ethernet slot (the range is 1 to 14) and port (the range is 0 to 0).
PortChannel	Selects a port channel interface as streaming interface.
num	Port channel port.
Standby	Selects a standby group as streaming interface.
num	Standby group number.

Defaults

None

Command Modes

Global configuration (config) mode.

Usage Guidelines

When upgrading from a previous software release, the primary interface is converted to a streaming interface by the upgrade process. When configuring new delivery traffic interfaces, either because of a new installation or because of removing existing configuration, use the **streaming-interface** command.

Examples

The following example shows how to configure port channel 1 as the streaming interface:

```
ServiceEngine# streaming-interface portChannel 1

ServiceEngine#
```

sysreport

To save the sysreport to a user-specified file, use the **sysreport** privilege command in EXEC configuration mode.

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 and distribution.
date-range	Specifies the date range of system report.
start_date	Specifies start date of system report following the yyyy/mm/dd format assuming local time zone.
end_date	The end date of system report following the yyyy/mm/dd format assuming local time zone.
filename	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 WMT.

Command Defaults

None

Command Modes

Privilege EXEC configuration mode.

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 {**host** {*hostname* | *ip_address*} [**primary**] | **key** *keyword* | **password ascii** | **retransmit** *retries* | **timeout** *seconds*}

no tacacs {**host** {*hostname* | *ip_address*} [**primary**] | **key** | **password ascii** | **retransmit** | **timeout**}

Syntax Description

host	Sets a server address.
hostname	Hostname of the TACACS+ server.
ip_address	IP address of the TACACS+ server.
primary	(Optional) Sets the server as the primary server.
key	Sets the security word.
keyword	Keyword. An empty string is the default.
password ascii	Specifies ASCII as the TACACS+ password type.
retransmit	Sets the number of times that requests are retransmitted to a server.
retries	Number of retry attempts allowed. The range is from 1 to 3. The default is 2.
timeout	Sets the number of seconds to wait before a request to a server is timed out.
seconds	Timeout, in seconds. The range is from 1 to 20. The default is 5.

Command Defaults

keyword: none (empty string)

timeout *seconds*: 5

retransmit *retries*: 2

password ascii: PAP

Command Modes

Global configuration (config) mode.

Usage Guidelines

Using the **tacacs** command, configure the TACACS+ key, the number of retransmits, the server hostname or IP address, and the timeout.

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
```

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** command in Global configuration 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 sent 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 cleartext 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 shows how to configure the key used in encrypting packets:

```
ServiceEngine(config)# tacacs key human789
```

The following example shows how to configure the host named spearhead as the primary TACACS+ server:

```
ServiceEngine(config)# tacacs host spearhead primary
```

The following example shows how to set the timeout interval for the TACACS+ server:

```
ServiceEngine(config)# tacacs timeout 10
```

The following example shows how to set 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

Command	Description
show authentication	Displays the authentication configuration.
show statistics tacacs	Displays the Service Engine TACACS+ authentication and authorization statistics.
show tacacs	Displays TACACS+ authentication protocol configuration information.

tcpdump

To dump the network traffic, use the **tcpdump** command in EXEC configuration mode.

tcpdump [*LINE*]

Syntax Description

LINE	(Optional) Dump options.

Command Defaults

None

Command Modes

EXEC configuration mode.

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 Technical Support. 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 GigabitEthernet 1/0 and GigabitEthernet 2/0. 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 GigabitEthernet 1/0 -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), 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 GigabitEthernet 1/0, link-type EN10MB (Ethernet), capture size 68 bytes
12:45:43.017677 IP ServiceEngine.cisco.com.ssh > 10.77.140.97.4314: P
3342832089:3342832201(112) ack 1248615673 win 15232
12:45:43.018950 IP 172.19.226.63 > ServiceEngine.cisco.com: icmp 36: 172.19.226.63 udp
port 2048 unreachable
12:45:43.019327 IP ServiceEngine.cisco.com.10015 > dns-sj2.cisco.com.domain:  49828+ [  |
domain ]
12:45:43.021158 IP dns-sj2.cisco.com.domain > ServiceEngine.cisco.com.10015:  49828
NXDomain* [  | domain ]
12:45:43.021942 IP ServiceEngine.cisco.com.10015 > dns-sj2.cisco.com.domain:  49829+ [  |
domain ]
12:45:43.023799 IP dns-sj2.cisco.com.domain > ServiceEngine.cisco.com.10015:  49829
NXDomain* [  | domain ]
12:45:43.024240 IP ServiceEngine.cisco.com.10015 > dns-sj2.cisco.com.domain:  49830+ [  |
domain ]
12:45:43.026164 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 GigabitEthernet 1/0, link-type EN10MB (Ethernet), capture size 68
bytes
216 packets captured
216 packets received by filter
0 packets dropped by kernel
```

tcpmon

To search all TCP connections, use the **tcpmon** command in EXEC configuration mode.

tcpmon *line*

Syntax Description

line	Shows TCP connection information, -h to get help.

Command Defaults

None

Command Modes

EXEC configuration.

Usage Guidelines

The **tcpmon** utility is a script that constantly calls the ss utility at specified intervals. The **tcpmon** utility searches all TCP connections every 30 seconds and displays information about any socket that meets the search criteria. To view the list of options, enter **tcpmon -h**.

```
ServiceEngine# tcpmon -h

Usage: Tcpmon [-N] [-R <Recv-Q-Threshold> | -S <Send-Q-threshold> | -T
<Retransmit-threshold>]
              [<loop-time-in-seconds>] [<iterations>]
       (runs every 30 sec forever by default)
```

Output Example

The following example shows the output for the **tcpmon** utility:

```
State    Recv-Q   Send-Q   Local Address:Port    Peer Address:Port  Rtt/var   Swnd  Retrans
ESTAB      0      257744      10.3.5.2:80         10.3.5.137:32963   530/15    13      0
ESTAB      0      861560      10.3.5.2:80         10.3.5.137:32849   545/24     4      0
ESTAB      0      234576      10.3.5.2:80         10.3.5.122:32979   547/22.2   6      0
ESTAB      0      254848      10.3.5.2:80         10.3.5.103:32909   531/14.8  10      0
ESTAB      0      231680      10.3.5.2:80         10.3.5.135:32925   532/11.5   9      0
ESTAB      0      224440      10.3.5.2:80         10.3.5.133:33057   550/32     7      0
ESTAB      0      267880      10.3.5.2:80         10.3.5.135:32985   530/18.2   7      0
ESTAB      0      291048      10.3.5.2:80         10.3.5.113:32909   539/12.2   6      0
ESTAB      0      249056      10.3.5.2:80         10.3.5.103:32903   520/23.2   8      0
ESTAB      0      218648      10.3.5.2:80         10.3.5.132:33069   522/14.5  16      0
ESTAB      0      702280      10.3.5.2:80         10.3.5.100:32829   539/24.5   5      0
ESTAB      0      412680      10.3.5.2:80         10.3.5.110:32992   546/22.8   7      0
ESTAB      0      254848      10.3.5.2:80         10.3.5.115:33136   552/37.2   5      0
```

Table 0-22 describes the tcpmon output fields.

Table 0-22 tcpmon Output Fields

Field	Description
State	One of the following TCP connection states: ESTAB, SYN-SENT, SYN-RECV, FIN-WAIT-1, FIN-WAIT-2, TIME-WAIT, CLOSE-WAIT, LAST-ACK, LISTEN, and CLOSING.
Recv-Q	Number of bytes in the receiving queue.
Send-Q	Number of bytes in the sending queue.
Local Address: Port	Source address and port.
Peer Address: Port	Destination address and port.
Rtt/var	Average round-trip time (in seconds) and the deviation.
Send	Current sending rate (in Mbps).
Retrans	Number of retransmit timeouts.

Examples

The following command sets the polling cycle to 30 seconds and the receive-queue threshold to 100:

```
ServiceEngine# tcpmon -R 100 30
```

The following command sets the polling cycle to 30 seconds and displays only the sockets with window scaling disabled:

```
ServiceEngine# tcpmon -N 30
```

Related Commands

Command	Description
gulp	Captures lossless gigabit packets and writes them to disk.
netmon	Displays the transmit and receive activity on an interface.
netstatr	Displays the rate of change of netstat statistics.
ss	Dumps socket statistics.

tcp timestamp

To enable and disable the TCP timestamp, use the **tcp timestamp** command in Global configuration mode. To disable the TCP timestamp, use the **no** form of this command.

tcp timestamp

no tcp timestamp

Syntax Description

This command has no arguments or keywords.

Command Defaults

TCP timestamp is enabled by default.

Command Modes

Global configuration (config) mode.

Examples

The following example shows how to disable the TCP timestamp:

```
ServiceEngine# no tcp timestamp
ServiceEngine#
```

telnet

To log in to a network device using the Telnet client, use the **telnet** command in EXEC configuration mode.

telnet {*hostname* | *ip_address*} [*port_num*]

Syntax Description

hostname	Hostname of the network device.
ip_address	IP address of the network device.
port_num	(Optional) Port number. The range is from 1 to 65535. Default port number is 23.

Command Defaults

The default port number is 23.

Command Modes

EXEC configuration mode.

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** command in Global configuration mode. To disable Telnet, use the **no** form of this command.

telnet enable

no telnet enable

Syntax Description

This command has no arguments or keywords.

Command Defaults

Enabled

Command Modes

Global configuration (config) mode.

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

Command	Description
show telnet	Displays the Telnet services configuration.

terminal

To set the number of lines displayed in the console window, or to display the current console **debug** command output, use the **terminal** command in EXEC configuration mode.

terminal {**length** *length* | **monitor** [**disable**]}

Syntax Description

length	Sets the length of the display on the terminal.
length	Length of the display on the terminal (the range is 0 to 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.

Command Defaults

The default length is 24 lines.

Command Modes

EXEC configuration mode.

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 shows how to set the number of lines to display to 20:

```
ServiceEngine# terminal length 20
```

The following example shows how to configure 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** command in EXEC configuration mode.

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.
url	FTP URL to be tested. Use one of the following formats to specify the FTP URL: • ftp://*domainname*/*path* • ftp://*user*:*password*@*domainname*/*path*
use-ftp-proxy	(Optional) Specifies the FTP proxy that is used to test the URL.
proxy_url	FTP proxy URL. Use one of the following formats to specify the proxy URL: • *proxy IP Address*:*proxy Port* • *proxy Username*:*proxy Password*@*proxy IP Address*:*proxy Port*
http	Specifies the HTTP URL to be tested.
url	HTTP URL to be tested. Use one of the following formats to specify the HTTP URL: • http://*domainname*/*path* • http://*user*:*password*@*domainname*/*path*
custom-header	(Optional) Specifies the custom header information to be sent to the server.
header	Custom header information to be sent to the server. Use the format *header*:*line* 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.
proxy_url	HTTP proxy URL. Use one of the following formats to specify the HTTP proxy URL: http://*proxyIp*:*proxyPort* http://*proxyUser*:*proxypasswd*@*proxyIp*:*proxyPort*
head-only	(Optional) Specifies that only the HTTPS header information must be retrieved.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The HTTP CLI client allows you to test connectivity and debug caching issues. The **test-url** command allows you 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://ce1.server.com
--02:27:20-- http://ce1.server.com/
           => `/dev/null'
Len - 22 , Restval - 0 , contlen - 0 , Res - 134728056Resolving ce1.server.com..

done.
Connecting to ce1.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: "1aee29-663-3ea928a8"
 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
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

Command	Description
acquirer (EXEC)	Starts or stops content acquisition on a specified acquirer delivery service.

top

To see a dynamic real-time view of a running CDS, use the **top** command in EXEC configuration mode.

top {*line*}

Syntax Description

line	Specifies top options, enter **-h** to get Help. Press **q** to quit from the output.

Command Defaults

No default behavior values

Command Modes

EXEC configuration mode.

Usage Guidelines

The memory usage reported in the output of the **top** command could fluctuate between 1x to 2x of SR's initial memory usage when the SR configuration changes. This fluctuation is between 'init memory with URT on' and 'init memory with URT off', when changing the URT configuration. Therefore, there is a 1.5GB limit so the SR has enough space to go as high as 3GB memory for TPS.

Considerations:

1. Make sure the SR initial memory usage is less than 1.5GB.
2. The memory usage after a configuration change causes the number reported by the **top** command to be higher, but that is acceptable.
3. If changing the URT, make sure the memory usage URT is turned off at less than 1.5GB; otherwise, there may be a problem.

Examples

The following example shows sample output from the **top** command on an SE:

```
ServiceEngine# top
top - 01:08:45 up 8 days, 23:39, 3 users, load average: 1244.22, 1246.32, 1243.66
Tasks: 1789 total,  4 running, 1785 sleeping,  0 stopped,  0 zombie
Cpu(s): 0.0%us, 13.2%sy, 18.1%ni, 57.8%id, 1.1%wa, 0.7%hi, 9.2%si, 0.0%st
Mem: 32825728k total, 32671416k used,  154312k free,  137164k buffers
Swap:       0k total,        0k used,        0k free, 21289468k cached
```

traceroute

To trace the route to a remote host, use the **traceroute** command in EXEC configuration mode.

On the CDSM and SE:

traceroute {*hostname* | *ip_address*}

On the SR:

traceroute {*hostname* | *ip_address* | **srp** *name*}

Syntax Description

hostname	Name of the remote host.
ip_address	IP address of the remote host.
srp	Specifies Traceroute Service Routing Protocol.
name	Name of the DHT key.

Command Defaults

No default behavior values

Command Modes

EXEC configuration mode.

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  213.088 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 **traceroute** command fails to trace the route to a remote host from the SE:

```
ServiceEngine# traceroute 10.0.0.1
traceroute 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 0-23 describes the fields in the **traceroute** command output.

Table 0-23 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

Command	Description
ping	Sends echo packets for diagnosing basic network connectivity on networks.

traceroute srp

To trace the Service Routing Protocol ring, use the **traceroute srp** command in EXEC configuration mode.

traceroute srp *name*

Syntax Description

name	Name of the DHT key.

Command Defaults

No default behavior values

Command Modes

EXEC configuration mode.

Usage Guidelines

The output from the **traceroute srp** command tells how to reach the owner node of the DHT key by looking up the SRP route table. Along the path each node responds if there is more than one node.

In following example, only the node SN-CDSM responds to the command, and it took 0.373206 ms for it to respond.

Examples

The following example shows how to trace the route to a remote host from the SR:

```
ServiceRouter# traceroute srp
feb5784c704bb8eddba9c2aaa831a2806cb606d2f9205bc1d3edfe770cbaa1dc
1 SN-CDSM:9000, 0.373206 ms
  id=feb5784c704bb8eddba9c2aaa831a2806cb606d2f9205bc1d3edfe770cbaa1dc
```

Related Commands

Command	Description
ping srp	Pings the Service Routing Protocol ring.

traceroute6

To trace the route to a remote IPv6-enabled host, use the **traceroute6** command in EXEC configuration mode.

traceroute6 *ip_address*

Syntax Description

ip_address	Remote IPv6-enabled host or IP address.

Command Defaults

No default behavior values

Command Modes

EXEC configuration mode.

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

Command	Description
ipv6	Specifies the IPv6 address of the default gateway.

transaction-log force

To force the archive or export of the transaction log, use the **transaction-log force** command in EXEC configuration mode.

transaction-log force {**archive** | **export**}

Syntax Description

archive	Forces the archive of the *working.log* file.
export	Forces the archived files to be exported to the server.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The **transaction-log force archive** command causes the transaction log *working.log* 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** command does 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
```

Related Commands

Command	Description
clear	Clears the HTTP object cache, the hardware interface, statistics, archive working transaction logs, and other settings.
show statistics transaction-logs	Displays the SE transaction log export statistics.
show transaction-logging	Displays the transaction log configuration settings and a list of archived transaction log files.
transaction-logs	Configures and enables the transaction logging parameters.

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* | **every-day** {**at** *hour:minute* | **every** *hours*} | **every-hour** {**at** *minute* | **every** *minutes*} | **every-week** [**on** *weekdays* **at** *hour:minute*]} | **max-file-number** *file_number* | **max-file-size** *file_size*} | **ds-snapshot-counter enable** | **enable** | **export** {**compress** | **enable** | **ftp-server** {*hostname* | *serv_ip_addrs*} *login passw directory* | **interval** {*minutes* | **every-day** {**at** *hour:minute* | **every** *hours*} | **every-hour** {**at** *minute* | **every** *minutes*} | **every-week** [**on** *weekdays* **at** *hour:minute*] | **sftp-server** {*hostname* | *serv_ip_addrs*} *login passw directory* | **format** {**apache** | **custom** *string* | **extended-squid**} | **log-windows-domain**}

no transaction-logs {**archive** {**interval** {*seconds* | **every-day** {**at** *hour:minute* | **every** *hours*} | **every-hour** {**at** *minute* | **every** *minutes*} | **every-week** [**on** *weekdays* **at** *hour:minute*]} | **max-file-number** *file_number* | **max-file-size** *file_size*} | **ds-snapshot-counter enable** | **enable** | **export** {**compress** | **enable** | **ftp-server** {*hostname* | *serv_ip_addrs*} *login passw directory* | **interval** {*minutes* | **every-day** {**at** *hour:minute* | **every** *hours*} | **every-hour** {**at** *minute* | **every** *minutes*} | **every-week** [**on** *weekdays* **at** *hour:minute*] | **sftp-server** {*hostname* | *serv_ip_addrs*} *login passw directory* | **format** {**apache** | **custom** *string* | **extended-squid**} | **log-windows-domain**}

Syntax Description

archive	Configures archive parameters.
interval	Determines how frequently the archive file is to be saved.
seconds	Frequency of archiving, in seconds. The range is from120 to 604800.
every-day	Archives using intervals of 1 day or less.
at	Specifies the local time at which to archive each day.
hour:minute	Time of day at which to archive in local time (hh:mm).
every	Specifies the interval in hours. Interval aligns with midnight.
hours	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.
minute	Minute alignment for the hourly archive. The range is from 0 to 59.
every	Specifies the interval in minutes for hourly archive that aligns with the top of the hour.

minutes	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.
weekdays	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.
hour:minute	Time of day at which to archive in local time (hh:mm).
max-file-number	Sets the maximum number of the archived log file.
file_number	Maximum number of the archived log file. The range is from 1 to 10000.
max-file-size	Sets the maximum archive file size.
filesize	Maximum archive file size in kilobytes. The range is from 1000 to 2000000.
ds-snapsot-counter enable	Enables the per delivery service snapshot counter.
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.
hostname	Hostname of the target FTP server.
serv_ip_addrs	IP address of the target FTP server.
login	User login to target FTP server.
passw	User password to target FTP server.
directory	Target directory path for exported files on FTP server.
interval	Determines how frequently the file is to be exported.
minutes	Number of minutes in the interval at which to export a file. The range is from 1 to 10080.
every-day	Specifies the exports using intervals of 1 day or less.
at	Specifies the local time at which to export each day.
hour:minute	Time of day at which to export in local time (hh:mm).
every	Specifies the interval in hours for the daily export.

hours	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.
minute	Minute alignment for the hourly export. The range is from 0 to 59.
every	Specifies the interval in minutes that align with the top of the hour.
minutes	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 of more times a week.
on	(Optional) Specifies the days of the week for the export.
weekdays	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.
hour:minute	Time of day at which to export in the local time (hh:mm).
sftp-server	Sets the SFTP[1] server to receive exported archived files.
hostname	Hostname of the target SFTP server.
serv_ip_addrs	IP address of the target SFTP server.
login	User login to the target SFTP server (less than 40 characters).
passw	User password to the target SFTP server (less than 40 characters).
directory	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 CLF[2].
custom	Configures the HTTP transaction logs output to the custom log format.
string	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.
parameter	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.
hostname	Hostname of the remote syslog server.
ip-address	IP address of the remote syslog server.
port	Configures the port to use when sending transaction log messages to the syslog server.
port-num	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.
rate	Rate (number of messages per second) at which the transaction logger is allowed to send messages to the remote syslog server.

1. SFTP = Secure File Transfer Protocol
2. CLF = common log format

Command 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 (config) mode.

Usage Guidelines

SEs 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 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 because of 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 4-29. The SE default archive interval is once an hour every day.

Note The time stamp in the transaction log filename is in UTC and is irrespective of the time zone configured on the SE. The time stamp in the transaction log filename is the time when the file was created. The logs entries in the transaction logs are in the time zone configured on the SE.

Use the **transaction-logs ds-snapshot-counter enable** command to enable or disable snapshot counter transaction logs. This command is available for both SE and SR. On SE, the snapshot counter transaction log records per delivery service Storage Usage. On the SR, the snapshot counter transaction log records per delivery service Session and Bandwidth Usage.

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 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. The *log format string* is a string that contains the tokens listed in Table 0-24 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 0-24 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 0-24 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 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 (').

Note Each transaction log includes a header line that provides the Cisco Internet Streamer CDS software version and a summary line as the last line in the transaction log, which includes a summary of all the requests that appear in the transaction log.

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 0-24 Custom Format Log Format String Values

Format Token	Value
%a	IP address of the requesting client.
%A	IP address of the SE.
%b	Bytes sent, excluding HTTP headers.
%c	Log Entry Generation Time.
%C	Records AuthLOOKupTime|CALLOOKuptime|CacheRouterTime|OSDownload Time in microseconds.
%D	Time consumed to serve the request in microseconds.
%g	Storage URL when URL Resolve rule action is configured in Service Rule file.
%G	Source URL when URL Resolve rule action is configured in Service Rule file.
%h	Remote host (IP address of the requesting client is logged).
%H	Request protocol.
%I	Bytes received from the client.
%J	Gives the average RTT (Round trip time) for that transaction.
%K	Gives the congestion window flickers for the transaction.

Table 0-24 Custom Format Log Format String Values (continued)

Format Token	Value
%L	Prints the asset size, irrespective of the bytes transferred.
%m	Request method.
%M	MIME type of the requested asset.
%N	The network interface and bytes transferred in that interface.
%O	Bytes sent to client, including the headers.
%p	The client who set up the transport session for the request.
%q	Query string (which is preceded by a question mark (?) if a query string exists; otherwise, it is an empty string).
%r	First line of the request. The space in the first line of the request is replaced with a vertical bar (|) delimiter (for example, Get|/index.html|HTTP/1.1)
%R	Request description (Squid description codes).
%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).
%T	Time consumed to serve the request in seconds (a floating point number with 3 decimal places).
%u	URL path requested, including query strings.
%U	URL path requested, not including query strings.
%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.
%X	Connection status when the response is completed. The %X field has the following possible values: X-Connection aborted before the response completed. + -Connection may be kept alive after the response is sent. - -Connection is closed after the response is sent.
%Z	Print the request received time stamp in milliseconds; otherwise, the request received time stamp is in seconds.
%{Header-Field}i	Any request header. Replace the Header-Field with the actual header field you want to log; for example, %{Cache-Control}i. **Note** All client request headers are only logged on the edge SE.

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* command in Global configuration

mode 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 naming convention:

- Module name
- Host IP address
- Date
- Time
- File generation number

For example, the filename for a Web Engine access log would be the following:

```
we_accesslog_apache_192.0.2.22_20091207_065624_00001
```

where we_accesslog_apache is the module name, 192.0.2.22 is the IP address of the device, 20091207 is the date of the log file (December 7, 2009), and 065624_00001 is the file generation number. The file generation number ranges from 00001 to 99999.

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** command in Global configuration mode allows the administrator to specify when the *working.log* file is archived.
- The **transaction-logs export interval** command in Global configuration mode 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.
- Selection of interval alignment is limited. If an interval is configured for every 4 hours, it aligns with midnight. It cannot align with 12:30 or with 7 a.m.
- 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 is *.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 0-25 describes the name elements.

Table 0-25 Archive Log Name Element Descriptions

Sample of Element	Description
acqdist_	Acquisition and distribution archive log file.
cseaccess	Cisco Streaming Engine archive file.
tftp_server_	TFTP server archive file.
webengine_apache	Web Engine Apache transaction logging format log file.
webengine_clf	Web Engine custom transaction logging format log file.
webengine_extsquid	WebEngine extended-squid transaction logging format log file.
fms_access	Flash Media Streaming transaction log file.
fms_authorization	Flash Media Streaming transaction log for authorization and diagnostic logs.
fms_wsl	Flash Media Streaming transaction log for wholesale licensing.
movie-streamer	Movie Streamer transaction log file.
cache_content	Content Access Layer transaction log file.
authsvr	CDS Authorization Server transaction log 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.
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 0-26 lists the directory names and the corresponding examples of the archive filenames.

Table 0-26 Archive Filename Examples and Directories

Directory	Archive Filename
logs/acqdist	acqdist_10.1.94.4_20050315_001545
logs/cisco-streaming-engine	cseaccess10.1.94.4__050315000.log
logs/tftp_server	tftp_server_10.1.94.4_20050315_001545
logs/webengine_apache	we_accesslog_apache_114.0.92.27_20110322_213143_00001

Table 0-26 Archive Filename Examples and Directories (continued)

Directory	Archive Filename
logs/webengine_clf	we_accesslog_clf_114.0.92.27_20110322_213143_00004
logs/webengine_extsquid	we_accesslog_extsqu_114.0.92.27_20110322_213143_00072
logs/fms_access	fms_access_10.1.94.4_20110323_210446_00001
logs/fms_authorization	fms_auth_10.1.94.4_20110323_210446_00001
logs/fms_wsl	fms_wsl_10.1.94.4_20110323_210446_00001
logs/movie-streamer	movie-streamer_10.1.94.4_20110323_210446_00001
logs/cache_content	cache_content_10.1.94.4_20110323_210446_00001
logs/authsvr	authsvr_10.1.94.4_20110323_210446_00001
logs/export	mms_export_18.0.101.116_20110318_121111_00120
logs/export/extended-wms-41	mms_export_e_wms_41_18.0.101.116_20110318_012847_00001
logs/wms-90	mms_export_wms_90_18.0.101.116_20110318_012847_00001
logs/export/extended-wms-90	mms_export_e_wms_90_18.0.101.116_20110318_012847_00001

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, 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. 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 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 three 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 align with the top of the hour. Every 5 minutes means that archiving occurs 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.

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 before export.

Monitoring HTTP Request Authentication Failures in Real Time

HTTP transaction log messages are sent 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.

Summary Line

The transaction logs include a summary line as the last line in the transaction log, which includes a summary of all the requests that appear in the transaction log.

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

Command	Description
clear	Clears the HTTP object cache, the hardware interface, statistics, archive working transaction logs, and other settings.
show statistics transaction-logs	Displays the SE transaction log export statistics.
show transaction-logging	Displays the transaction log configuration settings and a list of archived transaction log files.
transaction-log force	Forces the archive or export of the transaction log.

type

To display the contents of a file, use the **type** command in EXEC configuration mode.

type *filename*

Syntax Description

filename	Name of file.

Command Defaults

None

Command Modes

EXEC configuration mode.

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 shows how to display 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 - 000000000009ec00 (usable)
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SE-SYS-5-900001: <4> BIOS-e820:
000000000009ec00 - 00000000000a0000 (reserved)
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SE-SYS-5-900001: <4> BIOS-e820:
00000000000e0800 - 0000000000100000 (reserved)
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SE-SYS-5-900001: <4> BIOS-e820:
0000000000100000 - 0000000000f00000 (usable)
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SE-SYS-5-900001: <4> BIOS-e820:
0000000000f00000 - 0000000001000000 (reserved)
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SE-SYS-5-900001: <4> BIOS-e820:
0000000001000000 - 0000000010000000 (usable)
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SE-SYS-5-900001: <4> BIOS-e820:
00000000fff00000 - 0000000100000000 (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

Command	Description
cpfile	Copies a file.
dir	Displays the files in a directory in a long-list format.
lls	Displays a long list of directory names.
ls	Lists the files and subdirectories in a directory.
mkfile	Makes a file (for testing).

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 configuration mode.

type-tail *filename* [*line* | **follow**]

Syntax Description

filename	File to be examined.
line	(Optional) The number of lines from the end of the file to be displayed (the range is 1 to 65535).
follow	(Optional) Displays the end of the file continuously as new lines are added to the file.

Command Defaults

The default is ten lines shown.

Command Modes

EXEC configuration mode.

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 shows how to display 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 shows how to display the last 20 lines of the syslog.text 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.

Command Defaults

None

Command Modes

EXEC configuration mode.

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 2-122 for more information about debug functions.

Valid values for *command* are as follows:

Command	Description	Device Mode
aaa	AAA[1] debug commands.	CDSM
access-lists	Access Control List debug commands.	SE
acquirer	Acquirer debug commands.	SE
all	Disables all debugging.	All
authentication	Authentication debug commands.	All
authsvr	Authserver debug commands.	SE
bandwidth	Bandwidth module debug commands.Bandwidth module debug commands.	SE
buf	Buffer manager debug commands.	All
cache-content	Caching service debug commands.	SE
cache-router	Cache Router debug commands.	SE
cdnfs	Debugs the CDNFS[2].	SE
cli	CLI debug commands.	SE
cms	Debugs the CMS[3].	All
content-mgr	Content Manager debug commands.	SE
dataserver	Dataserver debug commands.	All
dfs	DFS[4] debug commands.	SE
dhcp	DHCP[5] debug commands.	All
distribution	Distribution component debug commands.	SE, SR
emdb	Embedded database debug commands.	All
flash-media-streaming	Flash Media Streaming debug commands.	SE, SR

http	HTTP debug commands.	SR
ip	Internet Protocol debug commands.	SR
isis	IS-IS Routing for IP.	SR
logging	LOG debug commands.	All
malloc	Memory allocation debug commands.	All
movie-streamer	Movie Streamer debug commands.	SE
ntp	NTP[6] debug commands.	All
qos	QOS component debug commands.	SE
rbcp	RBCP[7] debug commands.	SE
rpc	Interbox RPC[8] debug commands.	All
rtsp	RTSP[9]debug commands.	SE
rule	Rules Template debug commands.	SE
service-router	Service Router debug commands.	SE
session-manager	Session Manager Debug Commands.	SE
snmp	SNMP debug commands.	All
srp	Service Routing Protocol.	SR
svc	Service Registration Daemon and Descriptor Interpreter.	SR
standby	Standby debug commands.	SE
stats	Statistics debug commands.	CDSM
translog	Transaction Log debug commands.	SE, SR
uns	Unified naming service command.	SE
web-engine	Web Engine debug commands.	SE
wi	Web Interface debug commands.	SE
wmt	WMT[10] component debug commands.	SE

1. AAA = authentication, authorization, and accounting
2. CDNFS = CDS network file system
3. CMS = centralized management system
4. DFS = distributed filesystem
5. DHCP = Dynamic Host Configuration Protocol
6. NTP = network time protocol
7. RBCP = Router Blade Configuration Protocol
8. RPC = remote procedure call
9. RTSP = real-time streaming protocol
10. WMT = windows media technologies

Related Commands

Command	Description
debug	Configures the debugging options.
show debugging	Displays the state of each debugging option.

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** command in Global configuration mode.

url-signature key-id-owner *num* **key-id-number** *id_num* {**key** *keyword* | **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.
num	Specifies the ID for the owner of this key. The range is from 1 to 32.
key-id-number	Configures the number ID for this key.
id_num	Specifies the ID for the number of this key. The range is from 1 to 16.
key	Configures the encryption key for signing a URL.
keyword	Text of encryption key (maximum of 16 characters, no spaces). **Note** This field accepts only printable ASCII characters (alphabetic, numeric, and others) and does not support a space or the following special characters: pipe (|), question mark (?), double quotes (“), and apostrophe ('). The following special characters are allowed: {}!#$%&()*+,-./;:<=>@\~^[]_.
public-key	Configures the Public Key file location (PEM).
url	The URL from where the Public Key file can be downloaded (maximum of 54 characters).
symmetric-key	(Optional) Configure the Symmetric Key.
word	The Symmetric Key (Must be 16 characters, no spaces).
private-Key	(Optional) Configures the Private Key file location (PEM).
url	The URL from where the Private Key file can be downloaded (maximum of 54 characters).

Command Modes

Global configuration (config) mode.

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 Patern	Description
url-regex	Filters the request based on any regular expression n 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, 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 Patern	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 prepositioned 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 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=deebacde45bf71
6071c8b2fecaa755b9
```

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=8349348
ffac7987d11203122a98e7e64e410fa18
```

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=68b5f5e
d97d1255a0ec42a42a4f779e794df679c
```

Note The URL signature key field accepts only printable ASCII characters (alphabetic, numeric, and others) and does not support a space or the following special characters: pipe (|), question mark (?), double quotes (“), and apostrophe ('). The following special characters are allowed: {}!#$%&()*+,-./;:<=>@\~^[]_

For additional information on URL Sigining, see the 3.2 Configuring URL Signing" section and the "URL Signing and Validation" appendix in the *Cisco Internet Streamer CDS 3.2 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=deebacde45bf71
6071c8b2fecaa755b9
```

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=8349348
ffac7987d11203122a98e7e64e410fa18
```

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=68b5f5e
d97d1255a0ec42a42a4f779e794df679c
```

username

To establish username authentication, use the **username** command in Global configuration mode.

username *name* {**cifs-password** | **samba-password**} {**0** *plain_word* | **1** *lan_crypto nt_crypto* | *clear_text*} | **password** {**0** *plain_word* | **1** *crypto_word* | *clear_text*} [**uid** *u_id*] | **privilege** {**0** | **15**}}

no username *name*

Syntax Description

name	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.
plain_word	Clear-text user password.
1	Specifies a type 1 encrypted password.
lan_crypto	Encrypted password for LAN Manager networks.
nt_crypto	Encrypted password for Windows NT networks.
clear_text	Unencrypted (clear-text) password for Windows NT networks.
password	Sets the user password.
crypto_word	Encrypted user password.
uid	Sets the user ID for a clear-text password or an encrypted password.
u_id	Encrypted password user ID (the range is 2001 to 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.

Command Defaults

The **password** value is set to 0 (cleartext) by default.

Default administrator account:

- **Uid**: 0
- **Username**: admin
- **Password**: default
- **Privilege**: superuser (15)

Command Modes

Global configuration (config) mode.

Usage Guidelines

The **username** command changes the password and privilege level for existing user accounts.

Note The following characters are not permitted in a username or password: ? . / ; [ ] { } “ @ = |.

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            : bhlohlbIwAMOk
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.7P1Ld6
Privilege           : normal user
```

Related Commands

Command	Description
show user	Displays the user identification number and username information for a particular user.
show users	Displays the specified users.

web-engine (EXEC)

To configure the Web Engine, use the **web-engine** command in EXEC configuration mode.

web-engine {**debug-module** {**all** | **ContentStore** | **datasource** | **dataxferengine** | **httpcache** | **httpclient** | **httpsessionmgr** | **none**} | **realtime-monitor** {**start** *dirname* [*interval*] | **stop**} | **transaction-monitor** {**write-to-file** | *filename*} **undebug-module** {**datasource** | **dataxferengine** | **httpcache** | **httpclient** | **httpsessionmgr**}

Syntax Description

debug-module	Debugs the specific Web Engine module.
all	Enables debug for all modules.
ContentStore	CAL Content Store module.
datasource	DataSource Module.
dataxferengine	DataXferEngine module.
httpcache	HTTPCache module.
httpclient	HTTPClient module.
httpsessionmgr	HTTPSessionManager module.
none	Disable debug for all modules.
realtime-monitor	Starts or stops real-time transaction log monitoring. **Note** You must first enable transaction logging to see this command.
start	Starts the Realtime Monitor.
dirname	Directory name of the Realtime Monitor.
interval	(Optional) Interval at which the transaction logs and statistics are monitored.
stop	Stops the Realtime Monitor.
transaction-monitor	Lists the statistics of the current working.log file. **Note** You must first enable transaction logging to see this command.
write-to-file	(Optional) Writes out the statistics to the file.
filename	Name of the statistics file.
undebug-module	Undebugs the specific Web Engine module.
ContentStore	CAL Content Store module.
datasource	DataSource module.
dataxferengine	DataXferEngine module.
httpcache	HTTPCache module.
httpclient	HTTPClient module.
httpsessionmgr	HTTPSessionManager module.

Command Defaults

Realtime Monitor interval: 10 seconds

Command Modes

EXEC configuration mode.

Usage Guidelines

See the "web-engine (Global configuration)" section on page 2-758 for information on configuring caching parameters.

The **web-engine transaction-monitor** command monitors the transaction logs and publishes the statistics and information regarding latency. For this command to work, transaction logs have to be enabled and must be in apache format or extended squid format. There should be at least one transaction every 10 second, and the output of the command can be logged to a file or printed in the console.

The **web-engine realtime-monitor** command monitors the transaction logs and statistics every interval and publishes information about the requests received, such as response codes, cache access status, and memory utilization.

Transaction logs must be enabled to see this command. Enable Transaction logs by entering the **transaction-logs enable** command in Global configuration mode.

The logs are written to /local/local1/<*dirname*>. The logs are consumed by a GUI that displays this information as charts. There should be at least one transaction every interval.

Note If the transaction monitor is only run for a short duration, the script is killed before the block has been filled or flushed to a disk, and the output file is empty.

Examples

The following example shows how to debug CAL-related issues:

```
ServiceEngine# debug web-engine trace
ServiceEngine# web-engine debug-module contentStore
ServiceEngine#
```

The following example shows how to debug the DataSource module:

```
ServiceEngine# web-engine debug-module datasource
ServiceEngine#
```

The following example shows how to debug the DataSource module:

```
ServiceEngine# web-engine undebug-module datasource
ServiceEngine#
```

The following example shows how to display the Web Engine statistics without a file name:

```
ServiceEngine# web-engine transaction-monitor
================================================================================
The statistics will be generated every 10 secs if there are any transactions.
Please press Ctrl-C to stop monitoring the transactions logs
====================  Fri Oct 22 13:58:29 UTC 2010 ==================
HTTP Response Code - Statistics
------------------------------
  200  |  404  |

  414  |   44  |
Cache Access Status - Statistics
--------------------------------
TCP_HIT              ==> 414
TCP_MISS             ==> 44
Average Bitrate      ==> 1022.74899 kbps
Longest Latency      ==> 0.06369 secs[http://www.testing.com/index.html]
================================================================================
```

```
The statistics will be generated every 10 secs if there are any transactions.
Please press Ctrl-C to stop monitoring the transactions logs
====================  Fri Oct 22 13:58:44 UTC 2010 ==================
HTTP Response Code - Statistics
-------------------------------
  200  |  404  |

  606  |   66  |
Cache Access Status - Statistics
-------------------------------
TCP_HIT              ==> 606
TCP_MISS             ==> 66
Average Bitrate      ==> 1720.00367 kbps
Longest Latency      ==> 0.06369 secs[http://www.testing.com/index.html]
```

The following example shows how to display the Web Engine statistics with a file name:

```
ServiceEngine# web-engine transaction-monitor
================================================================================
The statistics will be generated every 10 secs if there are any transactions.
Please press Ctrl-C to stop monitoring the transactions logs
====================  Mon May 09 06:00:32 PDT 2011 ==================
HTTP Response Code - Statistics
-------------------------------
200  |
12  |
Cache Access Status - Statistics
-------------------------------
TCP_HIT              ==> 6
TCP_REFRESH_HIT      ==> 1
TCP_MISS             ==> 5
Average Bitrate      ==> 879.26616 kbps
Longest Latency      ==> 0.00627 secs[http://2.225.3.08/index.html]
================================================================================
The statistics will be generated every 10 secs if there are any transactions.

Please press Ctrl-C to stop monitoring the transactions logs
ServiceEngine#
```

The following example shows how to write transaction-monitor logs to an external file and issue a request that the statistics be redirected to the specified file:

```
ServiceEngine# web-engine transaction-monitor write-to-file sree2.txt
================================================================================
The statistics will be generated every 10 secs if there are any transactions.

Please press Ctrl-C to stop monitoring the transactions logs

The Statistics are written to the file /local1/logs/sree2.txt
ServiceEngine#
```

Related Commands

Command	Description
show statistics web-engine	Displays the Web Engine statistics.
show web-engine	Displays the Web Engine information.
web-engine (Global configuration)	Configures the Web Engine caching parameters.

web-engine (Global configuration)

To configure the Web Engine, use the **web-engine** command in Global Configuration mode. To negate these actions, use the **no** form of this command.

web-engine {**abr-session-log enable** | **cache** {**age-multiplier** {**days** *num* | **hours** *num* | **minutes** *num* | **seconds** *num*} | **feature-cachefill enable** | **max-ttl** {**days** *num* | **hours** *num* | **minutes** *num* | **seconds** *num*} | **min-ttl** *num*} | **http-ingest-logging enable** | **max-concurrent-sessions** *session_num* | **range-cache-fill enable** | **revalidation** {**disable** | **must revalidate**}}

no web-engine {**abr-session-log enable** | **cache** {**age-multiplier** {**days** *num* | **hours** *num* | **minutes** *num* | **seconds** *num*} | **feature-cachefill enable** | **max-ttl** {**days** *num* | **hours** *num* | **minutes** *num* | **seconds** *num*} | **min-ttl** *num*} | **http-ingest-logging enable** | **max-concurrent-sessions** *session_num* | **range-cache-fill enable** | **revalidation** {**disable** | **must revalidate**}}

Syntax Description

abr-session-log	Configures ABR session-based transaction logging.
enable	Enables session-based ABR transaction logging.
cache	Configures the Web Engine caching parameters.
age-multiplier	Expiration time as a percentage of their age.
days	Maximum time to live units, in days.
num	Number of days. The range is form 1 to 1825.
hours	Maximum time to live units, in hours.
num	Number of hours. The range is from 1 to 43800.
minutes	Maximum time to live units, in minutes.
num	Number of minutes. The range is from 1 to 2628000.
seconds	Maximum time to live units, in seconds.
num	Number of seconds. The range is from 1 to 157680000.
max-ttl	Maximum time to live for objects in the cache, in minutes.
min-ttl	Minimum time to live for objects in the cache, in minutes.
feature-cachefill	Configures cachefill features.
enable	Enables the cachefil feature.
http-ingest-logging	Configures http-ingest-logging for each request to Upstream.
enable	Enables http-ingest-logging for each request to Upstream.
max-concurrent-sessions	Configures the maximum concurrent sessions for the Web Engine.
session_num	Maximum number of concurrent sessions for the Web Engine. The range is from 100 to 60000.
range-cache-fill	Configures the cache fill for range (beginning with 0) request, https only.
enable	Enables the cache fill for range request.
revalidation	Enables and disables revalidation requests.
disable	Disables revalidation requests in the Web Engine.
must-revalidate	If **must-revalid**ate is configured, all requests are revalidated by the Web Engine.

Command Defaults

ABR Session Log: disabled
Age Multiplier: 30
min-ttl: 60
max-ttl: 61
Range Cache Fill: disabled
Revalidation: enabled

Command Modes

Global configuration (config) mode.

Usage Guidelines

During cache-miss scenarios, the **web-engine range-cache-fill enable** command enables the Web Engine to cache the full content when a client requests a content range where the first byte of the range is zero (0). The full content is cached and only the requested range is sent to the client.

If the first byte of the range is not zero (0), the content is not cached and the client receives only the requested content range from the content origin server.

If this configuration parameter is not enabled and the range request is specified with the first byte of the range being zero and the last byte not specified, the full content is cached on the SE and served to the client.

The request bundling has the following behavior during an active cache-fill session:

- If a content is not cached, the first client accessing that content goes to the origin server to download the full content. This is the cache-fill period.
- During the cache-fill period,
  - If other clients request the same content in a GET of the full object, those clients do not go to the origin server, but feed off of the cache-fill session.
  - If there are clients requesting the same content in a range-request (a portion of the file), those clients go to the origin server directly to fetch that range.

    For small files, when there is a cache-fill in progress that could satisfy the subsequent request, the clients are served the ongoing cache-fill without initiating a range request to the upstream device.

    For large files, if the ongoing cache-fill has not yet been cached, a new feed is immediately initiated for the request range and for subsequent range requests.
- After the object is fully cached, all future requests (both GET and range request) are served from the local cache.

For request bundling, if the range request portion is already cached, it is served out of the local cache, even if the full file is not finished downloading yet. Only when a portion of the range requested is not yet all on disk does the request follow the CDS hierarchy to locate the cached content, ending at the origin server.

The **no web engine range-cache-fill** command does not alter the behavior of the range request "bytes=0-" which caches full content and also serves full content to the client.

The **show running-config** command and the **show web-engine all** command display the configuration state of this parameter.

For dynamic cached contents, the **revalidation** command triggers only after the cached object is expired by the min/max ttl values. The **must-revalidate** command forces the revalidation of cached objects whether or not the cached object is expired.

Note Configuring Web Engine Service Rules is done though the CDSM, not the CLI.

The **web-engine feature-cachefill** command has just one configurable option, **enable**, which turns it on or off.

When the **web-engine abr-session-log enable** command is executed, the Web Engine uses Per Session ABR transaction logs. When it is disabled, the Web Engine uses Per Transaction ABR logs. If ABR session framework is not enabled, the Web Engine uses normal HTTP transaction logs disregarding this configuration. This command is disabled by default.

Web Engine Rule Action Order

The order in which the rule actions are executed for the Web Engine is as follows:

1. redirect (before cache lookup)
2. block or allow

Note The allow and block actions 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.

3. rewrite (before cache lookup)
4. use-icap-service
5. generate-url-signature
6. validate-url-signature
7. refresh (after cache lookup, in the case of cache hit)
8. no-cache

Ingest Transaction Logs

The **web-engine http-ingest-logging enable** command enables Web Engine ingest transaction logs that are used to log details of every upstream request sent by the Web Engine to the upstream SEs and origin servers. Ingest transaction logs only stores request details of cache-miss content and cache-hit content with a revalidation request; details of prefetched content are not stored in the ingest transaction logs.

The Web Engine ingest transaction logs are located in the /local/local1/logs/webengine_ingestlog_clf directory.

The ingest log file format is as follows:

Time URL FailOverSvrList ServerIP BytesRead BytesToRead AssetSize %DownloadComplete DownloadTime(Seconds) ReadCallBack Status-Returned MIME-Type Revalidation-Request CDSDomain ConnectionInfo(LocalPort|ConnectTime|Retry|ReUse) IngestStatus

The following are several ingest log file examples:

```
[26/Aug/2011:04:12:56.429-0700] http://3.1.7.30/error-b404-1170329 3.1.7.35/3.1.7.30/
3.1.7.35 0 0 0 0 6 0 504 - No spirent.spcdn.com 38694|Fri_Aug_26_04:12:56_2011|0|1
READ_TIMEOUT_HEADER

[26/Aug/2011:04:12:55.056-0700] http://3.1.7.30/error-b404-1187409 3.1.7.35/3.1.7.30/
3.1.7.35 0 0 0 0 3 1 500 - No spirent.spcdn.com 38194|Fri_Aug_26_04:12:55_2011|0|1
NO_NEED_TO_GET_BODY
```

```
[30/Aug/2011:05:19:02.700-0700] http://os.cdn.we.com/we/test.html 3.1.7.35/7.25.0.20/
3.1.7.35 18028071 18028071 18028071 100 3 1670 200 text/html;charset=UTF-8 No
youtube.cdn.we.com 21449|Tue_Aug_30_05:19:02_2011|0|1 SUCCESS_FINISH

[04/Aug/2011:22:24:11.810-0700] http://7.25.0.20/we/index1.html 7.25.0.20/ 7.25.0.20 0 0 0
0 2 0 504 - Yes[If_None_Match:"5a585a1-19-7a6c8580"] - 20345|Thu_Aug__4_22:24:11_2011|1|1
CONNECT_CB_SOCK_ERR
```

Table 4-27 describes the fields for the ingest transaction log.

Table 4-27 Ingest Transaction Log Fields

Field	Description
Time	Time the request was sent by the Web Engine to the upstream SE or origin server.
URL	Requested URL, including the query string, sent by the Web Engine.
FailOverSvrList	Hierarchical route look-up information to the upstream SE or origin server. When a cache route look-up is performed for the request, the list of upstream SEs and origin server contacted to fetch the content is included in the log entry.
ServerIP	IP address of the SE or origin server from which the content is downloaded. This is obtained from the FailOverSvrList.
BytesRead	Number of bytes downloaded from the upstream SE or origin server.
BytesToRead	Total number of bytes to be downloaded from the upstream SE or origin server.
AssetSize	Size of the asset (in bytes) requested.
%DownloadComplete	Percentage of asset that has been downloaded to the requesting SE.
DownloadTime (Seconds)	Time to download the incoming stream (in seconds granularity).
ReadCallBack	Number of read call back received to read the response body.
Status-Returned	HTTP status code returned from the upstream SE or origin server.
MIME-Type	MIME type.
Revalidation-Request	Either “Yes” if the request is a revalidation request for a cache hit, or “No” if the request is a cache-miss. If “Yes,” the Header-Name:HeaderValue follows. The “If-None-Match” or “If-Not-Modified” headers and their values are included in the log entry.
CDSDomain	This internal header is added by web-engine when reaching out to another streamer in the CDN hierarchy. This header value represents the request domain of the end client request.
ConnectionInfo	
LocalPort	Local port used by the streamer to talk to upstream.
ConnectTime	Time at which the connection was established.
Retry	Number of retries on the connection.

Table 4-27 Ingest Transaction Log Fields (continued)

Field	Description
Reuse	Number of times the same connection was reused.
IngestStatus	Status of the Ingest. The possible values for this field are: CONNECT_TIMEOUT, CONNECT_CB_SOCK_ERR, CONNECT_SOCK_ERR, CONNECT_TO_SELF, WRITE_READY_TIMEOUT, WRITE_SOCK_ER R_HWEADER, READ_TIMEOUT_HEADER, READ_TIMEOUT_BODY, READ_RCVD_ON_WRITE, READ_SOCK_ERR_HEADER, READ_SOCK_ERR_BODY, HEADER_INVALID_CONT_LEN, HEADER_PARSE_EXCEPTION, HEADER_PARSE_ERR, NO_NEED_TO_GET_BODY, NO_MORE_DATA_TO_READ, HEAD_RESPONSE, SUCCESS_FINISH, INVALID_STATE

Examples

The following example shows how to configure caching parameters:

```
ServiceEngine(config)# web-engine cache min-ttl 20
ServiceEngine(config)#

ServiceEngine(config)# web-engine cache max-ttl minutes 50
ServiceEngine(config)#
```

The following example shows how to enable http ingest logging for each request to Upstream:

```
ServiceEngine(config)# web-engine http-ingest-logging enable
ServiceEngine(config)#
```

The following example shows how to enable cache fill (of full content) on range requests when the first byte is 0(zero):

```
ServiceEngine(config)# web-engine range-cache-fill enable
ServiceEngine(config)#
```

So the following GET request caches full content (file_cache.html) and serves only 100 bytes (0-99) to the client:

```
GET http://171.79.89.10/file_cache.html HTTP/1.1
Host:171.79.89.10
Range:bytes=0-99
```

But the following GET request does *not* cache the content (here file_no_cache.html) and serves 100 bytes (10-109) to client:

```
GET http://171.79.89.10/file_no_cache.html HTTP/1.1
Host:171.79.89.10
Range:bytes=10-109
```

The following example shows how to disable the cache fill option on range request:

```
ServiceEngine(config)# no web-engine range-cache-fill enable
ServiceEngine(config)#
```

This GET request does not cache the contents and serves only requested bytes to client(s).

The following example shows how to disable revalidation on the Web Engine:

```
ServiceEngine(config)# web-engine revalidation disable
```

The following example shows how to enable ABR per Session logging:

```
ServiceEngine(config)# transaction-logs enable
ServiceEngine(config)# web-engine abr-session-log enable
```

Or

```
ServiceEngine(config)# transaction-logs enable
ServiceEngine(config)# web-engine abr-session-log enable exclusive
```

Related Commands

Command	Description
show statistics web-engine	Displays the Web Engine statistics.
show web-engine	Displays the Web Engine information.
web-engine (EXEC)	Configures the Web Engine module.

whoami

To display the username of the current user, use the **whoami** command in EXEC configuration mode.

whoami

Syntax Description

This command has no arguments or keywords.

Command Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Use this command to display the username of the current user.

Examples

The following example shows how to display the username of the user who has logged in to the SE:

```
ServiceEngine# whoami
admin
```

Related Commands

Command	Description
pwd	Displays the present working directory.

wmt

To configure WMT, use the **wmt** command in Global configuration mode. To negate these actions, use the **no** form of this command.

wmt {**accelerate** {**proxy-cache** | **vod**} **enable** | **advanced** {**client** {**maximum-packet-size** *number* | **idle-timeout**} | **server** {**log-forwarding** | **inactivity-timeout**} **enable**}| **cache** {**age-multiplier** *num* | **enable** | **max-obj-size** *size* | **max-ttl** {**days** *num* | **hours** *num* | **minutes** *num* | **seconds** *num*} | **min-ttl** *num* | **reval-each-request**} | **disallowed-client-protocols** {**http** [**rtspt** | **rtspu**] | **rtspt** [**http** | **rtspu**] | **rtspu** [**http** | **rtspt**]} | **enable** | **fast-cache** {**enable** | **max-delivery-rate** *num*} | **fast-start** {**enable** | **max-bandwidth** *num*} | **http allow extension** *file_extensions* | **max-concurrent-sessions** *num* | **proxy outgoing** {**http host** *hostname port_num* | **rtsp**} | **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** *num* | **enable** | **max-obj-size** *size* | **max-ttl** {**days** *num* | **hours** *num* | **minutes** *num* | **seconds** *num*} | **min-ttl** *num* | **reval-each-request**} | **disallowed-client-protocols** {**http** [**rtspt** | **rtspu**] | **rtspt** [**http** | **rtspu**] | **rtspu** [**http** | **rtspt**]} | **enable** | **fast-cache** {**enable** | **max-delivery-rate** *num*} | **fast-start** {**enable** | **max-bandwidth** *num*} | **http allow extension** *file_extensions* | **max-concurrent-sessions** *num* | **proxy outgoing** {**http host** *hostname port_num* | **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.
num	Maximum packet size of WMT stream in bytes. The range is from 512 to 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.
num	Timeout value, in seconds. The range is from 30 to 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.
number	Server data channel inactivity timeout. The range is from 60 to 65535.
bandwidth	Configures WMT bandwidth.

incoming	Specifies WMT incoming bandwidth configurations.
bypass-list	Specifies the hostname or IP address of the host for bypassing bandwidth limits.
name	Specifies the hostname or IP address of the host.
cache	Configures the WMT cache.
age-multiplier	Specifies the WMT caching heuristic modifiers.
number	Expiration time as a percentage of their age. The range is from 0 to 100.
enable	Enables the WMT media cache.
max-obj-size	Sets the maximum size of the object to be cached.
size	Object size in megabytes. The range is from 1 to 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.
num	Maximum time to live. The range is from 1 to 1825.
hours	Specifies the maximum time to live units, in hours.
num	Maximum time to live. The range is from 1 to 43800.
minutes	Specifies the maximum time to live units, in minutes.
num	Maximum time to live. The range is from 1 to 2628000.
seconds	Specifies the maximum time to live units, in seconds.
num	Maximum time to live. The range is from 1 to157680000.
min-ttl	Specifies the minimum time to live for objects in the cache.
num	Minimum time to live. The range is from 0 to 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.
num	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. The range is from 1 to 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.
num	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.
file_extensions	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.
num	Limit for incoming unicast requests; this limit is subject to physical resources on the platform. The range is from 1 to 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.
hostname	Hostname of an outgoing proxy.
ip_address	IP address of an outgoing proxy.
port	Port number of an outgoing proxy. The range is from 1 to 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.

Command Defaults

wmt: enabled

advanced client maximum-packet-size: 1500

advanced client idle-timeout: 60

advanced server log-forwarding: enabled

wmt cache max-ttl days: 1

wmt cache max-ttl hours: 72

wmt cache max-ttl minutes: 4320

wmt cache max-ttl seconds: 259200

wmt cache min-ttl: 60

wmt fast-cache: enabled

wmt fast-start: enabled

max-object-size: 1

wmt http allow extension *file_extensions*: asf, none, nsc, wma, wmv

Command Modes

Global configuration (config) mode.

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 see an error message and the services fail to install. Use the **show clock** command to display the system clock. To set the system clock, use the **clock set** 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 because of 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** command in Global configuration mode to limit the amount of bandwidth that Fast Start can use to stream content to each media player.

Adding or Removing WMT HTT- 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* command in Global configuration mode 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 several 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

For Multicast to SE and Multicast to client options, 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, 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 because of 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 XML. See Table 4-28.

Table 4-28 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** command in Global configuration mode. 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** command in Global configuration mode) but the extended WMT logging feature is disabled, the username field in the WMT transaction log is 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:

- File named /local1/logs/export/working.log
- 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 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** command in Global configuration mode. To re-enable this feature, enter the **wmt advanced server log-forwarding enable** command in Global configuration mode.

Examples

The following example shows how to display 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%
                    NTLM:          0                0.00%
                  Digest:          0                0.00%
                   Basic:          0                0.00%
```

The following example shows how to display 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-BCF5EEEDE3FF }  10.1.0.3055 en-US - - wmplayer.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 4-29 describes the fields shown in this example.

Table 4-29 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-startime	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).

Table 4-29 wmt multicast logging Field Descriptions (continued)

Field	Description
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.
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-send) 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 re-sent using UDP.
c-buffercount	Number of times that the client buffered while playing the stream.

Table 4-29 wmt multicast logging Field Descriptions (continued)

Field	Description
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.
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: [cPacketsRendered / (cPacketsRendered + 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** 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 shows how to set 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 shows how to enable the logging of usernames to the WMT transaction log:

```
ServiceEngine# wmt extended transaction-log enable
```

Related Commands

Command	Description
clear wmt	Clears the WMT streams.
show running-config	Displays the current operating configuration.
show statistics wmt	Displays the WMT statistics.
show tech-support	Displays the system information for Cisco technical support.
show wmt	Displays WMT bandwidth and proxy mode configuration.

write

To save startup configurations, use the **write** command in EXEC configuration mode.

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.

Command Defaults

The configuration is written to NVRAM by default.

Command Modes

EXEC configuration mode.

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.

Execute the **write memory** command 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 are 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

Command	Description
copy	Copies the configuration or image files to and from the CD-ROM, flash memory, disk, or remote hosts.
show running-config	Displays the current operating configuration.

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
AS	Autonomous System
AUP	acceptable use policy
BA	Behavior Aggregate
BGP	Border Gateway Protocol
BIOS	basic input/output system
CAL	Content Abstraction Layer
CAR	Committed Access Rate
CD	Carrier Detect
CDE	Content Delivery Engine
CDNFS	CDS network file system; also prepositioned file system
CDS	Content Delivery System
CDSM	Content Delivery System Manager
CIFS	Common Internet File System
CLF	Common Log format
CLI	command-line interface
CLNS	Connectionless Network Service
CMS	Centralized Management System
CoS	class of service
CSNP	Complete Sequence Number PDU
CSS	Content Services Switch

Table A-1 List of Acronyms (continued)

Acronym	Expansion
CTE	chunked transfer encoding
DC	domain controller
DHCP	Dynamic Host Configuration Protocol
DHT	distributed hash table
DNS	Domain Name System
DSCP	differentiated services code point
DSL	Digital Subscriber Line
ECN	Explicit Congestion Notification
EBGP	External Border Gateway Protocol
EIM	employee Internet management
ESIS	End System to Intermediate System
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
IIPC	Inter-process procedure
IPV6	Internet Protocol Version 6
IIS	Internet Information Services or Internet Information Server (Microsoft)
IMS	if-modified-since
IS-IS	Intermediate System-to-Intermediate System
ISO-IGRP	Intermediate System-to-Intermediate System Interior Gateway Routing Protocol
LDAP	Lightweight Directory Access Protocol
LCM	local/central management
LRU	least-recently-used

Table A-1 List of Acronyms (continued)

Acronym	Expansion
LSA	Link-state advertisement
LSDB	Link-state packet database
LSP	Link-state packet
MAC	Media Access Control
MIB	Management Information Base
MOTD	message-of-the-day
MPLS	Multiprotocol Label Switching
MSFC	Multilayer Switch Feature Card
MTU	maximum transmission unit
NACK	negative acknowledgement
NAS	network attached storage; network access server
NAT	Network Address Translation
NET	Network Entity Title
NFS	Network File System
NIC	Network Information Center
NNTP	Network News Transport Protocol
NSAP	network service access point
NSSA	not-so-stubby-area
NTP	Network Time Protocol
NTSC	National Television Systems Committee
NVRAM	nonvolatile random-access memory
OSPF	Open Shortest Path First
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

Table A-1 List of Acronyms (continued)

Acronym	Expansion
RBCP	Router Blade Configuration Protocol
RCP	Remote Copy Program
RIB	Routing Information Base
RPC	remote procedure call
RRM	Received Routing Message
RSA	Rivest, Shamir, Adelman
RSPF	OSPF reverse shortest path first
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)
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SPE	Synchronous Payload Envelope
SPF	Shortest Path First
SR	Service Router
SRAM	static random-access memory
SRHP	service routing host packet
SRM	Send Routing Message
SRP	Service Routing Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
SSN	Send Sequence Number
swfs	software file system
sysfs	system file system

Table A-1 List of Acronyms (continued)

Acronym	Expansion
syslog	system logging
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
TTL	Time-to-Live
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/London	0
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

Table B-1 List of Standard Time Zones and Offsets from UTC (continued)

Time Zone	Offset from UTC
Europe/Samara	+4
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

Table B-1 List of Standard Time Zones and Offsets from UTC (continued)

Time Zone	Offset from UTC
Libya	+2
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/Fakaofo	–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

Table B-1 List of Standard Time Zones and Offsets from UTC (continued)

Time Zone	Offset from UTC
Pacific/Saipan	+10
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

Table B-1 List of Standard Time Zones and Offsets from UTC (continued)

Time Zone	Offset from UTC
CST6CDT	–6
EST	–5
HST	–10
MST7MDT	+7
Navajo	–7
PST8PDT	–8
W-SU	+3
WET	0
Zulu	0
UTC	0
Universal	0
EST5EDT	–5

INDEX

Symbols

! (exclamation point) 4-722, 4-732

- (hyphen) 2-185, 4-732, 4-776

... (ellipsis) 4-732

.bin files
  installing 2-186

.nsc file 4-661

.pax files
  installing 2-186

/ (slash) 2-63

? (question mark) 2-184

A

aaa 2-23
  configuration, displaying 3-340

aaa accounting
  statistics for 4-613

access lists
  configuration, displaying 3-343
  configuring 2-27
  enabling 2-27
  group names 2-28
  interfaces and applications
    applying to 2-201
    status 3-418
  statistics
    clearing 2-92
    displaying 3-557

accounting, authentication, authorization
  statistics
    displaying 3-556

ACLs
  See IP ACLs

ACPI
  models supporting 4-668

acquirer
  delivery service information and content acquisition progress, displaying 3-344
  delivery service statistics, displaying 3-558
  proxy authentication 2-33
  starting and stopping acquisition on a specific delivery service 2-30

acquisition and distribution
  starting and stopping 2-35

action rule
  configuring 3-312

addmission control
  statistics
    displaying 3-561

address translation tables 3-349

administrative login authentication and authorization
  RADIUS
    enabling and disabling 3-291
  TACACS+
    enabling and disabling 4-700

administrative privileges
  users, clearing 2-98

alarm information
  for all alarms 3-346
  for critical alarms 3-347
  for major alarms 3-347
  for minor alarms 3-347

alarms
  displaying status and history 3-346

alarm traps

configuring 4-678
generating 4-678
Apache CLF transaction log format 4-732
applications
applying access lists to 2-201
archive log file
compressing 4-737
marking beginning and end 4-732
maximum size 4-732
naming convention 4-735
ARP table, displaying 3-349
authentication
access lists, enabling 2-27
configuration, displaying 3-350
outgoing proxy 2-33
proxy server 2-33
statistics, clearing 2-92
users
creating 4-752
authorization server
configuring 2-42
enabling 2-42
statistics, displaying 3-563

B

bandwidth
displaying 3-352
interface, configuring 2-47
multicast 3-249
network resources 2-44
setting for streaming media 2-44
bandwidth configuration
incoming and outgoing 2-45
banners
configuration of 2-49
displaying 3-354
enabling 2-50
types of
EXEC 2-50
login 2-50
motd 2-50
basic configuration settings
setting up 3-339
BGP (Border Gateway Protocol)
community string, displaying 3-423
configuration mode 1-4
debug information, displaying 2-133
memory, displaying 3-426
neighbor information, displaying 3-427
neighbors, configuring 3-259
next-hop information, displaying 3-429
routing process, configuring 3-301
routing table
content, displaying 3-420, 3-422
IPv4 unicast routes, displaying 3-425
summary 3-430
bit rate
displaying 3-355
movie-streamer and WMT, configuring 2-52
blink 2-55
bootstrap node
configuring IP address 2-56

C

cache
content 2-58
information, displaying 3-356, 3-358
caching
HTTP
objects 2-71
matching against parameters for requests 3-312
caching services
setting up 3-339
calendar
setting 2-100
capability

configuring 2-62
Cap-X profile ID
information, displaying 3-359
CAR
IP precedence
ToS 2-196
carousels
fixed 3-249
CDN file system
See cdnfs
cdnfs
information, displaying 3-361
managing 2-65
statistics, displaying 3-567
CDN Selector
enabling 2-64
information, displaying 3-360
CDS
content, displaying 3-368
content-mgr, displaying 3-371
installing 2-186
Centralized Management System
See CMS
CISCO-ENTITY-ASSET-MIB
configuring 2-41
Cisco script
executing 3-321
Cisco Streaming Engine server
live streaming with 3-307
Cisco Technical Assistance Center (TAC) 4-643
classification
IP precedence
ToS field 2-196
clock
clearing and setting 2-100
daylight saving and local time, setting 2-102
displaying standard timezones 3-363
Service Engine, synchronizing 3-270
software time and date, setting 3-272
system clock settings, displaying 3-363
UTC current time of day, setting 2-103
UTC offset, setting 2-103
CMS
database, configuring 2-106
enabling 2-109
maintenance routines, scheduling 2-109
process information, displaying 3-366
cold restart 3-295
command-line processing 1-1
command modes
EXEC 1-3
global configuration 1-3
interface configuration 1-4
command syntax 1-5
configuration mode
IS-IS 1-4
configuration modes
BGP 1-4
extended ACL 2-202
ICAP service 1-4
OSPF 1-4
SRP 1-4
standard ACL 2-202
configuring 2-117
alarm traps 4-678
disk space allocation 2-151
Connectionless Network Service (CLNS)
NET, configuring 3-262
packet routing 3-471
console
setting length of display 4-714
content acquisition
database cleanup 2-35
starting and stopping 2-35
Content Delivery System Manager
configuring IP address 2-68
primary role 2-105
SSL 2-106

standby role 2-68
content distribution
statistics, display 4-571
content manager 2-116
statistics, displaying 3-569
content origin 2-117
showing 3-374
copying
configuration data 2-118
files 2-120, 2-121
image data 2-118
crossdomain support 3-328
custom transaction log format 4-732
log format string values 4-733

D

database cleanup
content acquisition and distribution 2-35
date and time
setting 3-272
daylight saving time
setting 2-102
debug
disabling 4-746
information, displaying 3-376
software functions 2-122
debug cdnfs command 2-132
default gateway
defining 2-192
IPv6 address, configuring 2-213
removing 2-192
default status
restoring 3-297
deleting
directories 2-145, 3-300
directory trees 2-145
files 2-144
delivery service distribution
information, displaying 3-387
device mode
and linked CLI commands 1-1
configuring 2-146
displaying 3-380
devices
shutting down 4-668
DHT
clearing counters 2-93
deleting route 2-90
differentiated service model
classification 2-196
directories
changing 2-63
creating 3-242
deleting 2-145, 3-300
files, viewing 2-148, 3-230
Direct Server Return (DSR)
enabling a VIP 2-149
information, displaying 3-382
disk drives
error handling thresholds
description of 2-158
specifying 2-158
disks
configuring 2-151
space allocation 2-151
details, viewing 3-383
partitions, removing 3-297
space allocation 2-151
disk space allocated to system use 2-152
distribution
delivery service, displaying 3-387
refresh content 2-160
statistics
displaying 3-387
DNS lookup 2-164
domain ID
SRP, setting 2-165

domain name
resolving to IP address 2-164
dumping network traffic 4-704
DWRED
IP precedence
ToS 2-196

E

echo packets
sending 3-273
ellipsis (...) 4-732
embedded database parameters
configuring 2-105
enabling 2-227
accounting, authentication, authorization 2-23
RADIUS authentication and authorization 3-292
rules processing 3-310
TACACS+ authentication and authorization 4-700
exclamation point (!) 4-722, 4-732
EXEC command mode
described 1-3
returning to 2-170
exiting
from configuration modes 2-170
from privileged EXEC mode 2-150
exporting transaction logs
forced 4-725
to FTP server 4-737
to SFTP server 4-737
extended access lists 2-202
extended IP ACLs
configuration examples 2-208
configuring 2-203
ICMP message types 2-206
supported keywords 2-205
TCP keywords 2-205
Extended Squid transaction log format 4-732
external FTP server
exporting transaction logs to 4-737
permanent error from 4-738

F

Fast Cache
enabling 4-768
Fast Start
enabling 4-768
file
copying 2-121
creating 3-243, 4-725
deleting 2-144
displaying name 3-230, 4-741
management 2-63
renaming 3-296
fixed carousel 3-249
Flash Media Streaming, see FMS
flash memory
configuring upon reload 3-295
data, removing 3-297
version and usage, displaying 3-399
FMS
configuring 2-176
enabling 2-176
information, displaying 3-401
statistics, displaying 4-574
force reset of disk information 2-116
FTP
access lists 2-203
caching configuration, displaying 3-403
FTP over HTTP
Rules Template 3-313
FTP servers
exporting transaction logs to 4-737

G

geo location server 2-180
Gigabit Ethernet
  configuring 2-187
  negating interface configuration command 3-269
global configuration command mode
  enable password 2-167
  entering 2-112
  exiting 2-168
  negating command 3-267
  setting 2-112, 2-113
global configuration mode
  description 1-3
GMT
  changing local time in content to 2-30
  UTC and 2-103
Greenwich Mean Time
  See GMT
group names
  access lists 2-28
gulp 2-181

H

hardware interface
  displaying information 3-411
  shutting down 4-667
hardware status, displaying 3-404
help system 1-6, 2-184
history
  statistics, clearing 2-93
hostname
  of Service Engine 2-185
  resolving to IP address 2-164
hosts
  name servers and IP addresses, displaying 3-410
HTTP
  object cache
    clearing 2-71
  proxy
    support for root Service Engine 2-33
  status codes 4-732
  transaction logging 4-731
  users, managing 4-753
HTTPS
  Rules Template with 3-313
hyphen (-) 2-185, 4-732

I

ICAP service configuration mode 1-4
ICMP
  access lists 2-203
  keywords for message type and code 2-206
  statistics
    clearing 2-93
    displaying 4-583
image data
  copying 2-118
initial network device settings
  changing 2-192
installing system image 2-186
intelligent carousel 3-249
interface
  bandwidth 2-47
  configuring 2-187
  displaying hardware status 3-411
  standby 3-552
interface configuration command mode 1-4
interface IP
  configuring 2-198
Internet socket connection statistics
  displaying 4-598
inventory information
  displaying 3-416
IP ACLs
  activating on an interface 2-208

clearing IP ACL counter 2-75, 2-77
creating and modifying 2-201
description of 2-204
extended configuration mode
accessing 2-203
extended IP ACLs 2-205
standard configuration mode
accessing 2-202
standard IP ACLs 2-205
typical uses of 2-204
IP address
Content Delivery System Manager, configuring 2-68
starting autodiscovery utility 2-193
statistics, clearing 2-93
IP default domain name
defining 2-192
removing 2-192
IP default gateway
defining 2-192
removing 2-192
IP interface
information, displaying 3-431
IP precedence
edge function 2-196
ToS field
classification 2-196
IP route table, displaying 3-464
IP statistics, display 4-589
IS-IS (Intermediate System-to-Intermediate System)
adjacencies, displaying 3-469
adjacency levels, configuring 2-217
clearing counters 2-93
CLNS destinations, displaying 3-471
displaying debug information 2-141
hostname table, displaying 3-476
interface, specifying 2-212
interface information, displaying 3-477
link-state database, displaying 3-472
memory, displaying 3-484
neighbor status syslog 3-234
process, displaying 3-485
routing, enabling 3-302
RRM, displaying 3-486
RSPF route, displaying 3-480, 3-482
SPF information, displaying 3-487
SRM information, displaying 3-489
SSN information, displaying 3-490
statistics, displaying 4-593

K

kernel debugger 2-222
key chain
creating 2-225
displaying 3-491
key id 2-223
key string 2-224
keystroke combinations, CLI 1-2

L

Last-Modified-Time 2-30
launching
Setup utility 3-339
Link Aggregation Control Protocol (lacp) 2-227
link-state advertisement (LSA)
displaying OSPF information 3-435
request list, displaying 3-447
retransmission list, displaying 3-448
link-state packet (LSP)
MTU, configuring 3-241
lists
directory names 3-230
file 3-240
live events
about 3-503
configuration requirements 3-504

live streaming
with Cisco Streaming Engine 3-307
live stream interruptions 3-504
load balancing
for port channel 3-276
local time, changing to GMT 2-30
log file
number of lines to view 4-743
log files
exporting 4-735
restarting the export of 4-739
logging
configuring 3-235
file rotation of logs 3-237
RealProxy errors 3-238
WMT multicast 4-765
logging in
to Service Engine
using SSH 4-696
using Telnet 4-713

M

mapping syslog priority levels to RealProxy error codes 3-238
maximum concurrent jobs for multicast, setting 3-251
maximum transmission unit (MTU)
interface 3-248
LSP 3-241
MIB view
defining 4-690
minimum bandwidth for multicast, setting 3-251
modes
command
EXEC 1-3
global configuration 1-3
interface configuration 1-4
configuration
BGP 1-4
extended ACL 1-4
HTTP server 1-4
ICAP service 1-4
IS-IS (Intermediate System-to-Intermediate System) 1-4
OSPF 1-4
SRP 1-4
standard ACL 1-4
Movie Streamer
bit rate, setting 2-52
configuration, displaying 3-496
configuring 3-245
enabling 3-245
statistics, displaying 4-595
multicast 3-252
configuring client options 3-249
disabling backup senders 2-110
logging
WMT 4-770, 4-773
overview 4-769
priority 3-249
WMT, logging 4-770
multicast carousel 3-249
multicast cloud, displaying information 3-387
multicasting
definition 3-249

N

NAT
configuring 2-171, 2-172
negating interface configurations 3-269
neighbor resets, enabling logging 3-239
netmon 3-263
netstatr 3-264
Network Address Translation
See NAT
network connectivity
testing 3-273

network entity title (NET)
CLNS 3-262
network host name
Service Engine 2-185
network interfaces
EtherChannel 2-189
Network Time Protocol
See NTP
network traffic
dumping 4-704
node
activating 2-106
communication over secure channels 2-105
not-so-stubby area (NSSA)
configuring 2-39
NTP
configuring and enabling 3-270
setting software time and date 3-272
status, displaying 3-498
system clock, synchronizing 3-270
number of lines displayed 4-714
NVRAM
configuration stored, displaying 3-553
startup configuration, writing or erasing 4-779

O

offset from UTC B-1
online help 2-184
OSPF (Open Shortest Path First)
configuration mode 1-4
database, displaying 3-435
debug information, displaying 2-135
defining interfaces 3-265
enabling 3-304
information, displaying 3-432, 3-434
interface, displaying 3-441
interfaces, configuring area ID 3-265
LSA
request list, displaying 3-447
retransmission list, displaying 3-448
LSA, displaying 3-435
memory, displaying 3-443
neighbor, displaying 3-445
RSPF route, displaying 3-449, 3-451
setting priority 2-209
statistics, displaying 3-453
outgoing proxy
authentication 2-33

P

pacing bit rate
movie-streamer and WMT 2-52
patterns
lists described 3-314
rules for lists 3-312
searching in files 2-174
permanent errors
FTP server 4-738
PGM protocol 3-253
ping 3-273
Service Router 3-274
ping IPv6 address 3-275
policies
and the Rules Template 3-313
port channel
configuring 2-187
load balancing options 3-276
negating interface configuration 3-269
powering off 4-668
present working directory
information, displaying 3-230, 3-289
preserving configurations on device restore 3-297
preserving data on device restore 3-297
primary Content Delivery System Manager 2-68
primary interface
changing to a different interface 3-278

configuring for Ethernet 3-278
priority
multicast 3-249
privileged level EXEC commands
accessing 2-166
disabling 2-150
processes
CPU or memory, displaying 3-500
programs
displaying 3-502
live 3-503
movie streamer rebroadcast 3-504
WMT rebroadcast
about 3-504
Proximity
debugging 2-138
turning on debug information 2-140
Proximity Engine 2-210
BGP proximity algorithm, enabling 3-280
configuring location community 3-231
deleting neighbors 2-85
enabling 3-286
proximity algorithm, displaying 3-455
proximity servers, displaying 3-456
replica-set information, displaying 3-547
route information, displaying 3-548

Q

question mark (?) 2-184
queue
multicast priority 3-249
QuickTime 3-307

R

RADIUS server
authentication 3-290
excluding domains 3-291
information, displaying 3-508
parameters, configuring 3-290
statistics
clearing 2-93
displaying 4-599
RealProxy
access control 3-309
error logging 3-238
Real-Time Streaming Protocol
See RTSP
rebooting Service Engine 3-295
Received Routing Message (RRM)
IS-IS 3-486
regular pattern expression
searching 2-174
reload 3-295
reloading Service Engine
automatic reload option 2-158
Remote Copy Program (RCP) 3-510
enabling 3-294
remote host route trace 4-720, 4-723, 4-724
removing
nodes from the CDS network 2-106
renaming a file 3-296
replication status and statistics, displaying 4-600
resetting
device to default condition 3-297
restart, cold 3-295
restoring
device to default condition 3-297
RIB (Routing Information Base)
debug information, displaying 2-139
memory, displaying 3-458
recursive next-hop
displaying, information 3-460
routing protocol
clients, displaying 3-457
unresolved next-hop

displaying 3-463
rotated log files 3-237
routes
displaying table 3-464
traceroute6 4-724
tracing 4-720, 4-723
RSPF (Reverse Shortest Path First)
OSPF route 3-449, 3-451
RTSP
configurations and license agreements 3-511
configuring 3-307
gateway, purpose of 3-308
gateway overview 3-308
Rules Template 3-313
rule actions
supported action and pattern combinations 3-314
rules
configuration, displaying 3-512
matching against regular expressions 3-312
setting filters 3-310
statistics, clearing 2-93
See also Rules Template
Rules Template
actions
description 3-314
patterns
description 3-316
running configuration
current profile, displaying 3-514
saving 4-779
running statistics, clearing 2-93

S

saving
configuration changes 1-6
file system contents 3-295
scheduled WMT rebroadcasts
about 3-504
script
executing 3-321
secret keys
RADIUS 3-291
TACACS+ 4-701
Secure Shell
See SSH
send echo packets (ping) 3-273, 3-275
Send Routing Message
IS-IS 3-489
Send Sequence Number (SSN)
IS-IS 3-490
service 3-322
Service Engine
automatic reload 2-158
Service Router
configuration 3-518
configuring 3-323
crossdomain support 3-328
ping 3-274
statistics, displaying 4-604
services
access lists 2-201
information 3-524
statistics 4-609
setup
configuring 3-339
Shortest Path First (SPF)
IS-IS 3-487
shutting down
Content Delivery System Managers 4-668
hardware interfaces 4-667
Program Managers 4-668
Service Engines 4-668
Service Routers 4-668
slash (/) 2-63
SNMP
communications status, displaying 3-526
community string, configuring 4-676

host trap recipient, setting 4-682
security model group, defining 4-680
server user, defining 4-688
statistics, clearing 2-93
statistics, displaying 4-610
system location string, setting 4-685
system notify inform string, configuring 4-686
system server contact string, setting 4-677
traps, configuring 4-678
traps, disabling 4-678
traps, enabling 4-678
Version 2 MIB view, defining 4-690
socket connection
statistics, displaying 4-598
software clock
setting 3-272
source IP routing
configuring 2-193
Splunk Universal Forwarder
configuring 4-692
Squid transaction log format 4-732
SRP (Service Routing Protocol)
configuration, displaying 3-546
configuration mode 1-4, 3-306
database, clearing 2-82
debug flags, displaying 3-379
debug information, displaying 2-142
descriptor, clearing resource 2-88
descriptor, deleting 2-83
descriptor information, displaying 3-530
domain id, setting 2-165
information, displaying 3-543
leafset, displaying 3-537
memory, displaying 3-539
multicast database, displaying 3-540
multicast flooding threshold 2-179
multicast group, displaying 3-550
statistics
clearing 2-93
statistics, displaying 4-612
ss 4-694
SSH
configuration and status, displaying 3-551
enabling daemon 4-696
session timeout 2-169
standard access lists
creating 2-202
standard time zones
and offsets from UTC B-1
list of B-1
standard timezones, displaying 3-363
standby Content Delivery System Manager 2-68
standby interface
displaying information 3-552
starting service 3-322
startup configuration
displaying 3-553
static IP routing
configuring 2-193
statistics
clearing 2-92
storage
prepositioned CDS network content 2-65
streaming media players
IP/TV Viewer 3-503
QuickTime 3-503
stub area
defining 2-40
subdirectories
viewing names 3-230
summer daylight saving time
setting 2-102
synchronizing
system clock 3-270
syslog
configuration, displaying 3-494
configuring 3-235
hosts, configuring 3-237

RealProxy priority level error mapping 3-238
sysfs location 3-237
system clock
synchronized by time server 3-270
system disk space usage 2-152
system hardware
displaying status 3-404
system help 1-6
system image
installing 2-186
system inventory
displaying 3-416
system logging
configuring 3-237
to console 3-235
to disk 3-235
to remote hosts 3-237

T

TAC
viewing technical support information 4-643
TACACS+
authentication information, displaying 4-641
configuring server parameters 4-700
statistics
clearing 2-94
displaying 4-613
TCP
access lists 2-203
keywords and port numbers 2-205
statistics
clearing 2-94
displaying 4-614
timestamp 4-711
tcpmon 4-709
technical support information
viewing 4-643
Telnet services
configuration, displaying 4-649
enabling 4-713
session timeout 2-5, 2-169
terminal
setting number of lines to be displayed 4-714
testing
connectivity of URLs
for FTP-over-HTTP 4-716
for HTTP 4-716
test-url command
troubleshooting
with the HTTP CLI client 4-716
TFTP
access lists 2-203
thresholds
disk error handling 2-158
time, correcting 2-30
time and date
setting 3-272
timeout of a nonresponsive host 3-273
timestamp
TCP 4-711
time zone
list of B-1
offset setting 2-103
setting 2-102
token strings 4-732
ToS
classification 2-196
trace the route of remote host 4-720, 4-723, 4-724
transaction logging
archive file naming convention 4-735
archiving working log files 2-97
clearing log export statistics 2-94
compressing archive files 4-737
configuration and archived files, displaying 4-650
configuring and enabling 4-727
exporting 4-737
forcing archive or export 4-725

formats 4-732
log export statistics, displaying 4-623
permanent errors from external server 4-738
transaction logs
archiving of 4-735
clearing 2-97
displaying configuration of 4-650
exporting 4-735
sanitizing 4-734
traps
enabling 4-678
troubleshooting
with ping 3-273
with Telnet client 4-712
with the HTTP CLI client 4-716
with traceroute 4-720
troubleshooting utilities
gulp 2-181
netmon 3-263
netstatr 3-264
ss 4-694
tcpmon 4-709

U

UDI compliance 3-416
UDP
access lists 2-203
keywords and port numbers 2-205
statistics
clearing 2-94
displaying 4-625
undoing global configuration commands 3-267
unicast static routes 2-210
Universal Coordinated Time
See UTC B-1
updating the calendar 2-100
URL signature 4-748
information, displaying 4-654
shared key 4-750
user-level EXEC command mode 1-3
username
displaying 4-764
users
administrative and authenticated, displaying 4-656
authenticated users, clearing 2-98
authentication 4-752
defining for SNMP server 4-688
removing data from disk 3-297
user identification number and name, displaying 4-655
UTC
and standard time zones B-1
clock EXEC command 2-103
offsets from B-1

V

variable bit rates 2-53
version
displaying information about 4-657

W

Web Engine
configuring 4-755, 4-758
information, displaying 4-659
statistics, clearing 2-94
statistics, displaying 4-626
WFQ
IP precedence
ToS 2-196
WMT 4-635
bit rate, setting 2-52
caching proxy
variable bit rates 2-53
configuration and license information, displaying 4-661

configuring 4-765
conventional proxy service 4-768
enabling 4-768
Fast Cache
enabling 4-768
Fast Start
enabling 4-768
live splitting 4-771
multicast
logging 4-770
overview 4-769
multicast-in and multicast-out 4-770
multicast-in and unicast-out 4-770
multicast-in multicast-out
description of 4-770
multicast-in unicast-out 4-770
multicast logging 4-770, 4-773
multicasts, types of
multicast-in multicast-out 4-770
multicast-in unicast-out 4-770
rebroadcasts 3-504
statistics
clearing 2-94
displaying 4-635
streaming and caching 4-635
unicast-in unicast-out
description of 4-770
unicast-out and multicast-in 4-770
WMT transaction logs
formats 4-771
logging usernames 4-773
specifying format of 4-771
working.log file 4-731