



## Cisco VDS Service Broker 1.3 Command Reference

November 1, 2013

Cisco Systems, Inc.  
[www.cisco.com](http://www.cisco.com)

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

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](http://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 VDS Service Broker 1.3 Command Reference*  
© 2004–2013 Cisco Systems, Inc. All rights reserved.



<b>Preface</b>	<b>ix</b>
<b>Document Revision History</b>	<b>ix</b>
<b>Document Organization</b>	<b>ix</b>
<b>Audience</b>	<b>x</b>
<b>Conventions</b>	<b>x</b>
<b>Related Documentation</b>	<b>xi</b>
<b>Obtaining Documentation and Submitting a Service Request</b>	<b>xi</b>

---

CHAPTER 1

<b>Command-Line Interface Command Summary</b>	<b>1-1</b>
<b>Using VDS-SB Device Modes</b>	<b>1-1</b>
<b>Using Command-Line Processing</b>	<b>1-2</b>
<b>Using Command Modes</b>	<b>1-3</b>
<b>Using EXEC Mode</b>	<b>1-3</b>
<b>Using Global Configuration Mode</b>	<b>1-4</b>
<b>Using Interface Configuration Mode</b>	<b>1-4</b>
<b>Using Other Configuration Modes</b>	<b>1-4</b>
<b>Checking the Command Syntax</b>	<b>1-5</b>
<b>System Help</b>	<b>1-7</b>
<b>Filtering Output Using Output Modifiers</b>	<b>1-7</b>
<b>Saving Configuration Changes</b>	<b>1-7</b>

---

CHAPTER 2

<b>Cisco VDS Service Broker Release 1.3 Software Commands</b>	<b>2-1</b>
<b>access-lists</b>	<b>2-13</b>
<b>alarm</b>	<b>2-16</b>
<b>asset</b>	<b>2-18</b>
<b>banner</b>	<b>2-19</b>
<b>cd</b>	<b>2-22</b>
<b>clear ip</b>	<b>2-23</b>
<b>clear logging</b>	<b>2-24</b>
<b>clear statistics</b>	<b>2-25</b>
<b>clear transaction-log</b>	<b>2-27</b>
<b>clear users</b>	<b>2-28</b>

<b>clock (EXEC Configuration)</b>	2-29
<b>clock (Global configuration)</b>	2-31
<b>cms (EXEC Configuration)</b>	2-34
<b>cms (Global configuration)</b>	2-38
<b>configure</b>	2-41
<b>copy</b>	2-42
<b>core-dump</b>	2-45
<b>cpfile</b>	2-46
<b>debug</b>	2-47
<b>delfile</b>	2-50
<b>deltree</b>	2-51
<b>device</b>	2-52
<b>dir</b>	2-54
<b>disable</b>	2-55
<b>disk (EXEC Configuration)</b>	2-56
<b>disk (Global configuration)</b>	2-61
<b>dnslookup</b>	2-65
<b>enable (EXEC Configuration)</b>	2-66
<b>enable (Global Configuration)</b>	2-67
<b>end</b>	2-68
<b>exec-timeout</b>	2-69
<b>exit</b>	2-70
<b>expert-mode</b>	2-71
<b>external-ip</b>	2-72
<b>find-pattern</b>	2-74
<b>ftp</b>	2-76
<b>geo-location-server</b>	2-77
<b>gulp</b>	2-78
<b>help</b>	2-81
<b>hostname</b>	2-82
<b>http</b>	2-83
<b>install</b>	2-84
<b>interface</b>	2-85
<b>iostat</b>	2-89
<b>ip (Global configuration)</b>	2-90

<b>ip (Interface configuration)</b>	2-96
<b>ip access-list</b>	2-99
<b>kernel</b>	2-107
<b>line</b>	2-108
<b>lls</b>	3-109
<b>logging</b>	3-110
<b>ls</b>	3-114
<b>mkdir</b>	3-115
<b>mkfile</b>	3-116
<b>model</b>	3-117
<b>mount-option</b>	3-118
<b>mpstat</b>	3-119
<b>netmon</b>	3-120
<b>netstatr</b>	3-121
<b>no (Global configuration)</b>	3-122
<b>no (Interface configuration)</b>	3-124
<b>ntp</b>	3-126
<b>ntpdate</b>	3-128
<b>ping</b>	3-129
<b>port-channel</b>	3-130
<b>primary-interface</b>	3-132
<b>pwd</b>	3-134
<b>radius-server</b>	3-135
<b>reload</b>	3-139
<b>rename</b>	3-140
<b>restore</b>	3-141
<b>rmdir</b>	3-144
<b>script</b>	3-145
<b>service</b>	3-146
<b>setup</b>	3-147
<b>show aaa</b>	3-148
<b>show access-lists</b>	3-151
<b>show alarms</b>	3-152
<b>show arp</b>	3-155
<b>show authentication</b>	3-156

<b>show banner</b>	3-157
<b>show bitrate</b>	3-158
<b>show clock</b>	3-159
<b>show cms</b>	3-162
<b>show debugging</b>	3-164
<b>show device-mode</b>	3-165
<b>show disks</b>	3-167
<b>show flash</b>	3-172
<b>show ftp</b>	3-174
<b>show geo-location-server</b>	3-175
<b>show geo-location-service</b>	3-176
<b>show hardware</b>	3-177
<b>show hosts</b>	3-183
<b>show interface</b>	3-184
<b>show inventory</b>	3-189
<b>show ip</b>	3-191
<b>show lacp</b>	3-193
<b>show logging</b>	3-195
<b>show mount-option</b>	3-197
<b>show ntp</b>	3-198
<b>show processes</b>	3-200
<b>show radius-server</b>	3-202
<b>show running-config</b>	3-204
<b>show service-broker</b>	3-208
<b>show services</b>	3-210
<b>show snmp</b>	3-212
<b>show ssh</b>	3-216
<b>show standby</b>	3-217
<b>show startup-config</b>	3-218
<b>show statistics</b>	3-221
<b>show statistics access-lists</b>	3-223
<b>show statistics admission</b>	3-224
<b>show statistics fd</b>	3-226
<b>show statistics icmp</b>	4-227
<b>show statistics ip</b>	4-233

<b>show statistics lsof</b>	4-236
<b>show statistics netstat</b>	4-237
<b>show statistics radius</b>	4-238
<b>show statistics services</b>	4-239
<b>show statistics snmp</b>	4-240
<b>show statistics tacacs</b>	4-242
<b>show statistics tcp</b>	4-243
<b>show statistics transaction-logs</b>	4-252
<b>show statistics udp</b>	4-254
<b>show tacacs</b>	4-255
<b>show tech-support</b>	4-257
<b>show telnet</b>	4-261
<b>show transaction-logging</b>	4-262
<b>show url-signature</b>	4-266
<b>show user</b>	4-267
<b>show users</b>	4-268
<b>show version</b>	4-269
<b>shutdown (Interface configuration)</b>	4-271
<b>shutdown (EXEC Configuration)</b>	4-272
<b>snmp-server community</b>	4-280
<b>snmp-server contact</b>	4-281
<b>snmp-server enable traps</b>	4-282
<b>snmp-server group</b>	4-284
<b>snmp-server host</b>	4-286
<b>snmp-server location</b>	4-288
<b>snmp-server notify inform</b>	4-289
<b>snmp-server user</b>	4-291
<b>snmp-server view</b>	4-293
<b>ss</b>	4-295
<b>ssh-key-generate</b>	4-297
<b>sshd</b>	4-298
<b>sysreport</b>	4-300
<b>tacacs</b>	4-301
<b>tcpdump</b>	4-305
<b>tcpdumpx</b>	4-310

<a href="#">tcpmon</a>	4-312
<a href="#">tcp</a>	4-314
<a href="#">telnet (EXEC Configuration)</a>	4-315
<a href="#">telnet (Global Configuration)</a>	4-316
<a href="#">terminal</a>	4-317
<a href="#">test-url</a>	4-318
<a href="#">top</a>	4-322
<a href="#">traceroute</a>	4-323
<a href="#">transaction-log force</a>	4-326
<a href="#">transaction-logs</a>	4-328
<a href="#">type</a>	4-342
<a href="#">type-tail</a>	4-344
<a href="#">undebug</a>	4-347
<a href="#">url-signature</a>	4-349
<a href="#">username</a>	4-353
<a href="#">vds</a>	4-356
<a href="#">whoami</a>	4-359
<a href="#">write</a>	4-360

---

APPENDIX A

---

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 ix](#)
- [Document Organization, page ix](#)
- [Audience, page x](#)
- [Conventions, page x](#)
- [Related Documentation, page xi](#)
- [Obtaining Documentation and Submitting a Service Request, page xi](#)

## 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-29483-01	April, 2013	This is the first release of this document.
OL-29483-02	May, 2013	Updated the title to 1.0.1 and modified the release date.
OL-29907-01	June, 2013	Updated the geo-location-server command.
OL-30247-01	July, 2013	Updated the show service-broker command.
OL-30247-02	November, 2013	Added the cdn-metric-provider option for the show service-broker command.

## Document Organization

[Table 2](#) describes the organization of the document.

**Table 2** Document Organization

Chapter	Description
<a href="#">Chapter 1, “Command-Line Interface Command Summary”</a>	This chapter describes how to use the VDS-SB <sup>1</sup> CLI <sup>2</sup> to configure software features.
<a href="#">Chapter 2, “Cisco VDS Service Broker Release 1.3 Software Commands”</a>	This chapter provides a complete list of Cisco Internet Streamer commands, listed alphabetically.
<a href="#">Appendix A, “Acronyms”</a>	This appendix lists the abbreviations and acronyms used in this guide.
<a href="#">Appendix B, “Standard Time Zones”</a>	This appendix lists all the standard time zones that you can configure on a CDE <sup>3</sup> and the offset from UTC <sup>4</sup> for each standard time zone.

1. VDS-SB = Videoscape Distribution Suite (VDS) Service Broker
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 VDS Service Broker Release 1.3. Before using this guide, you should have experience working with the Cisco VDS Service Broker 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 VDS-SB and are available from [cisco.com](http://cisco.com):

- *Cisco VDS Service Broker 1.3 API Guide*
- *Cisco VDS Service Broker 1.3 Command Reference*
- *Cisco VDS Service Broker 1.2 Alarms and Error Messages Guide*
- *Release Notes for Cisco VDS Service Broker 1.3*
- *Open Sources Used in VDS Service Broker Release 1.0.*

You can access the software documents at the following URL:

[http://www.cisco.com/en/US/products/ps7127/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps7127/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](http://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](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](http://www.cisco.com/en/US/docs/unified_computing/ucs/c/hw/C210M1/install/C210M1.html)

Cisco UCS B200 M3 Blade Server Installation and Service Note

[http://www.cisco.com/en/US/docs/unified\\_computing/ucs/hw/chassis/install/B200M3.html](http://www.cisco.com/en/US/docs/unified_computing/ucs/hw/chassis/install/B200M3.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.





# Command-Line Interface Command Summary

---

Release 1.3 of the Cisco Videoscape Distribution Suite Service Broker (VDS-SB) is the first release of the Videoscape Distribution System (VDS) group. VDS-SB is an extension of the Internet Streamer Content Delivery System (CDS).

As an extension of the Internet Streamer CDS, VDS-SB provides advanced request routing engine supporting different match criteria, flexible configurations, and adaptation techniques for performing request routing or brokering.

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

- [Using VDS-SB Device Modes, page 1-1](#)
- [Using Command-Line Processing, page 1-2](#)
- [Using Command Modes, page 1-3](#)
- [Checking the Command Syntax, page 1-5](#)
- [System Help, page 1-7](#)
- [Filtering Output Using Output Modifiers, page 1-7](#)
- [Saving Configuration Changes, page 1-7](#)



Note

---

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

---

## Using VDS-SB Device Modes

In the Cisco VDS-SB software, the device mode determines whether the VDS-SB device is functioning as a Service Broker(SB), or a Videoscape Distribution Suite Manager (VDSM). The commands available from a specific CLI mode are determined by the VDS-SB device mode that is 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 VDS Service Broker 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*

<b>Keystroke Combination</b>	<b>Function</b>
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 VDS Service Broker Release 1.3 software is similar to the CLI for the Cisco IOS software. Both the Cisco IOS software and the VDS-SB 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 VDS Service Broker Release 1.3 software CLI, and includes the following topics:

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

```
ServiceBroker> enable
ServiceBroker#
```

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:

```
ServiceBroker# 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 VDS-SB 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:

```
ServiceBroker# configure
ServiceBroker(config)#
```

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

```
ServiceBroker(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 VDS-SB 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:

```
ServiceBroker# configure
ServiceBroker(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:

```
ServiceBroker(config-if)# exit
ServiceBroker(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	<b>ip access-list standard</b>
Extended ACL configuration mode	<b>ip access-list extended</b>

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 VDS Service Broker Release 1.3 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:

```
ServiceBroker# 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:

```
ServiceBroker# 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:

```
ServiceBroker# 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:

```
ServiceBroker# 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:

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

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

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

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**:

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

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

## ■ Checking the Command Syntax

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

## 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 (?):

```
ServiceBroker# c1?  
clear clock
```

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

```
ServiceBroker# 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:

```
ServiceBroker# copy running-config startup-config
```

or

```
ServiceBroker# write
```

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





# Cisco VDS Service Broker Release 1.3 Software Commands

---

This chapter contains an alphabetical listing of all the commands in Cisco VDS Service Broker Release 1.3 software. The VDS-SB 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 VDS-SB 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 VDS-SB 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 VDS-SB software device mode determines whether the VDS-SB device is functioning as a Service Broker (SB), or Videoscape Distribution Suite Manager (VDSM). The commands available from a specific CLI mode are determined by the VDS-SB 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
<a href="#">access-lists</a>	Configures the access control list entries.	Global configuration	SB
<a href="#">alarm</a>	Configures alarms.	Global configuration	SB
<a href="#">asset</a>	Configures the CISCO-ENTITY-ASSET-MIB.	Global configuration	All
<a href="#">banner</a>	Configures the EXEC, login, and MOTD <sup>1</sup> banners.	Global configuration	All
<a href="#">cd</a>	Changes the directory.	User-level EXEC and privileged-level EXEC	All
<a href="#">clear ip</a>	Clears the IP configuration.	Privileged-level EXEC	All
<a href="#">clear logging</a>	Clears the syslog messages saved in the disk file.	Privileged-level EXEC	All
<a href="#">clear statistics</a>	Clears the statistics.	Privileged-level EXEC	All
<a href="#">clear transaction-log</a>	Clears and archives the working transaction logs.	Privileged-level EXEC	SB
<a href="#">clear users</a>	Clears the connections (login) of authenticated users.	Privileged-level EXEC	All
<a href="#">clock (EXEC Configuration)</a>	Manages the system clock.	Privileged-level EXEC	All
<a href="#">clock (Global configuration)</a>	Sets the summer daylight saving time of day and time zone.	Global configuration	All
<a href="#">cms (EXEC Configuration)</a>	Configures the CMS <sup>2</sup> -embedded database parameters.	Privileged-level EXEC	All
<a href="#">cms (Global configuration)</a>	Schedules the maintenance and enables the Centralized Management System on a given node.	Global configuration	All
<a href="#">configure</a>	Enters configuration mode from privileged EXEC mode <sup>3</sup> .	Privileged-level EXEC	All
<a href="#">copy</a>	Copies the configuration or image files to and from the CD-ROM, flash memory, disk, or remote hosts.	Privileged-level EXEC	All
<a href="#">core-dump</a>	Configures a coredump file.	Privileged-level EXEC	All
<a href="#">cpfile</a>	Copies a file.	User-level EXEC and privileged-level EXEC	All
<a href="#">debug</a>	Configures the debugging options.	Privileged-level EXEC	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
<a href="#">delfile</a>	Deletes a file.	User-level EXEC and privileged-level EXEC	All
<a href="#">deltree</a>	Deletes a directory and its subdirectories.	User-level EXEC and privileged-level EXEC	All
<a href="#">device</a>	Configures the mode of operation on a device.	Global configuration	All
<a href="#">dir</a>	Displays the list of files in a directory.	User-level EXEC and privileged-level EXEC	All
<a href="#">disable</a>	Turns off the privileged EXEC commands.	Privileged-level EXEC	All
<a href="#">disk (EXEC Configuration)</a>	Allocates the disks among the CDNFS and sysfs file systems.	Privileged-level EXEC	All
<a href="#">disk (Global configuration)</a>	Configures how the disk errors should be handled.	Global configuration	All
<a href="#">dnslookup</a>	Resolves a host or domain name to an IP address.	User-level EXEC and privileged-level EXEC	All
<a href="#">enable (EXEC Configuration)</a>	Accesses the privileged EXEC commands.	User-level EXEC and privileged-level EXEC	All
<a href="#">enable (Global Configuration)</a>	Changes the enable password.	Global configuration	All
<a href="#">end</a>	Exits configuration and privileged EXEC modes.	Global configuration	All
<a href="#">exec-timeout</a>	Configures the length of time that an inactive Telnet or SSH session remains open.	Global configuration	All
<a href="#">exit</a>	Exits from interface, Global configuration, or privileged EXEC modes.	All	All
<a href="#">expert-mode</a>	Configures debugshell.	Global configuration	All
<a href="#">external-ip</a>	Configures up to a maximum of eight external IP addresses.	Global configuration	All
<a href="#">find-pattern</a>	Searches for a particular pattern in a file.	Privileged-level EXEC	All
<a href="#">ftp</a>	Enables FTP <sup>4</sup> services.	Global configuration	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
<code>geo-location-server</code>	Monitors primary and secondary servers.	User-level EXEC and privileged-level EXEC	All
<code>gulp</code>	Captures lossless gigabit packets and writes them to disk.	Privileged-level EXEC	All
<code>help</code>	Obtains online help for the command-line interface.	Global configuration and user-level EXEC	All
<code>hostname</code>	Configures the device network name.	Global configuration	All
<code>http</code>	Configures HTTP-related parameters	Privileged-level EXEC	SB
<code>install</code>	Installs a new version of the caching application.	Privileged-level EXEC	All
<code>interface</code>	Configures a Gigabit Ethernet or port channel interface. Provides access to interface configuration mode.	Global configuration	All
<code>iostat</code>	Shows CPU and I/O statistics for devices and partitions.	Global configuration	All
<code>ip (Global configuration)</code>	Configures the Internet Protocol.	Global configuration	All
<code>ip (Interface configuration)</code>	Configures the interface Internet Protocol.	Interface configuration	All
<code>ip access-list</code>	Creates and modifies the access lists for controlling access to interfaces or applications. Provides access to ACL configuration mode.	Global configuration	All
<code>kernel</code>	Configures the kernel.	Global configuration	All
<code>line</code>	Specifies the terminal line settings.	Global configuration	All
<code>lls</code>	Displays the files in a long-list format.	User-level EXEC and privileged-level EXEC	All
<code>logging</code>	Configures syslog <sup>5</sup> .	Global configuration	All
<code>ls</code>	Lists the files and subdirectories in a directory.	User-level EXEC and privileged-level EXEC	All
<code>mkdir</code>	Makes a directory.	User-level EXEC and privileged-level EXEC	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
<a href="#">mkfile</a>	Makes a file (for testing).	User-level EXEC and privileged-level EXEC	All
<a href="#">model</a>	Changes the CDE250 platform model number after a remanufacturing or rescue process.	User-level EXEC and privileged-level EXEC	All
<a href="#">mount-option</a>	Configures the mount option profile for remote storage.	Global Configuration	SB
<a href="#">mpstat</a>	Displays processor-related statistics.	Privileged-level EXEC	SB
<a href="#">netmon</a>	Displays the transmit and receive activity on an interface.	Privileged-level EXEC	All
<a href="#">netstatr</a>	Displays the rate of change of netstat statistics.	Privileged-level EXEC	All
<a href="#">no (Global configuration)</a>	Negates a Global configuration command or sets its defaults.	Global configuration	All
<a href="#">no (Interface configuration)</a>	Negates an interface command or sets its defaults.	Interface configuration	All
<a href="#">ntp</a>	Configures the Network Time Protocol server.	Global configuration	All
<a href="#">ntpdate</a>	Sets the NTP software clock.	Privileged-level EXEC	All
<a href="#">ping</a>	Sends the echo packets.	User-level EXEC and privileged-level EXEC	All
<a href="#">port-channel</a>	Configures the port channel load balancing options.	Global configuration	All
<a href="#">primary-interface</a>	Configures a primary interface for the VDS-SB network to be a Gigabit Ethernet or port channel interface.	Global configuration	All
<a href="#">pwd</a>	Displays the present working directory.	User-level EXEC and privileged-level EXEC	All
<a href="#">radius-server</a>	Configures the RADIUS authentication.	Global configuration	All
<a href="#">reload</a>	Halts a device and performs a cold restart.	Privileged-level EXEC	All
<a href="#">rename</a>	Renames a file.	User-level EXEC and privileged-level EXEC	All
<a href="#">restore</a>	Restores a device to its manufactured default status.	Privileged-level EXEC	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
<code>rmdir</code>	Removes a directory.	User-level EXEC and privileged-level EXEC	All
<code>script</code>	Checks the errors in a script or executes a script.	Privileged-level EXEC	All
<code>service</code>	Specifies the type of service.	Privileged-level EXEC	All
<code>setup</code>	Configures service routing.	Global configuration	All
<code>setup</code>	Configures the basic configuration settings and a set of commonly used caching services.	Privileged-level EXEC	All
<code>show aaa</code>	Display the accounting, authentication, and authorization configuration	User-level EXEC and privileged-level EXEC	All
<code>show access-lists</code>	Displays the access control list configuration.	User-level EXEC and privileged-level EXEC	SB
<code>show alarms</code>	Displays information on various types of alarms, their status, and history.	User-level EXEC and privileged-level EXEC	All
<code>show arp</code>	Displays the Address Resolution Protocol entries.	User-level EXEC and privileged-level EXEC	All
<code>show authentication</code>	Displays the authentication configuration.	User-level EXEC and privileged-level EXEC	All
<code>show banner</code>	Displays information on various types of banners.	User-level EXEC and privileged-level EXEC	All
<code>show bitrate</code>	Displays the SB bit-rate configuration.	User-level EXEC and privileged-level EXEC	SB
<code>show clock</code>	Displays the system clock.	User-level EXEC and privileged-level EXEC	All
<code>show cms</code>	Displays the Centralized Management System protocol, embedded database content, maintenance status, and other information.	User-level EXEC and privileged-level EXEC	All
<code>show debugging</code>	Displays the state of each debugging option.	User-level EXEC and privileged-level EXEC	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
<code>show device-mode</code>	Displays the configured or current mode of a VDSM, or SB	User-level EXEC and privileged-level EXEC	All
<code>show disks</code>	Displays the disk configurations.	User-level EXEC and privileged-level EXEC	All
<code>show flash</code>	Displays the flash memory information.	User-level EXEC and privileged-level EXEC	All
<code>show ftp</code>	Displays the caching configuration of the FTP.	User-level EXEC and privileged-level EXEC	All
<code>show geo-location-server</code>	Displays the Geo Location Server details.	User-level EXEC and privileged-level EXEC	All
<code>show geo-location-service</code>	Displays if location service is enabled or disabled.	User-level EXEC and privileged-level EXEC	All
<code>show hardware</code>	Displays the system hardware information.	User-level EXEC and privileged-level EXEC	All
<code>show hosts</code>	Displays the IP domain name, name servers, IP addresses, and host table.	User-level EXEC and privileged-level EXEC	All
<code>show interface</code>	Displays the hardware interface information.	User-level EXEC and privileged-level EXEC	All
<code>show inventory</code>	Displays the system inventory information.	User-level EXEC and privileged-level EXEC	All
<code>show ip</code>	Displays the contents of a particular host in the BGP routing table.	User-level EXEC and privileged-level EXEC	All
<code>show lacp</code>	Displays LACP information.	User-level EXEC and privileged-level EXEC	All
<code>show logging</code>	Displays the system logging configuration.	User-level EXEC and privileged-level EXEC	All
<code>show mount-option</code>	Displays mount options.	User-level EXEC and privileged-level EXEC	SB

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
<code>show ntp</code>	Displays the Network Time Protocol configuration status.	User-level EXEC and privileged-level EXEC	All
<code>show processes</code>	Displays the process status.	User-level EXEC and privileged-level EXEC	All
<code>show radius-server</code>	Displays the RADIUS server information.	User-level EXEC and privileged-level EXEC	All
<code>show running-config</code>	Displays the current operating configuration.	User-level EXEC and privileged-level EXEC	All
<code>show service-broker</code>	Display the Service Broker configuration.	User-level EXEC and privileged-level EXEC	All
<code>show services</code>	Displays the services-related information.	User-level EXEC and privileged-level EXEC	All
<code>show snmp</code>	Displays the SNMP <sup>6</sup> parameters.	User-level EXEC and privileged-level EXEC	All
<code>show ssh</code>	Displays the Secure Shell status and configuration.	User-level EXEC and privileged-level EXEC	All
<code>show standby</code>	Displays the information related to the standby interface.	User-level EXEC and privileged-level EXEC	All
<code>show startup-config</code>	Displays the startup configuration.	User-level EXEC and privileged-level EXEC	All
<code>show statistics</code>	Display the Service Broker statistics.	User-level EXEC and privileged-level EXEC	All
<code>show statistics access-lists</code>	Displays the access control list statistics.	User-level EXEC and privileged-level EXEC	SB
<code>show statistics admission</code>	Displays admission control statistics.	User-level EXEC and privileged-level EXEC	SB
<code>show statistics fd</code>	Displays the file descriptors limits.	User-level EXEC and privileged-level EXEC	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
<code>show statistics icmp</code>	Displays the ICMP <sup>7</sup> statistics.	User-level EXEC and privileged-level EXEC	All
<code>show statistics ip</code>	Displays the Internet Protocol statistics.	User-level EXEC and privileged-level EXEC	All
<code>show statistics lsof</code>	Displays the List of Open File descriptors.	User-level EXEC and privileged-level EXEC	All
<code>show statistics netstat</code>	Displays the Internet socket connection statistics.	User-level EXEC and privileged-level EXEC	All
<code>show statistics radius</code>	Displays the RADIUS authentication statistics.	User-level EXEC and privileged-level EXEC	All
<code>show statistics services</code>	Displays the services statistics.	User-level EXEC and privileged-level EXEC	All
<code>show statistics snmp</code>	Displays the SNMP statistics.	User-level EXEC and privileged-level EXEC	All
<code>show statistics tacacs</code>	Displays the Service Engine TACACS+ authentication and authorization statistics.	User-level EXEC and privileged-level EXEC	All
<code>show statistics tcp</code>	Displays the Transmission Control Protocol statistics.	User-level EXEC and privileged-level EXEC	All
<code>show statistics transaction-logs</code>	Displays the transaction log export statistics.	User-level EXEC and privileged-level EXEC	SB
<code>show statistics udp</code>	Displays the User Datagram Protocol statistics.	User-level EXEC and privileged-level EXEC	All
<code>show tacacs</code>	Displays TACACS+ authentication protocol configuration information.	User-level EXEC and privileged-level EXEC	All
<code>show tech-support</code>	Displays the system information for Cisco technical support.	User-level EXEC and privileged-level EXEC	All
<code>show telnet</code>	Displays the Telnet services configuration.	User-level EXEC and privileged-level EXEC	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
<code>show transaction-logging</code>	Displays the transaction logging information.	User-level EXEC and privileged-level EXEC	SB
<code>show url-signature</code>	Displays the URL signature information.	User-level EXEC and privileged-level EXEC	SB
<code>show user</code>	Displays the user identification number and username information.	User-level EXEC and privileged-level EXEC	All
<code>show users</code>	Displays the specified users.	User-level EXEC and privileged-level EXEC	All
<code>show version</code>	Displays the software version.	User-level EXEC and privileged-level EXEC	All
<code>shutdown (Interface configuration)</code>	Shuts down the specified interface.	Interface configuration	All
<code>shutdown (EXEC Configuration)</code>	Shuts down the device (stops all applications and operating system).	Privileged-level EXEC	All
<code>snmp-server community</code>	Configures the community access string to permit access to the SNMP.	Global configuration	All
<code>snmp-server contact</code>	Specifies the text for the MIB object sysContact.	Global configuration	All
<code>snmp-server enable traps</code>	Enables the SNMP traps.	Global configuration	All
<code>snmp-server group</code>	Defines a user security model group.	Global configuration	All
<code>snmp-server host</code>	Specifies the hosts to receive SNMP traps.	Global configuration	All
<code>snmp-server location</code>	Specifies the path for the MIB object sysLocation.	Global configuration	All
<code>snmp-server notify inform</code>	Configures the SNMP inform request.	Global configuration	All
<code>snmp-server user</code>	Defines a user who can access the SNMP engine.	Global configuration	All
<code>snmp-server view</code>	Defines an SNMPv2 <sup>8</sup> MIB view.	Global configuration	All
<code>ss</code>	Dumps socket statistics.	Privileged-level EXEC	All
<code>ssh-key-generate</code>	Generates the SSH host key.	Global configuration	All
<code>sshd</code>	Configures the SSH service parameters.	Global configuration	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
<a href="#">sysreport</a>	Saves the sysreport to a user-specified file.	Privileged-level EXEC	SB
<a href="#">tacacs</a>	Configures TACACS+ server parameters.	Global configuration	All
<a href="#">tcpdump</a>	Dumps the TCP traffic on the network.	Privileged-level EXEC	All
<a href="#">tcpdumpx</a>	Dumps the network traffic with the tcpdump extension for a multi-interface capture.	Privileged-level EXEC	All
<a href="#">tcpmon</a>	Searches all TCP connections.	Privileged-level EXEC	All
<a href="#">tcp</a>	Configures TCP-related parameters.	Global configuration	All
<a href="#">telnet (EXEC Configuration)</a>	Starts the Telnet client.	User-level EXEC and privileged-level EXEC	All
<a href="#">telnet (Global Configuration)</a>	Enables Telnet service.	Global configuration	All
<a href="#">terminal</a>	Sets the terminal output commands.	User-level EXEC and privileged-level EXEC	All
<a href="#">test-url</a>	Tests the accessibility of a URL using FTP, HTTP, or HTTPS.	User-level EXEC and privileged-level EXEC	SB
<a href="#">top</a>	Displays a dynamic real-time view of a running VDS-SB.	Privileged-level EXEC	All
<a href="#">traceroute</a>	Traces the route to a remote host.	User-level EXEC and privileged-level EXEC	All
<a href="#">transaction-log force</a>	Forces archiving of the working log file to make a transaction log file.	Privileged-level EXEC	SB
<a href="#">transaction-logs</a>	Configures and enables the transaction logging parameters.	Global configuration	SB
<a href="#">type</a>	Displays a file.	User-level EXEC and privileged-level EXEC	All
<a href="#">type-tail</a>	Displays the last several lines of a file.	User-level EXEC and privileged-level EXEC	All
<a href="#">undebug</a>	Disables debugging functions.	Privileged-level EXEC	All
<a href="#">url-signature</a>	Configures the URL signature.	Global configuration	SB

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
<code>username</code>	Establishes the username authentication.	Global configuration	All
<code>vds</code>	Configure the VDS-SB IP address to be used for the SBs , or configures the role and GUI parameters on a VDSM <sup>9</sup> device.	Global configuration	All
<code>whoami</code>	Displays the current user's name.	User-level EXEC and privileged-level EXEC	All
<code>write</code>	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. MOTD = message-of-the-day
2. CMS = Centralized Management System
3. Commands used to access configuration modes.
4. FTP = File Transfer Protocol
5. syslog = system logging
6. SNMP = Simple Network Management Protocol
7. ICMP = Internet Control Message Protocol
8. SNMPv2 = Simple Network Management Protocol version 2
9. Virtual Service Broker Manager

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

**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 SB. 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 SB. For instance, use the **access-lists 300 deny groupname marketing** command to prevent any user from the marketing group from accessing content through an SB.

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 string* 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:

```
ServiceBroker# 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:

```
ServiceBroker# 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:

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

### Related Commands

Command	Description
<b>show access-lists 300</b>	Displays the ACL configuration.
<b>show statistics access-list 300</b>	Displays the ACL statistics.

# 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

<b>admin-shutdown-alarm</b>	Generates a linkdown alarm when an interface shuts down.
<b>enable</b>	Enables admin shutdown alarm overload detection.
<b>overload-detect</b>	Specifies alarm overload configuration.
<b>clear</b>	Specifies the threshold below which the alarm overload state on an SB is cleared and the Simple Network Management Protocol (SNMP) traps and alarm notifications to the Centralized Management System (CMS) resume.  <b>Note</b> The <b>alarm overload-detect clear</b> command value must be less than the <b>alarm overload-detect raise</b> value.
<i>1-999</i>	Number of alarms per second that ends an alarm overload condition.
<b>raise</b>	(Optional) Specifies the threshold at which the CDE enters an alarm overload state and SNMP traps and alarm notifications to CMS are suspended.
<i>10-1000</i>	Number of alarms per second that triggers an alarm overload.
<b>enable</b>	Enables the detection of alarm overload situations.

## 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 SB experience problems at the same time, numerous alarms are set off simultaneously, and an SB 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 SB enters an alarm overload state until the number of alarms drops down to the number defined in the **clear**.

When an SB 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.
- SB 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 SB. 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:

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

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

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

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

```
ServiceBroker(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:

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

### Related Commands

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

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

**Defaults** None

**Command Modes** Global configuration (config) mode.

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

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

# 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

<b>enable</b>	Enables banner support on the SB.
<b>exec</b>	Configures an EXEC banner.
<b>message</b>	Specifies a message to be displayed when an EXEC process is created.
<i>line</i>	EXEC message text on a single line. The SB translates the \n portion of the message to a new line when the EXEC banner is displayed to the user.
<i>message_text</i>	EXEC message text on one or more lines. Press the <b>Return</b> 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.  <b>Note</b> The EXEC banner content is obtained from the command-line input that the user enters after being prompted for the input.
<b>login</b>	Configures a login banner.
<b>message</b>	Specifies a message to be displayed before the username and password login prompts.
<i>line</i>	Login message text on a single line. The SB translates the \n portion of the message to a new line when the login banner is displayed to the user.
<i>message_text</i>	Login message text on one or more lines. Press the <b>Return</b> 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.  <b>Note</b> The login banner content is obtained from the command-line input that the user enters after being prompted for the input.
<b>motd</b>	Configures an MOTD banner.
<b>message</b>	Specifies an MOTD message.
<i>line</i>	MOTD message text on a single line. The SB translates the \n portion of the message to a new line when the MOTD banner is displayed to the user.
<i>message_text</i>	MOTD message text on one or more lines. Press the <b>Return</b> 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.  <b>Note</b> The MOTD banner content is obtained from the command line input that the user enters after being prompted for the input.

---

**Defaults** Banner support is disabled by default.

---

**Command Modes** Global configuration (config) mode.

---

**Usage Guidelines** You can configure the following three types of banners in any VDS-SB 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 SB. 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 SB, 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 SB.

---



---

**Examples** The following example shows how to enable banner support on the SB:

```
ServiceBroker(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.

```
ServiceBroker(config)# banner motd message This is an VDS-SB 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 SB translates the \n portion of the message to a new line when the MOTD message is displayed to the user.

```
ServiceBroker(config)# banner motd message "This is the motd message.
\nThis is an VDS-SB 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, SB A translates the \n portion of the message to a new line in the login message that is displayed to the user.

```
ServiceBroker(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.

```
ServiceBroker(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 VDS-SB username and password to log in to this SB.\n
.
Message has 99 characters.
ServiceBroker(config)#
```

Assume that the SB 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 SB, 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 VDS-SB 2.3 device
This is login banner.
Use your password to login.
```

```
Cisco SB
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 VDS-SB 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 VDS-SB username and password to log in to this SB.
```

After the user enters a valid VDS-SB username and password, the SB 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:

```
ServiceBroker#
```

## Related Commands

Command	Description
<b>show banner</b>	Enables banner support on the SB.

# cd

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

**cd** *directoryname*

<b>Syntax Description</b>	<i>directoryname</i>	Directory name.
---------------------------	----------------------	-----------------

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	EXEC configuration mode.
----------------------	--------------------------

<b>Usage Guidelines</b>	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 (/).
-------------------------	--

<b>Examples</b>	The following example shows how to use a relative path:
-----------------	---

```
ServiceBroker(config)# cd local1
```

	The following example shows how to use an absolute path:
--	--

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

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

# clear ip

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

**clear ip access-list counters** [*standard\_acl\_num* | *extended\_acl\_num* | *acl-name*]

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

**Defaults** None

**Command Modes** EXEC configuration mode.

**Examples** The following example shows how to clear IP counters:

```
ServiceRouter# clear ip counters
ServiceRouter#
```

Related Commands	Command	Description
	<b>show ip bgp summary</b>	Displays the status of all BGP connections.

# 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.

---

**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 ServiceBroker# exec_clear_logging:Syslog cleared
```

---

**Examples** The following example shows how to clear the syslogs:

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

## clear statistics

Command	Description
<b>ssh-key generate</b>	Generates an ssh key.

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

On the SB:

```
clear statistics {all | history | icmp | ip | radius | running | service-broker | snmp | tacacs | tcp |
udp}
```

On the VDSM:

```
clear statistics {all | history | icmp | ip | radius | running | snmp | tacacs | tcp | udp}
```

Syntax Description	all	Description
	<b>all</b>	Clears all statistics.
	<b>history</b>	Clears the statistics history.
	<b>icmp</b>	Clears the ICMP statistics.
	<b>ip</b>	Clears the IP statistics.
	<b>radius</b>	Clears the RADIUS statistics.
	<b>running</b>	Clears the running statistics.
	<b>service-broker</b>	Clears Service Broker statistics.
	<b>snmp</b>	Clears the SNMP statistics.
	<b>tacacs</b>	Clears the TACACS+ statistics.
	<b>tcp</b>	Clears the TCP statistics.
	<b>udp</b>	Clears the UDP statistics.

**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.

The **clear statistics all** commands clear only normal statistics.

**Examples** The following example shows how to clear all statistics on the Service Broker:

```
ServiceRouter# clear statistics all
ServiceRouter#
```

■ clear statistics

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show statistics</b>	Displays statistics information.

# clear transaction-log

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

## clear transaction-log

**Syntax Description** This command has no keywords or arguments.

**Defaults** None

**Command Modes** EXEC configuration mode.

**Usage Guidelines** The **clear transaction-log** command causes the transaction log to be archived immediately to the SB 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:

```
ServiceBroker# clear transaction-log
```

Related Commands	Command	Description
	<b>show statistics transaction-logs</b>	Displays SB transaction log export statistics.
	<b>show transaction-logging</b>	Displays transaction log information.
	<b>transaction-log force</b>	Forces the archive or export of the transaction log.
	<b>transaction-logs</b>	Configures and enables transaction logs.

# clear users

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

## clear users administrative

<b>Syntax Description</b>	<b>administrative</b>	Clears the connections of administrative users who have been authenticated through a remote login service.
---------------------------	-----------------------	--

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	EXEC configuration mode.
----------------------	--------------------------

<b>Usage Guidelines</b>	The <b>clear users administrative</b> 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.
-------------------------	--

<b>Examples</b>	The following example shows how to clear the connections of the authenticated users:
-----------------	--

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

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show user</b>	Displays the user identification number and username information for a particular user.
	<b>show users</b>	Displays the specified users.
	<b>username</b>	Establishes the username authentication.

## clock (EXEC Configuration)

Command	Description
<b>show statistics wmt</b>	Displays the WMT statistics.
<b>show wmt</b>	Displays WMT bandwidth and proxy mode configuration.

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

**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 SB 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 SB for the NTP by using the **ntp** command. See the “[ntp](#)” section on page -126 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 SB:

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

---

**Related Commands**

Command	Description
<b>clock timezone</b>	Sets the clock timezone.
<b>ntp</b>	Configures the Network Time Protocol server.
<b>show clock detail</b>	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 houroffset minutesoffset}}
```

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

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

## clock (Global configuration)

<i>houroffset</i>	Hours offset (see <a href="#">Table B-1</a> ) from UTC. The range is from -23 to +23.
<i>minutesoffset</i>	Minutes offset (see <a href="#">Table B-1</a> ) from UTC. The range is from 0 to 59.

**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 *00* is the offset (ahead or behind) Coordinated Universal Time (UTC) in hours and minutes. UTC was formerly known as *Greenwich Mean Time* (GMT).

```
SB(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:

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

The following example shows how to configure a standard time zone on the SB:

```
ServiceBroker(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.
ServiceBroker(config)#
```

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

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

The following example shows how to configure daylight saving time:

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

---

**Related Commands**

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

## cms (EXEC Configuration)

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

**Defaults** None

**Command Modes** EXEC configuration mode.

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

Use the **cms config-sync** command to enable registered SBs, and standby VDSM to contact the primary VDSM 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 VDSM and activated, it appears as Pending in the VDSM 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 VDS-SB 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 VDSM over the SSL protocol and then stores the new node information. The VDSM 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 VDSM GUI.

Once the node is activated, it automatically receives configuration updates and the necessary security RSA certificate-key pair from the VDSM. This security key allows the node to communicate with any other node in the VDS-SB network. The **cms deregister** command removes the node from the VDS-SB 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 SB as the Content Acquirer in each delivery service where this SB is assigned as the Content Acquirer and try the **cms deregister** command again.

To back up the existing management database for the VDSM, 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 VDSM GUI.

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

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

When you enter the **cms lcm disable** command, the CMS process running on SBs, and the standby VDSM does not send the CLI changes to the primary VDSM. Settings configured using the device CLIs are not sent to the primary VDSM.

If LCM is disabled, the settings configured through the VDSM GUI overwrite the settings configured from the SB; however, this rule applies only to those local device settings that have been overwritten by the VDSM 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 VDSM, the local device configuration is applicable until the VDSM requests a full-device statistics update from the SB

(clicking the **Force full database update** button from the Device Home window of the VDSM GUI triggers a full update). When the VDSM requests a full update from the device, the VDSM settings overwrite the local device settings.

The **cms deregister force** command should be used only as the last option, because the VDSM 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 VDSM or registering the device to another VDSM. The **cms deregister force** command forces the deregistration to continue.

## Examples

The following example shows how to back up the database management tables:

```
VDSM# cms database backup
creating backup file with label `backup'
backup file local1/VDS-SB-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:

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

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

```
ServiceBroker# 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 VDSM
10.107.192.168
...
ServiceBroker#
```

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

```
ServiceBroker# 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 VDSM
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 SB.
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_VDSM.
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-VDSM 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.
ServiceBroker#

```

The following example shows the use of the **cms recover identity** command when the hostname of the SB does not match the hostname configured in the VDSM GUI:

```

ServiceBroker# 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 VDSM
10.107.192.168
There are no SB devices in CDN
register: Registration failed.
ServiceBroker#

```

### Related Commands

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

**Defaults**

**database maintenance regular:** enabled  
**database maintenance full:** enabled  
**connection:** 30 seconds for VDSM; 180 seconds for the SB  
**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 SB from the VDS-SB 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.:

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

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

```
ServiceBroker(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 VDSM
10.107.192.168
Thu Jun 26 13:18:27 UTC 2003 [ I ] main: Connecting storeSetup for SB.
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_VDSM.
Thu Jun 26 13:18:40 UTC 2003 [ I ] main: Created SYS_MESS_TIME_IDX index.
Thu Jun 26 13:18:40 UTC 2003 [ I ] main: Created SYS_MESS_NODE_IDX index.
Thu Jun 26 13:18:40 UTC 2003 [ I ] main: No Consistency check for store.
Thu Jun 26 13:18:40 UTC 2003 [ I ] main: Successfully created management tables
Thu Jun 26 13:18:40 UTC 2003 [ I ] main: Registering object factories for persistent
store...
```

## ■ cms (Global configuration)

```

Thu Jun 26 13:18:40 UTC 2003 [ I ] main: AStore Loading store data...
Thu Jun 26 13:18:41 UTC 2003 [ I ] main: ExtExpiresRecord Loaded 0 Expires records.
Thu Jun 26 13:18:41 UTC 2003 [ I ] main: Skipping Construction RdToClusterMappings on
non-VDSM 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 VDSM. Any configuration changes
made via CLI on this device will be overwritten if they conflict with settings on the
VDSM.
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 VDSM UI.
management services enabled
ServiceBroker(config)#

```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>cms database</b>	Creates, backs up, deletes, restores, or validates the CMS-embedded database management tables or files.
<b>show cms</b>	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.

---

**Defaults** None

---

**Command Modes** EXEC configuration mode.

---

**Examples** The following example shows how to enable Global configuration mode:

```
ServiceBroker# configure
ServiceBrokerServiceBroker(config)#
```

---

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

---

# 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*} *remotefile* *remotefilename* *localfilename* | **startup-config** *filename*}

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

**copy http install** {{*hostname* | *ip-address*} *remotefile* *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

<b>cdnfs</b>	Copies a file from the CDNFS to the sysfs.
<b>disk</b>	Copies a file to the disk.
<i>url</i>	URL of the CDNFS file to be copied to the sysfs.
<i>sysfs-filename</i>	Filename to be copied in the sysfs.
<b>disk</b>	Copies a local disk file.
<b>ftp</b>	Copies to a file on an FTP server.
<i>hostname</i>	Hostname of the FTP server.
<i>ip-address</i>	IP address of the FTP server.
<i>remotefile</i>	Directory on the FTP server to which the local file is copied.
<i>remotefilename</i>	Name of the local file after it has been copied to the FTP server.
<i>localfilename</i>	Name of the local file to be copied.
<b>startup-config</b>	Copies the configuration file from the disk to startup configuration (NVRAM).
<i>filename</i>	Name of the existing configuration file.
<b>ftp</b>	Copies a file from an FTP server.
<b>disk</b>	Copies a file to a local disk.
<i>hostname</i>	Hostname of the FTP server.
<i>ip-address</i>	IP address of the FTP server.
<i>remotefile</i>	Directory on the FTP server where the file to be copied is located.
<i>remotefilename</i>	Name of the file to be copied to the local disk.
<i>localfilename</i>	Name of the copied file as it appears on the local disk.

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

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

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

# core-dump

To configure a coredump file, use the **core-dump** command in EXEC configuration mode.

```
core-dump {backtrace {all| word} | service { cms force | dns force | service-broker force | wmt pid}}
```

Syntax	Description
<b>backtrace</b>	Displays the backtrace of a coredump file.
<b>all</b>	Displays the backtraces of all core files.
<i>word</i>	Specifies the name of the core file.
<b>service</b>	Creates a core dump of a specific service.
<b>force</b>	Forces a core dump of the service.
<b>cms</b>	Specifies cms services.
<b>dns</b>	Specifies dns services.
<b>service-broker</b>	Specifies service-broker services.
<b>wmt</b>	Specifies wmt services.
<b>pid</b>	Specifies the PID of the process.

**Defaults** None

**Command Modes** EXEC configuration mode.

**Examples** The following example shows how to display the backtrace of all coredump files:

```
ServiceBroker# core backtrace al
```

# cpfile

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

**cpfile** *oldfilename newfilename*

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

**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:

```
ServiceBroker# cpfile syslog.txt syslog.txt.save
```

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

<b>Syntax Description</b>	<i>option</i>	Specifies the debugger type; see the <a href="#">Usage Guidelines</a> section for valid values.
---------------------------	---------------	---

**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 SB 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 SB, 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 -347](#) 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*

<b>access-lists 300</b>	Debugs the ACL.
<b>dump</b>	Dumps the ACL contents.
<b>query</b>	Queries the ACL configuration.
<b>username</b> <i>username</i>	Queries the ACL username.
<b>groupname</b> <i>groupnames</i>	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.
<b>all</b>	Enables all debugging.

Table 2-2 *debug Command Options*

<b>authentication</b>	Debugs authentication.
<b>user</b>	Debugs the user login against the system authentication.
<b>cli</b>	Debugs the CLI command.
<b>all</b>	Debugs all CLI commands.
<b>bin</b>	Debugs the CLI command binary program.
pam	Debugs the CLI command pam.
<b>parser</b>	Debugs the CLI command parser.
<b>cms</b>	Debugs the CMS.
<b>dataserver</b>	Debugs the data server.
<b>all</b>	Debugs all data server functions.
<b>clientlib</b>	Debugs the data server client library module.
<b>server</b>	Debugs the data server module.
<b>dhcp</b>	Debugs the DHCP.
<b>emdb</b>	Embedded database debug commands.
<b>logging</b>	Debugs logging.
<b>all</b>	Debugs all logging functions.
<b>malloc</b>	Debug commands for memory allocation.
<b>cache-app</b>	Debugging commands for cache application memory allocation.
<b>all</b>	Sets the debug level to all.
<b>caller-accounting</b>	Collects statistics for every distinct allocation call-stack.
<b>catch-double-free</b>	Alerts if application attempts to release the same memory twice.
<b>check-boundaries</b>	Checks boundary over and under run scribble.
<b>check-free-chunks</b>	Checks if free chunks are over-written after release.
<b>clear-on-alloc</b>	Ensures all allocations are zero-cleared.
<b>statistics</b>	Allocator use statistical summary.
<b>dns-server</b>	DNS Caching Service memory allocation debugging.
<b>all</b>	Sets the debug level to all.
<b>caller-accounting</b>	Collects statistics for every distinct allocation call-stack.
<b>catch-double-free</b>	Alerts if application attempts to release the same memory twice.
<b>check-boundaries</b>	Checks boundary over and under run scribble.
<b>log-directory</b>	Memory allocation debugging log directory.
<b>word</b>	Directory path name.
<b>ntp</b>	Debugs NTP.
<b>rpc</b>	Displays the remote procedure call (RPC) logs.
<b>detail</b>	Displays the RPC logs of priority <i>detail</i> level or higher.
<b>trace</b>	Displays the RPC logs of priority <i>trace</i> level or higher.

Table 2-2 *debug Command Options*

<b>service-broker</b>	Debug commands for the Service Broker.
<b>service-monitor</b>	Debug commands for the Service Monitor.
<b>snmp</b>	Debugs SNMP.
<b>agent</b>	SNMP agent debug.
<b>all</b>	Debugs all SNMP functions.
<b>cli</b>	Debugs the SNMP CLI.
<b>main</b>	Debugs the SNMP main.
<b>mib</b>	Debugs the SNMP MIB.
<b>traps</b>	Debugs the SNMP traps.
<b>standby</b>	Debugs standby functions.
<b>all</b>	(Optional) Debugs all standby functions.
<b>stats</b>	Debugs the statistics.
<b>all</b>	Debugs all statistics functions.
<b>collection</b>	Debugs the statistics collection.
<b>computation</b>	Debugs the statistics computation.
<b>history</b>	Debugs the statistics history.
<b>translog</b>	Debugs the transaction logging.
<b>all</b>	Debugs all transaction logging.
<b>archive</b>	Debugs the transaction log archive.
<b>export</b>	Debugs the transaction log FTP export.

### 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 SB 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.

### Related Commands

Command	Description
<b>show debugging</b>	Displays the state of each debugging option.
<b>undebug</b>	Disables the debugging functions (see also <b>debug</b> ).

# delfile

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

**delfile** *filename*

<b>Syntax Description</b>	<i>filename</i>	Name of the file to delete.
---------------------------	-----------------	-----------------------------

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	EXEC configuration mode.
----------------------	--------------------------

<b>Usage Guidelines</b>	Use this command to remove a file from a sysfs partition.
-------------------------	---

<b>Examples</b>	The following example shows how to delete a file:
-----------------	---

```
ServiceBroker# delfile /local1/tempfile
```

Related Commands	Command	Description
	<b>cpfile</b>	Copies a file.
	<b>deltree</b>	Deletes a directory and its subdirectories.
	<b>mkdir</b>	Creates a directory.
	<b>mkfile</b>	Creates a file (for testing).
	<b>rmdir</b>	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

<i>directory</i>	Name of the directory tree to delete.
------------------	---------------------------------------

## Defaults

None

## Command Modes

EXEC configuration mode.

## Usage Guidelines

Use this command to remove a directory and all files within the directory from the SB sysfs file system. Do not remove files or directories required for proper SB functioning.

## Examples

The following example shows how to delete a directory from the /local1 directory:

```
ServiceBroker# deltree /local1/testdir
```

## Related Commands

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

# device

To configure the mode of operation on a device as a VDSM or SB, 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** { **service-broker** | **videoscope-distribution-suite-manager** }

**no device mode** { **service-broker** | **videoscope-distribution-suite-manager** }

## Syntax Description

<b>mode</b>	Sets the mode of operation of a device to VDSM, SB.
<b>service-broker</b>	Configures the device operation mode as an SB.
<b>videoscope-distribution-suite-manager</b>	Configures the device to function as a VDSM

## Defaults

The default device operation mode is SB.

## Command Modes

Global configuration (config) mode.

## Usage Guidelines

A VDSM is the content management and device management station of an VDS-SB network that allows you to specify what content is to be distributed, and where the content should be distributed. If an SB is deployed in the VDS-SB network, the SB redirects the client based on redirecting policy. An SB is the device that serves content to the clients. There are typically many SBs deployed in an VDS-SB network, each serving a local set of clients. IP/TV brings movie-quality video over enterprise networks to the desktop of the VDS-SB 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 SB to VDSM (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 SB mode. Disk configuration changes using the **disk configure** command takes effect after the next device reboot.

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

All VDS-SB devices ship from the factory as SBs. Before configuring network settings for VDSMs and SBs using the CLI, change the device from an SB 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 SBs.

To change the device mode of your SB, 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 to an SB or VDSM, you may need to reconfigure the system file system (sysfs). However, SBs and VDSMs do not require any disk space other than sysfs. When you change the device mode to an SB or a VDSM, 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 VDS-SB network device.

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

---

### Examples

The following examples show the configuration from the default mode, SB to the VDSM, modes:

```
ServiceBroker(config)# device mode virtual-origin-system-manager
```

```
VDSM(config)# device mode service-broker
```

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

---

### Related Commands

Command	Description
<b>show device-mode</b>	Displays the configured or current mode of a VDSM, or SB device.

# dir

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

**dir** [*directory*]

<b>Syntax Description</b>	<i>directory</i> (Optional) Name of the directory to list.
---------------------------	--

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	EXEC configuration mode.
----------------------	--------------------------

<b>Usage Guidelines</b>	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 <b>lls</b> .
-------------------------	--

<b>Examples</b>	The following example shows how to view a list of files in a directory:
-----------------	---

```
ServiceBroker# 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
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>lls</b>	Displays the files in a long list format.
	<b>ls</b>	Lists the files and subdirectories in a directory.

# 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.

### 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:

```
ServiceBroker# disable
ServiceBroker>
```

### Related Commands

Command	Description
<b>enable</b>	Accesses the privileged EXEC commands.

## disk (EXEC Configuration)

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

**Defaults** 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. 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 VDS-SB 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 repairs 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 SB to ensure all VDS-SB software services are functioning correctly.

**Caution**

The device should be off-line 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:

```
ServiceBroker# 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:

```
ServiceBroker# disk unuse disk00
disk00 has key CDNFS data and can not be unused!
```

```
ServiceBroker# 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.

```

```

ServiceBroker# 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:

```

ServiceBroker# 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:

```

ServiceBroker# 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:

```

ServiceBroker# 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

```

## disk (EXEC Configuration)

```

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 SB:

```

ServiceBroker# 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 SB on the VDSM GUI so the SB is no longer sending
traffic to this SB.
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
<b>disk</b> (Global configuration mode)	Configures how the disk errors should be handled.
<b>show cdnfs</b>	Displays the CDS network file system information.
<b>show disk</b>	Displays the disk configurations.
<b>show disk details</b>	Displays more detailed SMART disk monitoring information.
<b>show statistics</b>	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

<b>error-handling</b>	Configures disk error handling.
<b>bad-sectors-mon-period</b>	Active bad sectors monitoring period (minutes).
<i>minutes</i>	Default value is 1440 minutes (24 hours); 0 disables sector monitoring. The range is from 0 to 525600.
<b>reload</b>	Whether to reload system if SYSFS disk(s) have problems.
<b>threshold</b>	Configure disk error handling thresholds.
<b>alarm-bad-sectors</b>	Configures the bad sector alarm threshold.
<i>bad-sectors</i>	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.
<b>alarm-remapped-sectors</b>	Configure SMARTinfo remapped sectors alarm threshold (hard drives only).
<i>remapped-sectors</i>	Number of remapped sectors before alarm is triggered. Default value is 128 (hard drives only). The range is from 0 to 8192.
<b>bad-sectors</b>	Configure number of allowed (Active) bad sectors before disk is marked bad.
	
<b>Note</b>	Only applies to bad sectors detected since system boot.
<i>bad-sectors</i>	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.
<b>errors</b>	Configure number of allowed disk errors before marking disk bad.
	
<b>Note</b>	Only applies to disk or sector errors detected since system boot.
<i>errors</i>	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.

---

**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 SB 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 SB.

**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 SBs have only one critical disk drive. Higher-end SBs that have more than one disk drive may have more than one critical disk drive.

When an SB is booted and a critical disk drive is not detected at system startup time, the VDS-SB system on the SB 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 VDS-SB system applications can malfunction, hang, or crash, or the VDS-SB system can hang or crash. Monitor the critical disk drives on an SB 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 VDS-SB 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 SB 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 SB.

In addition to tracking the state of critical disk drives, you can define a disk device error-handling threshold on the SB. 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 SB either records this event or reboots. If the automatic reload feature is enabled and this threshold is exceeded, then the VDS-SB system automatically reboots the SB. For more information about specifying this threshold, see the [“Specifying the Disk Error-Handling Threshold” section on page 2-63](#).

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 VDS-SB software marks the disk drive as bad and the SB is automatically reloaded. After the SB 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 SB. 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:

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

## ■ disk (Global configuration)

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

# dnslookup

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

## **dnslookup** *line*

<b>Syntax Description</b>	<i>line</i> Domain name of host on the network.
---------------------------	---

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	EXEC configuration mode.
----------------------	--------------------------

<b>Usage Guidelines</b>	The <b>dnslookup</b> command accepts IP address. If an IP address is specified in the dnslookup command, the server replies to a query including the IP address and the IP address displays in the output of the and <b>tcpdump</b> and <b>netstat</b> commands and all logs.
-------------------------	---

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

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

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

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

## enable (EXEC Configuration)

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.

---

**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:

```
ServiceBroker> enable
ServiceBroker#
```

---

Related Commands	Command	Description
	<b>disable</b>	Turns off the privileged EXEC commands.
	<b>exit</b>	Exits from interface, Global configuration, or privileged EXEC configuration modes.

---

## enable (Global Configuration)

To modify enable password parameters, use the **enable password** command in Global configuration mode.

```
enable password {0 | 1 | word}
```

Syntax Description	password	Assigns a privileged-level password.
	0	Specifies an unencrypted password will follow.
	1	Specifies a hidden password will follow.
	<i>word</i>	The unencrypted (cleartext) user password.

**Defaults** None

**Command Modes** Global configuration mode.

**Examples** The following example shows how to assign a privileged-level unencrypted password:

```
ServiceBroker> enable password 0 xxxx
ServiceBroker#
```

■ end

# end

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

**end**

---

**Syntax Description** This command has no arguments or keywords.

---

**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:

```
ServiceBroker(config)# end
ServiceBroker#
```

---

Related Commands	Command	Description
	<b>exit</b>	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**

<b>Syntax Description</b>	<i>timeout</i> Timeout in minutes. The range is from 0–44640. The default is 15.						
<b>Defaults</b>	The default is 15 minutes.						
<b>Command Modes</b>	Global configuration (config) mode.						
<b>Usage Guidelines</b>	<p>A Telnet or SSH session with the SB can remain open and inactive for the interval of time specified by the <b>exec-timeout</b> command. When the exec-timeout interval elapses, the SB automatically closes the Telnet or SSH session.</p> <p>Configuring a timeout interval of 0 minutes by entering the <b>exec-timeout 0</b> command is equivalent to disabling the session-timeout feature.</p>						
<b>Examples</b>	<p>The following example shows how to configure a timeout of 100 minutes:</p> <pre>ServiceBroker(config)# <b>exec-timeout 100</b></pre> <p>The following example negates the configured timeout of 100 minutes and reverts to the default value of 15 minutes:</p> <pre>ServiceBroker(config)# <b>no exec-timeout</b></pre>						
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>ssh</b></td> <td>Configures the SSH service parameters.</td> </tr> <tr> <td><b>telnet enable</b></td> <td>Enables the Telnet services.</td> </tr> </tbody> </table>	Command	Description	<b>ssh</b>	Configures the SSH service parameters.	<b>telnet enable</b>	Enables the Telnet services.
Command	Description						
<b>ssh</b>	Configures the SSH service parameters.						
<b>telnet enable</b>	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.

---

**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:

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

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

```
ServiceBroker# exit
ServiceBroker>
```

---

Related Commands	Command	Description
	<b>end</b>	Exits configuration and privileged EXEC configuration modes.

---

# expert-mode

To configure debugshell, use the **expert-mode** command in Global configuration mode.

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

Syntax Description		
	<b>password</b>	Sets the expert mode password.
	<b>encrypted</b>	(Optional) Encrypts the password.
	<i>password</i>	The encrypted password.

**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 debugshell:

```
ServiceBroker(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*

<b>Syntax Description</b>	<i>ip_addresses</i>	A maximum of eight external or NAT IP addresses can be configured.
<b>Defaults</b>	None	
<b>Command Modes</b>	Global configuration (config) mode.	
<b>Usage Guidelines</b>	<p>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 SB, then the external IP address is configured as the IP address of the RTSP gateway.</p> <p>In an VDS-SB network, there are two methods for a device registered with the VDSM (SBs, or the standby VDSM) to obtain configuration information from the primary VDSM. The primary method is for the device to periodically poll the primary VDSM on port 443 to request a configuration update. You cannot configure this port number. The backup method is when the VDSM 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. VDS-SB networks do not work reliably if devices registered with the VDSM are unable to poll the VDSM for configuration updates. When a receiver SB requests the content and content metadata from a forwarder SB, it contacts the forwarder SB on port 443.</p> <p>When a device (SBs at the edge of the network, SBs, and primary or standby VDSMs) 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 VDSM. 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.</p> <p>If the primary VDSM 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 VDSM's inside local IP address on its NAT, and using this address, rather than the VDSM's inside local IP address in the <b>VDSM ip ip_address</b> command when you register the device to the VDSM. If an SB is inside a NAT and the VDSM is outside the NAT, you can allow the SB to poll for getUpdate requests by configuring a static translation (NAT IP address or inside global IP address) for the SB's inside local address on its NAT.</p>	

**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:

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

**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:

```
ServiceBroker# 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:

```
ServiceBroker# 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:

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

### Related Commands

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

# ftp

To enable File Transfer Protocol (FTP) services, use the **ftp** command in Global configuration mode. To cancel the request, use the **no** form of this command.

**ftp enable**

**no ftp enable**

Syntax Description	enable	Enables FTP services.
--------------------	--------	-----------------------

Defaults	None
----------	------

Command Modes	Global configuration (config) mode.
---------------	-------------------------------------

**Examples** The following example shows how to enable FTP services:

```
ServiceRouter# ftp enable
```

Related Commands	Command	Description
	<b>show ftp</b>	Displays the caching configuration of the FTP.

## geo-location-server

To monitor primary and secondary servers, use the **geo-location-server** command in EXEC configuration mode. To disable monitoring, restore default values for type, timeout and poll-rate, use the no form of this command.

```
geo-location-server { geo-pre-cache-file | monitor | poll-rate | timeout | type | primary |
secondary | pre-cache }
```

```
no geo-location-server { geo-pre-cache-file | monitor | poll-rate | timeout | primary | secondary
| pre-cache }
```

Syntax	Description
<b>geo-pre-cache-file</b>	Configures Geo Pre-Cache config file.
<b>monitor</b>	Enables or Disables Geolocation Server monitoring.
<b>poll-rate</b>	Configures Geolocation Server polling interval.
<b>timeout</b>	Configures Geolocation Server timeout.
<b>type</b>	Configures Geolocation Server type.
<b>primary</b>	Configures Primary Geolocation server ip address and port.
<b>secondary</b>	Configures Secondary Geolocation server ip address and port.
<b>pre-cache</b>	Configures Geo Pre-Cache settings.

### Defaults

Monitor: enabled

Poll-rate: 60 seconds

Timeout: 1 second

Type: neustar-lib

### Command Modes

EXEC configuration mode.

### Examples

The following example shows how to enable geo-location-server monitor for the SB:

```
ServiceBroker# geo-location-server monitor
ServiceBroker# show geo-location-server
Geo Location server monitoring is enabled
Geo Location server poll rate 60 seconds
Geo Location server timeout 1 seconds
Geo pre-cache size is 500
Geo Location server type neustar-lib
```

The following example shows how to disable geo-location-server monitor for the SB:

```
ServiceBroker# no geo-location-server monitor
ServiceBroker# show geo-location-server
Geo Location server monitoring is disabled
Geo Location server poll rate 60 seconds
Geo Location server timeout 1 seconds
Geo pre-cache size is 500
Geo Location server type neustar-lib
```

# gulp

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

**gulp** *line*

<b>Syntax Description</b>	<i>line</i> (Optional) Specifies gulp options, enter <b>-h</b> to get help.
---------------------------	---

<b>Task ID</b>	None
----------------	------

<b>Command Modes</b>	EXEC configuration mode.
----------------------	--------------------------

<b>Usage Guidelines</b>	The <b>gulp</b> utility captures lossless gigabit packets and writes them to disk, as well as captures packets remotely. The <b>gulp</b> utility has the ability to read directly from the network.
-------------------------	---

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

```
ServiceBroker# 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 2-3](#) lists the gulp options and provides a description of each.

Table 2-3 *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 <b>gulp</b> utility and then filtering them out.
-i <i>eth#</i>	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 <b>gulp</b> utility running. If other instances are already running, they must be stopped before the <b>gulp</b> utility can start with this option.
-X	Override an exclusive lock (-x option) and run anyway. An instance of <b>gulp</b> 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 2-3 *gulp Options (continued)*

Option	Description
-o <i>dir</i>	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 <b>gulp</b> 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 <b>gulp</b> 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:

```
ServiceBroker# 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:

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

**Related Commands**

Command	Description
<b>netmon</b>	Displays the transmit and receive activity on an interface.
<b>netstatr</b>	Displays the rate of change of netstat statistics.
<b>ss</b>	Dumps socket statistics.
<b>tcpmon</b>	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.

---

**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:

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

Defaults	The default hostname is the SB model number.
----------	--

Command Modes	Global configuration (config) mode.
---------------	-------------------------------------

Usage Guidelines	Use this command to configure the hostname for the SB. 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:
----------	--

```
ServiceBroker(config)# hostname Sandbox
Sandbox(config)#
```

The following example removes the hostname:

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

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

# http

To configure HTTP-related parameters, use the **http** command in EXEC configuration mode.

## **http asx-302-redirect enable**

Syntax	Description
<b>asx-302-redirect</b>	Configures 302 response for asx requests.
<b>enable</b>	Enables 302 redirection for asx requests.

**Defaults** None

**Command Modes** EXEC configuration mode.

**Examples** The following example shows how to install a .bin file on the SB:

```
ServiceBroker# install VDS-SB-2.2.1.7-K9.bin
```

# install

To install the VDS-SB software image, use the **install** command in EXEC configuration mode.

```
install imagefile_name
```

<b>Syntax Description</b>	<i>imagefile_name</i>	Name of the .bin file that you want to install.
---------------------------	-----------------------	---

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	EXEC configuration mode.
----------------------	--------------------------

<b>Usage Guidelines</b>	<p>The <b>install</b> command loads the system image into flash memory and the disk.</p> <p>To install a system image, copy the image file to the sysfs directory local1 or local2. Before entering the <b>install</b> command, change the present working directory to the directory where the system image resides. When the <b>install</b> command is executed, the image file is expanded. The expanded files overwrite the existing files in the SB. The newly installed version takes effect after the system image is reloaded.</p>
-------------------------	--



### Note

The **install** command does not accept .pax files. Files should be of the .bin type (for example, VDS-SB-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.

<b>Examples</b>	The following example shows how to install a .bin file on the SB:
-----------------	---

```
ServiceBroker# install VDS-SB-2.2.1.7-K9.bin
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>copy ftp install</b>	Installs an image file from an FTP server onto a local device.
	<b>copy http install</b>	Installs an image file from an HTTP server onto a local device.
	<b>reload</b>	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
{ 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 }
```

```
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
{ 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 }
```

## Syntax Description

<b>GigabitEthernet</b>	Selects a Gigabit Ethernet interface to configure.
<i>slot/port_num</i>	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 (/).
<b>autosense</b>	(Optional) Specifies interface autosense.
<b>bandwidth</b>	(Optional) Configures the interface bandwidth.
<b>10</b>	Specifies the interface bandwidth as 10 Mbits per second.
<b>100</b>	Specifies the interface bandwidth as 100 Mbits per second.

<b>1000</b>	Specifies the interface bandwidth as 1000 Mbits per second.
<b>channel-group</b>	(Optional) Configures the EtherChannel group.
<i>group_interface</i>	EtherChannel group to which the interface belongs. The range is 1 to 4.
<b>description</b>	(Optional) Specifies interface specific description.
<i>line</i>	Text describing this interface
<b>full-duplex</b>	(Optional) Specifies full-duplex.
<b>half-duplex</b>	(Optional) Specifies half-duplex.
<b>ip</b>	(Optional) Interface Internet Protocol configuration commands.
<b>access-group</b>	Specifies access control for packets.
<i>access_list_num</i>	IP access list (standard or extended).
<b>in</b>	Specifies inbound packets.
<b>out</b>	Specifies outbound packets.
<i>name</i>	Specifies the access-list name.
<b>address</b>	Sets the IP address of the interface.
<i>ip_address</i>	IP address of the interface
<i>netmask</i>	Netmask of the interface.
<i>range</i>	IP address range.
<i>low_num</i>	IP address low range of the interface.
<i>high_num</i>	IP address low range of the interface.
<i>netmask</i>	Netmask of the interface.
<b>access-group</b>	Specifies access control for packets.
<i>ip_access_list</i>	IP access list (standard or extended).
<b>in</b>	Inbound packets.
<b>out</b>	Outbound packets.
<i>access-list-name</i>	Specifies an access list name.
<i>prefix</i>	Interface prefix. The range is from 1 to 128.
<b>mtu</b>	Sets the interface Maximum Transmission Unit (MTU).
<i>mtu_size</i>	MTU size in bytes. The range is 576 to 9216.
<b>shutdown</b>	(Optional) Shuts down the specific portchannel interface.
<b>standby</b>	(Optional) Standby interface configuration commands.
<i>interface_group_num</i>	Group number for the selected interface. The range is from 1 to 4.
<b>priority</b>	Sets the priority of the interface. Default value is 100.
<i>standby_group_priority</i>	Set the priority of the interface for the standby group. The range is from 0 to 4294967295.
<b>tx-queue-limit</b>	Sets the interface maximum Transmission Queue Length.
<i>queue_length</i>	Sets the limit on the transmission queue length. The range is from 1000 to 80000.
<b>PortChannel</b>	Selects the Ethernet Channel of interfaces to be configured.
<i>num</i>	Sets the Ethernet Channel interface number. The range is from 1 to 4.
<b>lACP</b>	Specifies Link Aggregation Control Protocol.
<b>Standby</b>	Specifies a standby group number.
<i>standby_group_num</i>	Standby group number. The range is from 1 to 4.

<b>description</b>	(Optional) Standby interface description.
<i>line</i>	Text describing this interface.
<b>errors</b>	Sets the maximum number of errors allowed on this interface.
<i>error_num</i>	Maximum number of errors allowed on this interface for the standby group. The range is from 1 to 2147483647.
<b>ip</b>	Sets the IP address of the standby group.
<b>address</b>	Sets the IP address of the interface.
<i>standby_group_ip_addr</i>	IP address of the standby group.
<i>standby_group_netmask</i>	Netmask of the standby group.
<b>range</b>	Sets the IP address range of the standby group.
<i>low_range</i>	IP address low range of an interface.
<i>high_range</i>	IP address high range of an interface.
<i>interface_netmask</i>	Netmask of the interface.
<b>TenGigabitEthernet</b>	Selects a ten Gigabit Ethernet interface to configure.

**Defaults**

Standby priority: 100.

**Command Modes**

Global configuration (config) mode.

**Usage Guidelines**

**Note** The Gigabit Ethernet interfaces are shared between CIMC and UCS for UCS devices (specifically UCS220). The default values for duplex, speed, auto negotiation and advertising *cannot* be changed.

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

EtherChannel for Cisco VDS Service Broker 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 SB 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.

**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:

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

The following example shows how to remove an EtherChannel:

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

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

```
ServiceBroker# 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:

```
ServiceBroker# 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 SBs:

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

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

```
ServiceBroker(config)# interface PortChannel 2
ServiceBroker(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:

```
ServiceBroker# 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
<b>show interface</b>	Displays the hardware interface information.
<b>show running-config</b>	Displays the current operating configuration.
<b>show startup-config</b>	Displays the startup configuration.

# iostat

To Show CPU and I/O statistics for devices and partitions, use the **iostat** command in EXEC configuration mode.

**iostat** [*line*]

Syntax Description	<i>line</i>	Specifies iostat options.
--------------------	-------------	---------------------------

Defaults	None
----------	------

Command Modes	EXEC configuration mode.
---------------	--------------------------

Examples	The following example shows how to display CPU statistics:
----------	--

```
ServiceBroker# iostat
Linux 2.6.32.52-cds-64 (W14-UCS220-2) 10/16/12 _x86_64_ (32 CPU)

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
           0.00    0.03   0.03   0.00   0.00   99.93

Device:            tps    kB_read/s    kB_wrtn/s    kB_read    kB_wrtn
sdc                 1.79         7.24         30.89     580715     2478770
sdd                 0.00         0.05          0.03         4143         2057

ServiceBroker#
```

## 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 99) | **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
<b>access-list</b>	Specifies the access list.
<b>default-gateway</b>	Specifies the default gateway (if not routing IP).
<i>ip_address</i>	IP address of the default gateway.
<i>gateway_ip_addr</i>	(Optional) Gateway IP address (maximum of 14).
<b>domain-name</b>	Specifies domain names.
<i>name1</i> through <i>name3</i>	Domain name (up to three can be specified).
<b>name-server</b>	Specifies the address of the name server.
<i>ip_addresses</i>	IP addresses of the domain server (up to a maximum of eight).
<b>path-mtu-discovery</b>	Configures RFC 1191 Path Maximum Transmission Unit (MTU) discovery.
<b>enable</b>	Enables Path MTU discovery.
<b>route</b>	Specifies the net route.
<i>dest_IP_addr</i>	Destination route address.
<i>dest_netmask</i>	Netmask address.
<i>default_gateway</i>	Gateway address.
<b>interface</b>	Configures source policy routing to route outgoing traffic using the same interface where the request was received.
<i>source_IP_addr</i>	IP address of the interface configured for source policy routing.

**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 SB 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 SB 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 SB 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 SB uses DNS servers. Use the **ip name-server** command to point the SB 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 VDS Service Broker 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 SB 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>**

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 the software with the default source policy routes highlighted in bold and the non-default policy routes highlighted in italics:

```
ServiceBroker# 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 the 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 the 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 VDS-SB 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:

$$dP(AFny) \geq dP(AFnz) \geq dP(AFnx)$$

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:

$$dP(AF13) \geq dP(AF12) \geq dP(AF11)$$

The  $dP$  method penalizes traffic flows within a particular BA that exceed the assigned bandwidth. Packets on these offending flows could be re-marked by a policer to a higher drop precedence.

### 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 VDS-SB 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 SB:

```
ServiceBroker(config)# ip default-gateway 192.168.7.18
```

The following example disables the default gateway:

```
ServiceBroker(config)# no ip default-gateway
```

The following example shows how to configure a static IP route for the SB:

```
ServiceBroker(config)# ip route 172.16.227.128 255.255.255.0 172.16.227.250
```

The following example negates the static IP route:

```
ServiceBroker(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 SB:

```
ServiceBroker(config)# ip domain-name cisco.com
```

The following example negates the default domain name:

```
ServiceBroker(config)# no ip domain-name
```

The following example shows how to configure a name server for the SB:

```
ServiceBroker(config)# ip name-server 10.11.12.13
```

The following example disables the name server:

```
ServiceBroker(config)# no ip name-server 10.11.12.13
```

The following example shows how to configure source policy routing for the SB interface assigned with the IP address 192.168.1.5:

```
ServiceBroker(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.1 interface 192.168.1.5
```

### Related Commands

Command	Description
<b>ip</b> (Interface configuration)	Configures the interface Internet Protocol.
<b>show ip routes</b>	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		
<b>access-group</b>		Specifies access control for incoming or outgoing packets.
<i>num</i>		Specifies an IP access list by number, in standard or extended form. The range is from 1-199.
<b>in</b>		Configures the IP access list that apply to inbound packets.
<b>out</b>		Configures the IP access list that apply to outbound packets.
<i>name</i>		Name of the access list.
<b>in</b>		Configures the access list name inbound packets.
<b>out</b>		Configures the access list name outbound packets.
<b>address</b>		Set the IP address of an interface.
<i>ip_addr</i>		IP address of the interface.
<i>netmask</i>		Netmask of the interface.
<b>range</b>		Specifies the IP address range.
<i>ip_addr_low</i>		IP address low range of an interface.
<i>ip_addr_high</i>		IP address high range of an interface.
<i>netmask</i>		Netmask of the interface.

**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 SBs. With multiple IP support, the SBs 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 SB and VDSM 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:

```
ServiceBroker(config)# interface PortChannel 1
ServiceBroker(config-if)# ip address 2.2.2.2 255.255.255.0
ServiceBroker(config-if)# ip address range 2.2.2.3 2.2.2.10 255.255.255.0
ServiceBroker(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:

```
ServiceBroker# configure terminal
ServiceBroker(config)# interface PortChannel 1
ServiceBroker(config-if)# ip address range 2.2.2.3 2.2.2.4 255.255.255.0
ServiceBroker(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:

```
ServiceBroker# configure terminal
ServiceBroker(config)# interface PortChannel 1
ServiceBroker(config-if)# ip address range 2.2.3.9 2.2.3.15 255.255.255.0
ServiceBroker(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:

```
ServiceBroker(config)# interface PortChannel 1
ServiceBroker(config-if)# ip address 2.2.2.2 255.255.255.0
ServiceBroker(config-if)# ip address 2.2.2.3 255.255.255.0
ServiceBroker(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:

```
ServiceBroker(config)# interface PortChannel 1
```

## ip (Interface configuration)

```
ServiceBroker(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:

```
ServiceBroker(config)# interface PortChannel 1
ServiceBroker(config-if)# no ip address 2.2.2.3 255.255.255.
```

### Related Commands

Command	Description
<b>interface</b> (Global configuration)	Configures a Gigabit Ethernet or port channel interface.
<b>show interface</b>	Displays the hardware interface information.
<b>show running-config</b>	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_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 } } } | 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 { 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_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 } } } | 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 { 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

<b>standard</b>	Enables the standard ACL configuration mode.
<i>acl_num</i>	Access list to which all commands entered from access list configuration mode apply, using a numeric identifier. For standard access lists, the valid range is 1 to 99; for extended access lists, the valid range is 100 to 199.
<i>acl_name</i>	Access list to which all commands entered from ACL configuration mode apply, using an alphanumeric string of up to 30 characters, beginning with a letter.
<b>delete</b>	(Optional) Deletes the specified entry.
<i>num</i>	(Optional) Position of condition to delete. The range is from 1 to 500.
<b>deny</b>	(Optional) Causes packets that match the specified conditions to be dropped.

<i>num</i>	IP Protocol Number.
<i>ip address</i>	Source IP address.
<i>any</i>	Any source host.
<i>host</i>	A single host address.
<b>gre</b>	Specifies GRE Tunneling by Cisco.
<b>icmp</b>	Specifies Internet Control Message Protocol.
<b>ip</b>	Specifies Any IP Protocol.
<b>tcp</b>	Specifies Transport Control Protocol.
<b>udp</b>	Specifies User Datagram Protocol.
<b>insert</b>	(Optional) Inserts the conditions following the specified line number into the access list.
<i>num</i>	Identifies the position at which to insert a new condition.
<b>deny</b>	Specifies packets to deny.
<b>permit</b>	Specifies packets to permit.
<b>list</b>	(Optional) Lists the specified entries (or all entries when none are specified).
<i>start_line_num</i>	(Optional) Line number from which the list begins.
<i>end_line_num</i>	(Optional) Last line number in the list.
<b>move</b>	(Optional) Moves the specified entry in the access list to a new position in the list.
<i>old_line_num</i>	Line number of the entry to move.
<i>new_line_num</i>	New position of the entry. The existing entry is moved to the following position in the access list.
<b>permit</b>	(Optional) Causes packets that match the specified conditions to be accepted for further processing.
<b>extended</b>	Enables the extended ACL configuration mode.

**Defaults**

An access list drops all packets unless you configure at least one **permit** entry.

**Command Modes**

Global configuration (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 2-6](#). For a list of supported UDP and TCP keywords, see [Table 2-4](#) and [Table 2-5](#).

Use access lists to control access to specific applications or interfaces on an SB. An ACL consists of one or more condition entries that specify the kind of packets that the SB drops or accepts for further processing. The SB 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 SBs:

- SB 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.
- SB 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 SB'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 SB.
- SB is deployed as a reverse proxy in an untrusted environment. The SB 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 SB 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 2-4](#) lists the UDP keywords that you can use with extended access lists.

*Table 2-4 UDP Keywords and Port Numbers*

CLI Keyword	Description	UDP Port Number
<b>bootpc</b>	BOOTP <sup>1</sup> client service	68
<b>bootps</b>	BOOTP server service	67
<b>domain</b>	DNS <sup>2</sup> service	53
<b>netbios-dgm</b>	NetBIOS datagram service	138
<b>netbios-ns</b>	NetBIOS name resolution service	137
<b>netbios-ss</b>	NetBIOS session service	139
<b>nfs</b>	Network File System service	2049
<b>ntp</b>	Network Time Protocol settings	123
<b>snmp</b>	Simple Network Management Protocol service	161
<b>snmptrap</b>	SNMP traps	162
<b>tftp</b>	Trivial File Transfer Protocol service	69

1. BOOTP = bootstrap protocol

2. DNS = Domain Name System

Table 2-5 lists the TCP keywords that you can use with extended access lists.

**Table 2-5** TCP Keywords and Port Numbers

CLI Keyword	Description	TCP Port Number
<b>domain</b>	Domain Name System	53
<b>exec</b>	Remote process execution	512
<b>ftp</b>	File Transfer Protocol service	21
<b>ftp-data</b>	FTP data connections (used infrequently)	20
<b>nfs</b>	Network File System service applications	2049
<b>rtsp</b>	Real-Time Streaming Protocol applications	554
<b>ssh</b>	Secure Shell login	22
<b>telnet</b>	Remote login using telnet	23
<b>www</b>	World Wide Web (HTTP) service	80

Table 2-6 lists the keywords that you can use to match specific ICMP message types and codes.

**Table 2-6** 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 <sup>1</sup> 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.

Table 2-6 Keywords for ICMP Message Type and Code (continued)

Field	Description
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.
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 <sup>2</sup> 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 <i>router advertisements</i> .
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.

Table 2-6 Keywords for ICMP Message Type and Code (continued)

Field	Description
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.
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):

```
ServiceBroker(config)# ip access-list extended example
ServiceBroker(config-ext-nacl)# permit tcp any any eq www
ServiceBroker(config-ext-nacl)# permit tcp host 10.1.1.5 any eq ssh
ServiceBroker(config-ext-nacl)# exit
```

The following example shows how to activate the access list for an interface:

```
ServiceBroker(config)# interface gigabitethernet 1/0
ServiceBroker(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
<b>clear ip access-list counters</b>	Clears the IP access list statistical information.
<b>show ip access-list</b>	Displays the access lists that are defined and applied to specific interfaces or applications.

# 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	Field	Description
	<b>kdb</b>	Specifies the kernel debugger (kdb).
	<b>optimization</b>	Enables kernel performance optimization.
	<b>network</b>	Optimizes network performance.

**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 VDS-SB 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:

```
ServiceBroker(config)# kernel kdb
```

The following example shows how to disable KDB:

```
ServiceBroker(config)# no kernel kdb
```

# 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.
	<b>carrier-detect</b>	Sets the device to check the carrier detect signal before writing to the console.

**Defaults** This feature is disabled by default.

**Command Modes** Global configuration (config) mode.

**Usage Guidelines** You should enable carrier detection if you connect the SB, or VDSM 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:

```
ServiceBroker(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*]

<b>Syntax Description</b>	<i>directory</i> (Optional) Name of the directory for which you want a long list of files.
---------------------------	--

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	User EXEC configuration mode.
----------------------	-------------------------------

<b>Usage Guidelines</b>	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 <b>dir</b> command.
-------------------------	---

<b>Examples</b>	The following example shows how to view a long list of directory names:
-----------------	---

```
ServiceBroker# 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
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>dir</b>	Displays a detailed list of files contained within the working directory, including names, sizes, and time created.
	<b>ls</b>	Lists the files or subdirectory names within a directory.

# 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
<b>console</b>	Sets system logging to a console.
<b>enable</b>	Enables system logging to a console.
<b>priority</b>	Sets which priority level messages to send to a syslog file.
<i>loglevel</i>	
<b>alert</b>	Immediate action needed. Priority 1.
<b>critical</b>	Immediate action needed. Priority 2.
<b>debug</b>	Debugging messages. Priority 7.
<b>emergency</b>	System is unusable. Priority 0.
<b>error</b>	Error conditions. Priority 3.
<b>information</b>	Informational messages. Priority 6.
<b>notice</b>	Normal but significant conditions. Priority 5.
<b>warning</b>	Warning conditions. Priority 4.
<b>disk</b>	Sets system logging to a disk file.
<b>enable</b>	Enables system logging to a disk file.
<b>filename</b>	Sets the name of the syslog file.
<i>filename</i>	Specifies the name of the syslog file.
<b>recycle</b>	Overwrites the <i>syslog.txt</i> when it surpasses the recycle size.
<i>size</i>	Size of the syslog file in bytes (100000000 to 500000000).
<b>facility</b>	Sets the facility parameter for syslog messages.
<i>facility</i>	
<b>auth</b>	Authorization system.
<b>daemon</b>	System daemons.
<b>kernel</b>	Kernel.
<b>local0</b>	Local use.
<b>local1</b>	Local use.
<b>local2</b>	Local use.
<b>local3</b>	Local use.
<b>local4</b>	Local use.
<b>local5</b>	Local use.
<b>local6</b>	Local use.

<b>local7</b>	Local use.
<b>mail</b>	Mail system.
<b>news</b>	USENET news.
<b>syslog</b>	Syslog itself.
<b>user</b>	User process.
<b>uucp</b>	UUCP system.
<b>host</b>	Sets the system logging to a remote host.
<i>hostname</i>	Hostname of the remote syslog host. Specifies up to four remote syslog hosts. <b>Note</b> To specify more than one syslog host, use multiple command lines; specify one host per command.
<i>ip_address</i>	IP address of the remote syslog host. Specifies up to four remote syslog hosts. <b>Note</b> To specify more than one syslog host, use multiple command lines; specify one host per command.
<b>port</b>	(Optional) Specifies the port to be used when logging to a host.
<i>port_num</i>	Port to be used when logging to a host. The default port is 514.
<b>priority</b>	(Optional) Sets the priority level for messages when logging messages to a host. The default priority is warning.
<i>loglevel</i>	
<b>alert</b>	Immediate action needed. Priority 1.
<b>critical</b>	Immediate action needed. Priority 2.
<b>debug</b>	Debugging messages. Priority 7.
<b>emergency</b>	System is unusable. Priority 0.
<b>error</b>	Error conditions. Priority 3.
<b>information</b>	Informational messages. Priority 6.
<b>notice</b>	Normal but significant conditions. Priority 5.
<b>warning</b>	Warning conditions. Priority 4.
<b>rate-limit</b>	(Optional) Sets the rate limit (in messages per second) for sending messages to a host.
<i>message_rate</i>	Rate limit (in messages per second) for sending messages to the host. (0 to 10000). Setting the rate limit to 0 disables rate limiting.

**Defaults**

Logging: on  
Priority of message for console: warning  
Priority of message for log file: debug  
Priority of message for a host: warning  
Log file: /local1/syslog.txt  
Log file recycle size: 10,000,000

**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 SB. The system log file is located on the sysfs partition as /local1/syslog.txt. This file contains the output from many of the VDS-SB components running on the SB, 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 VDS-SB network, you can use the system message log feature. When a problem occurs in the VDS-SB network, use the system message logs to diagnose and correct such problems.

The syslog.txt file on the VDSM contains information about events that have occurred on the VDSM 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 VDSM because the problem never occurred on the VDSM 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 SB 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 SB:

```
ServiceBroker(config)# logging host hostname
ServiceBroker(config)# logging priority priority
```

You can configure an SB 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:

```
ServiceBroker(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 SB 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 SB 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 SB is configured to send messages that have a priority code of “error” (level 3) to the console:

```
ServiceBroker(config)# logging console priority warnings
```

The following example shows that the SB is configured to disable sending of messages that have a priority code of “error” (level 3) to the console:

```
ServiceBroker(config)# no logging console warnings
```

The following example shows that the SB 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:

```
ServiceBroker(config)# logging host 172.31.2.160 priority error
```

### Related Commands

Command	Description
<b>clear logging</b>	Removes all current entries from the syslog.txt file, but does not make an archive of the file.
<b>debug</b>	Monitors and records caching application functions.
<b>show logging</b>	Displays the system message log confirmation.

# ls

To view a list of files or subdirectory names within a directory, use the **ls** command in EXEC configuration mode.

**ls** [*directory*]

<b>Syntax Description</b>	<i>directory</i> (Optional) Name of the directory for which you want a list of files.
---------------------------	---

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	EXEC configuration mode.
----------------------	--------------------------

<b>Usage Guidelines</b>	To list the filenames and subdirectories within a particular directory, use the <b>ls <i>directory</i></b> command; to list the filenames and subdirectories of the current working directory, use the <b>ls</b> command. To view the present working directory, use the <b>pwd</b> command.
-------------------------	--

<b>Examples</b>	The following example shows how to display a list of files within the current working directory:
-----------------	--

```
ServiceBroker# ls
/local1
```

The following example shows how to display a list of files within the /local1 directory:

```
ServiceBroker# ls /local1
core_dir
crash
errorlog
logs
lost+found
service_logs
smartfilter
syslog.txt
```

Related Commands	Command	Description
	<b>dir</b>	Displays a detailed list of files contained within the working directory, including names, sizes, and time created.
	<b>lls</b>	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.
	<b>pwd</b>	Displays the present working directory of the SB.

# mkdir

To create a directory, use the **mkdir** command in EXEC configuration mode.

**mkdir** *directory*

<b>Syntax Description</b>	<i>directory</i>	Name of the directory to create.
---------------------------	------------------	----------------------------------

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	EXEC configuration mode.
----------------------	--------------------------

<b>Usage Guidelines</b>	Use this command to create a new directory or subdirectory in the SB file system.
-------------------------	---

<b>Examples</b>	The following example shows how to create a new directory under local1:
-----------------	---

```
ServiceBroker# mkdir /local1/mydir
```

Related Commands	Command	Description
	<b>dir</b>	Displays a detailed list of files contained within the working directory, including names, sizes, and time created.
	<b>lls</b>	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.
	<b>ls</b>	Lists the files or subdirectory names within a directory.
	<b>pwd</b>	Displays the present working directory of the SB.
	<b>rmdir</b>	Removes a directory from the SB file system.

# mkfile

To create a new file, use the **mkfile** command in EXEC configuration mode.

**mkfile** *filename*

<b>Syntax Description</b>	<i>filename</i>	Name of the file that you want to create.
---------------------------	-----------------	---

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	EXEC configuration mode.
----------------------	--------------------------

<b>Usage Guidelines</b>	Use this command to create a new file in any directory of the SB.
-------------------------	---

<b>Examples</b>	The following example shows how to create a new file:
-----------------	---

```
ServiceBroker# mkfile traceinfo
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>lls</b>	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.
	<b>ls</b>	Lists the files or subdirectory names within a directory.
	<b>mkdir</b>	Creates a new directory or subdirectory in the SB 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		
	<b>cde250-2S10</b>	Configures this platform as CDE250-2S10.
	<b>cde250-2S6</b>	Configures this platform as CDE250-2S6.
	<b>cde250-2S8</b>	Configures this platform as CDE250-2S8.
	<b>cde250-2S9</b>	Configures this platform as CDE250-2S9.

**Defaults** None

**Command Modes** EXEC configuration mode.

**Usage Guidelines** Use the **model** command to change the CDE250 model type. [Table 0-1](#) shows the internal and external drives for the CDE250 models.

*Table 0-1 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:

```
ServiceBroker# model CDE250-2S6
```

```
This platform is already a CDE250-2S6.
```

```
ServiceBroker#
```

# mount-option

To configure the mount option profile for remote storage, use the **mount-option** command in Global configuration mode. To delete the configuration, use the **no** form of this command.

**mount-option config-url** *url* [**username** *username* **password** *password*]

**no mount-option config-url** *url* [**username** *username* **password** *password*]

Syntax Description	config-url	Specifies the URL for the mount option configuration file.
	<i>url</i>	URL format [ftp http]://domain/path/config.xml.
	<b>username</b>	Configures the username to access the configuration file.
	<i>username</i>	Username.
	<b>password</b>	Configures the password to access the configuration file.
	<i>password</i>	Password.

**Command Default** None

**Command Modes** Global configuration (config) mode.

**Examples** The following example shows how configure the mount option:

```
ServiceBroker(config)# mount-option config-url ftp://domain/path/config.xml
```

Related Commands	Command	Description
	<b>show mount-option</b>	Displays the mount options.

# mpstat

To display processor-related statistics, use the **mpstat** command in EXEC configuration mode.

**mpstat** *line*

<b>Syntax Description</b>	<i>line</i> mpstat options, -h to get help.
---------------------------	---

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	EXEC configuration mode.
----------------------	--------------------------

<b>Examples</b>	The following example shows how to display the mpstat list of options:
-----------------	--

```
ServiceBroker# mpstat -h
Linux 2.6.32.52-cds-64 (W14-UCS220-3) 10/17/12 _x86_64_ (8 CPU)

01:50:50 CPU %usr %nice %sys %iowait %irq %soft %steal %guest %idle
01:50:50 all 0.01 0.11 0.12 0.02 0.00 0.00 0.00 0.00 99.74

ServiceBroker#
```

# netmon

To display the transmit and receive activity on an interface, use the **netmon** command in EXEC configuration mode.

**netmon** *line*

<b>Syntax Description</b>	<i>line</i> netmon options, -h to get help.
---------------------------	---

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	EXEC configuration mode.
----------------------	--------------------------

<b>Usage Guidelines</b>	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).
-------------------------	--

<b>Examples</b>	The following example shows how to display the netmon list of options:
-----------------	--

```
ServiceBroker# netmon -h
Usage: netmon [<loop-time-in-seconds>] [<iterations>]
        (runs forever if iterations not specified)
```

Related Commands	Command	Description
	<b>gulp</b>	Captures lossless gigabit packets and writes them to disk.
	<b>netstatr</b>	Displays the rate of change of netstat statistics.
	<b>ss</b>	Dumps socket statistics.
	<b>tcpmon</b>	Searches all TCP connections.

# netstatr

To display the rate of change of netstat statistics, use the **netstatr** command in EXEC configuration mode.

**netstatr** *line*

<b>Syntax Description</b>	<i>line</i> netmon options, -h to get help.
---------------------------	---

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	EXEC configuration mode.
----------------------	--------------------------

<b>Usage Guidelines</b>	The <b>netstatr</b> 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 <b>netstatr -h</b> .
-------------------------	---

<b>Examples</b>	The following example shows how to display the netstart list of options:
-----------------	--

```
ServiceBroker# 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
	<b>gulp</b>	Captures lossless gigabit packets and writes them to disk.
	<b>netmon</b>	Displays the transmit and receive activity on an interface.
	<b>ss</b>	Dumps socket statistics.
	<b>tcpmon</b>	Searches all TCP connections.

## 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 VDS-SB device (including the **no** form of each command) vary based on whether the device is configured as a VDSM, or SB. See [Table 2-1](#) to identify the commands available for a specific device.

### Syntax Description

<i>command</i>	Specifies the command type; see the <a href="#">Usage Guidelines</a> section for valid values.
----------------	--

### Defaults

None

### Command Modes

Global configuration (config) mode.

### Usage Guidelines

Valid values for *command* are as follows:

<b>aaa</b>	Configures accounting, authentication and authorization methods.
<b>alarm</b>	Configures the alarms
<b>asset</b>	Configures the asset tag name string.
<b>banner</b>	Defines a login banner.
<b>clock</b>	Configures the time-of-day clock.
<b>cms</b>	Configures the CMS <sup>1</sup> .
<b>device</b>	Configures the device mode.
<b>direct-server-return</b>	Configure direct-server-return.
<b>disk</b>	Configures disk-related settings.
<b>enable</b>	Modify enable password parameters.
<b>exec-timeout</b>	Configures the EXEC timeout.
<b>expert-mode</b>	Configures debugshell.
<b>external-ip</b>	Configures up to eight external (NAT) IP addresses.
<b>ftp</b>	Configures FTP caching-related parameters.
<b>geo-location-server</b>	Configure geo location server ip address and port.
<b>geo-location-service</b>	Configure geo location service parameters.
<b>hostname</b>	Configures the system's network name.
<b>interface</b>	Configures a Gigabit Ethernet interface.
<b>ip</b>	Configures IP parameters.

<b>ipv6</b>	IPv6 Configuration commands.
<b>kernel</b>	Enables access to the kernel debugger.
<b>line</b>	Specifies terminal line settings.
<b>logging</b>	Configures the syslog <sup>2</sup> .
<b>ntp</b>	Configures the NTP <sup>3</sup> .
<b>port-channel</b>	Configures port channel global options.
<b>primary-interface</b>	Configures a primary interface.
<b>radius-server</b>	Configures RADIUS server authentication.
<b>service-broker</b>	Configures Service Broker-related parameters.
<b>service-monitor</b>	Configure Service Monitor related parameters.
<b>snmp-server</b>	Configures the SNMP server.
<b>ssh-key-generate</b>	Generates the SSH <sup>4</sup> host key.
<b>sshd</b>	Configures the SSH service.
<b>tacacs</b>	Configures Tacacs+ authentication.
<b>tcp</b>	Configures global TCP parameters.
<b>telnet</b>	Configures Telnet services.
<b>transaction-logs</b>	Configures the transaction logging.
<b>url-signature</b>	Configures an encryption key to use when signing a URL.
<b>username</b>	Establishes username authentication.
<b>VDSM</b>	Configures the VDSM settings.

1. CMS = Centralized Management System
2. syslog = system logging
3. NTP = Network Time Protocol
4. SSH = Secure Shell

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 an interface configuration mode, use the **no** command in interface configuration mode.

```
no { autosense | bandwidth { 10-10 | 100-100 | 1000-1000 | 10000-10000 } | description |
    full-duplex | half-duplex | ip { access-group { num { in | out } | name { in | out } | address
    ip-addr } | ipv6 { access-group { num { in | out } | name { in | out } | address ip-addr } | lacp | mtu
    | shutdown | standby group-num [priority interface] }
```

Syntax	Description
<b>autosense</b>	Negates an autosense interface.
<b>bandwidth</b>	Negates a bandwidth interface.
<b>10-10</b>	Specifies 10 Mb per second bandwidth.
<b>100-100</b>	Specifies 100 Mb per second bandwidth.
<b>1000-1000</b>	Specifies 1000 Mb per second bandwidth.
	<b>Note</b> Not available on all ports.
<b>10000-10000</b>	Specifies 10000 Mb per second bandwidth.
	<b>Note</b> Not available on all ports.
<b>description</b>	Negates a description-specific interface.
<b>full-duplex</b>	Negates a full-duplex interface.
<b>half-duplex</b>	Negates a half-duplex interface.
<b>ip</b>	Negates Internet Protocol configuration commands.
<b>access-group</b>	Specifies access control for packets.
<i>num</i>	IP access list number (standard or extended).
<b>in</b>	Inbound packets.
<b>out</b>	Outbound packets.
<b>name</b>	Access list name.
<b>address</b>	Sets the IP address of the interface.
<i>ip-addr</i>	Interface IP address.
<i>netmask</i>	Interface netmask.
<b>range</b>	Sets the IP address range.
<i>low-num</i>	IP address low range of the interface.
<i>high-num</i>	IP address high range of the interface.
<b>lacp</b>	Negates the Link Aggregation Control Protocol.
<b>mtu</b>	Sets the interface Maximum Transmission Unit.
<i>size</i>	MTU size in bytes.
<b>shutdown</b>	Shuts down the specific portchannel interface.
<b>standby</b>	Negates the standby interface configuration commands.
<i>group-num</i>	Specifies the standby group number.
<b>priority</b>	Sets the priority of the interface for the standby group.
<i>interface</i>	Interface priority.

---

**Defaults**

**Priority:** 100.

---

**Command Modes**

Interface configuration (config-if) mode.

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>interface</b>	Configures a Gigabit Ethernet or port channel interface.
<b>show interface</b>	Displays the hardware interface information.
<b>show running-config</b>	Displays the current running configuration information on the terminal.
<b>show startup-config</b>	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

<b>server</b>	Sets the NTP server IP address.
<i>ip_address</i>	NTP server IP address.
<i>hostname</i>	NTP server hostname.
<i>ip_addresses</i>	(Optional) IP address of the time server providing the clock synchronization (maximum of four).
<i>hostnames</i>	(Optional) Hostname of the time server providing the clock synchronization (maximum of four).

## Defaults

None

## Command Modes

Global configuration (config) mode.

## Usage Guidelines

Use this command to synchronize the SB or VDSM clock with the specified NTP server. The **ntp server** command enables NTP servers for timekeeping purposes and is the only way to synchronize the system clock with a time server.

When you synchronize the VDSM clock with an NTP server, there is a possibility of all devices registered with the VDSM being shown as offline and then reverted to online status. This situation can occur when synchronization with the NTP server sets the VDSM clock forward in time by an interval greater than at least two polling intervals or when the software clock on the VDSM is changed by a similar value using the **clock** command in EXEC configuration mode. The VDSM determines the status of devices in the VDS-SB network depending on when it was last contacted by the devices for a getUpdate request. If you set the VDSM clock ahead in time, you have added that amount of time to the period since the VDSM received the last getUpdate request. However, it is only a transient effect. Once the devices contact the VDSM for their next getUpdate request after the clock setting change, the VDSM 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:

```
ServiceBroker(config)# ntp 172.16.22.44
```

The following example shows how to reset the time server providing the clock synchronization:

```
ServiceBroker(config)# no ntp 172.16.22.44
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>clock</b>	Sets or clears clock functions or updates the calendar.
	<b>show clock</b>	Displays the system clock.
	<b>show ntp</b>	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.

**Defaults** None

**Command Modes** EXEC configuration mode.

**Usage Guidelines** Use NTP to find the current time of day and set the SB 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 SB using an NTP server:

```
ServiceBroker# ntpdate 10.11.23.40
```

Related Commands	Command	Description
	<b>clock set</b>	Sets the time and date.
	<b>show clock</b>	Displays the system clock.

# ping

To send echo packets for diagnosing basic network connectivity on networks, use the **ping** command in EXEC configuration mode.

```
ping {hostname | ip_address}
```

Syntax Description	<i>hostname</i>	Hostname of system to ping.
	<i>ip_address</i>	IP address of system to ping.

**Defaults** 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 SB. 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 SB found no corresponding entry in the route table.

**Examples** The following example shows how to test the basic network connectivity with a host:

```
ServiceBroker# 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
ServiceBroker#
```

# 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-mixed-ip-port** | **dst-port** | **round-robin** | **src-dst-mac** | **src-dst-mixed-ip-port** | **src-dst-port** | **src-mixed-ip-port** | **src-port** }

**no port-channel load-balance**

Syntax Description		
<b>load-balance</b>		Configures the load balancing method.
<b>dst-ip</b>		Specifies the load balancing method using destination IP addresses.
<b>dst-mac</b>		Specifies the load balancing method using destination MAC addresses.
<b>dst-mixed-ip-port</b>		Specifies the destination IP Addr and Layer 4 port.
<b>dst-port</b>		Specifies the load balancing method using destination Layer 4 port.
<b>round-robin</b>		Specifies the load balancing method using round-robin sequential, cyclical resource allocation (each interface in the channel group).
<b>src-dst-mac</b>		Specifies the load balancing method using source and destination MAC address.
<b>src-dst-mixed-ip-port</b>		Specifies the source and destination IP Addr and Layer 4 port.
<b>src-dst-port</b>		Specifies the load balancing method using source and destination port.
<b>src-mixed-ip-port</b>		Specifies the source and destination IP Addr and Layer 4 port.
<b>src-port</b>		Specifies the load balancing method using source Layer 4 port.

**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 VDS-SB 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 VDS-SB 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 SB:

```
ServiceBroker(config)# port-channel load-balance round-robin
```

**Related Commands**

Command	Description
<b>interface</b>	Configures a Gigabit Ethernet or port-channel interface

# primary-interface

To configure the primary interface for the VDS-SB 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

<b>GigabitEthernet</b>	Selects a Gigabit Ethernet interface as the VDS-SB network primary interface.
<i>1-2/</i>	Gigabit Ethernet slot numbers 1 or 2.
<i>port</i>	Port number of the Gigabit Ethernet interface.
<b>PortChannel</b>	Selects a port channel interface as the VDS-SB network primary interface.
<i>1-2</i>	Port channel number 1 or 2.
<b>Standby</b>	Selects a standby group as the VDS-SB network primary interface.
<i>group_num</i>	Standby group number.

## Defaults

The default primary interface is the first operational interface on which a link beat is detected. Interfaces with lower-number IDs are polled first (for example, GigabitEthernet 0/0 is checked before 1/0). Primary interface configuration is required for the proper functioning of the Centralized Management System (CMS). After devices are registered to the VDSM, the VDSM uses the configured primary interface to communicate with the registered devices.

You cannot enable the VDS-SB 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 VDS-SB 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 SB.

## 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 VDS-SB network.

The primary interface can be changed without disabling the VDS-SB 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 VDS-SB network, if you want to re-enable the VDS-SB 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 SB:

```
ServiceBroker(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 SB:

```
ServiceBroker(config)# primary-interface GigabitEthernet 2/0
```

# 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.

---

**Defaults** None

---

**Command Modes** EXEC configuration mode.

---

**Usage Guidelines** Use this command to display the present working directory of the SB.

---

**Examples** The following example shows how to view the present working directory:

```
ServiceBroker# pwd
/local1
```

---

Related Commands	Command	Description
	<b>cd</b>	Changes from one directory to another directory.
	<b>dir</b>	Displays a detailed list of files contained within the working directory, including names, sizes, and time created.
	<b>lls</b>	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.
	<b>ls</b>	Lists the files or subdirectory names within a directory.

---

# radius-server

To configure RADIUS authentication parameters, use the **radius-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
<b>enable</b>	Enables HTTP RADIUS authentication.
<b>host</b>	Specifies a RADIUS server.
<i>hostname</i>	Hostname of the RADIUS server.
<i>host_ipaddr</i>	IP address of the RADIUS server.
<b>auth-port</b>	(Optional) Sets the UDP port for the RADIUS Authentication Server.
<i>port</i>	UDP port number (from 1 to 65535). The default is 1645.
<b>key</b>	Specifies the encryption key shared with the RADIUS server.
<i>keyword</i>	Text of the shared key (maximum of 15 characters).
<b>redirect</b>	Redirects the response if an authentication request fails.
<b>enable</b>	Enables the redirect feature.
<b>message</b>	Replies with an authentication failure message.
<i>reply</i>	Reply message text string (maximum of 24 characters).
<b>location</b>	Sets the HTML page location, for example, <a href="http://www.cisco.com">http://www.cisco.com</a> .
<i>url</i>	URL destination of authentication failure instructions.
<b>retransmit</b>	Specifies the number of transmission attempts to an active server.
<i>retries</i>	Number of transmission attempts for a transaction (from 1 to 3).
<b>timeout</b>	Time to wait for a RADIUS server to reply.
<i>seconds</i>	Wait time in seconds (from 1 to 20).

Defaults
<b>auth-port</b> <i>port</i> : UDP port 1645
<b>retransmit</b> <i>retries</i> : 2
<b>timeout</b> <i>seconds</i> : 5

Command Modes
Global configuration (config) mode.

Usage Guidelines
<i>RADIUS</i> is a client/server authentication and authorization access protocol used by an VDS-SB network device to authenticate users attempting to connect to a network device. The VDS-SB network device functions as a client, passing user information to one or more RADIUS servers. The VDS-SB 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 SB to configure the SB for monitoring, configuration, or troubleshooting purposes. For more information, see the [“Enabling and Disabling Administrative Login Authentication Through RADIUS” section on page 2-160](#).
- HTTP request authentication—When an end user sends a service request that requires privileged access to content that is served by the SB. For more information, see the [“Configuring RADIUS Authentication of HTTP Requests” section on page 2-161](#).

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 SB to use RADIUS to authenticate and authorize administrative login requests, follow these guidelines:

- By default, RADIUS authentication and authorization is disabled on an SB.
- Before enabling RADIUS authentication on the SB, you must specify at least one RADIUS server for the SB 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 VDSM GUI or the CLI to enable RADIUS authentication on an SB.

**Tip**

From the VDSM GUI, choose **Devices > General Settings > Authentication**. Use the displayed Authentication Configuration window.

To use the SB CLI to enable RADIUS authentication on an SB, enable RADIUS authentication for normal login mode by entering the **authentication login radius enable** command in Global configuration mode as follows:

```
ServiceBroker(config)# authentication login radius enable [primary] [secondary]
```

Use the **authentication configuration radius** command in Global configuration mode to enable RADIUS authorization as follows:

```
ServiceBroker(config)# authentication configuration radius enable [primary] [secondary]
```

**Note**

To disable RADIUS authentication and authorization on an SB, use the **no radius-server enable** command.

**Configuring RADIUS Authentication of HTTP Requests**

To configure RADIUS authentication for HTTP requests on an SB, configure the RADIUS server settings on the SB and enable RADIUS authentication for HTTP requests on the SB 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.

```
ServiceBroker(config)# radius-server enable
ServiceBroker(config)# radius-server host 172.16.90.121
ServiceBroker(config)# radius-server key myradiuskey
ServiceBroker(config)# rule action no-auth pattern-list 2
ServiceBroker(config)# rule pattern-list 2 domain mydomain.net
```

```
ServiceBroker# 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
```

```
ServiceBroker# show rule all
Rules Template Configuration
-----
Rule Processing Enabled
rule no-auth domain mydomain.net
```

The following example disables RADIUS authentication on the SB:

```
ServiceBroker(config)# no radius-server enable
```

The following example shows how to force the SB to try RADIUS authentication first:

```
ServiceBroker(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 SB filters HTTP, HTTPS, and RTSP traffic.
show radius-server	Displays RADIUS information.

# reload

To halt and perform a cold restart on the SB, use the **reload** command in EXEC configuration mode.

**reload [force]**

<b>Syntax Description</b>	<b>force</b> (Optional) Forces a reboot without further prompting.
<b>Defaults</b>	None
<b>Command Modes</b>	EXEC configuration mode.
<b>Usage Guidelines</b>	<p>To reboot the SB, use the <b>reload</b> 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.</p> <p>To save any file system contents to disk from memory before a restart, use the <b>cache synchronize</b> command.</p>

**Examples** The following example shows how to reload the SB after you have saved the configuration changes.

```
ServiceBroker# 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 SB:

```
ServiceBroker# reload force
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>cache synchronize</b>	Saves any file system contents to disk from memory before a restart.
	<b>write</b>	Saves startup configurations.
	<b>write erase</b>	Erases the startup configuration from NVRAM.

# rename

To rename a file on the SB, use the **rename** command in EXEC configuration mode.

```
rename old_filename new_filename
```

Syntax Description	<i>old_filename</i>	Original filename.
	<i>new_filename</i>	New filename.

**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:

```
ServiceBroker# rename errlog.txt old_errlog.txt
```

Related Commands	Command	Description
	<b>cpfile</b>	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.
	<b>preserve</b>	(Optional) Preserves certain configurations and data on the device.
	<b>basic-config</b>	(Optional) Selects basic network configurations.

**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:

```
ServiceBroker# restore factory-default

Need to cd to / before issuing this command

Command aborted.
ServiceBroker#
```

Be sure to back up the VDSM database and copy the backup file to a safe location that is separate from that of the VDSM, or change over from the primary to a standby VDSM before you use the **restore factory-default** command on your primary VDSM. The primary VDSM 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 VDSM 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 VDSM database, all configuration records for the entire VDS-SB network are deleted. If you do not have a valid backup file or a standby VDSM, you must use the **cms deregister force** command and reregister every SB after you have reconfigured the VDSM, because all previously configured data is lost.

If you used your standby VDSM to store the database while you reconfigured the primary, you can simply register the former primary as a new standby VDSM.

If you created a backup file while you configured the primary VDSM, you can copy the backup file to this newly reconfigured VDSM 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 VDS Service Broker 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 VDS Service Broker 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 VDS-SB network after using the **restore factory-default preserve basic-config** command, reconfigure the primary interface after the factory defaults have been restored.

```
VDSM# restore factory-default
```

```
This command will wipe out all of data on the disks
and wipe out VDS-SB 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 ]
```

```
VDSM# restore factory-default preserve basic-config
```

```
This command will wipe out all of data on the disks
and all of VDS-SB 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):

```
ServiceBroker# 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
<b>cms database backup</b>	Backs up the existing management database for the VDSM.
<b>cms database restore</b>	Restores the database management tables using the backup local filename.
<b>show disks</b>	Displays the names of the disks currently attached to the SB.
<b>show running-config</b>	Displays the current running configuration information on the terminal.
<b>show startup-config</b>	Displays the startup configuration.
<b>show wmt</b>	Displays WMT bandwidth and proxy mode configuration.

# rmdir

To delete a directory, use the **rmdir** command in EXEC configuration mode.

**rmdir** *directory*

<b>Syntax Description</b>	<i>directory</i> Name of the directory that you want to delete.								
<b>Defaults</b>	None								
<b>Command Modes</b>	EXEC configuration mode.								
<b>Usage Guidelines</b>	Use this command to remove any directory from the SB file system. The <b>rmdir</b> command removes only empty directories.								
<b>Examples</b>	The following example shows how to remove the oldfiles directory under /local1: <pre>ServiceBroker# rmdir /local1/oldfiles</pre>								
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>lls</b></td> <td>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.</td> </tr> <tr> <td><b>ls</b></td> <td>Lists the files or subdirectory names within a directory.</td> </tr> <tr> <td><b>mkdir</b></td> <td>Creates a new directory or subdirectory in the SB file system.</td> </tr> </tbody> </table>	Command	Description	<b>lls</b>	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.	<b>ls</b>	Lists the files or subdirectory names within a directory.	<b>mkdir</b>	Creates a new directory or subdirectory in the SB file system.
Command	Description								
<b>lls</b>	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.								
<b>ls</b>	Lists the files or subdirectory names within a directory.								
<b>mkdir</b>	Creates a new directory or subdirectory in the SB file system.								

# 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.
	<b>execute</b>	Executes the script. The script file must be a sysfs file in the current directory.
	<i>file_name</i>	Name of the script file.

**Defaults** 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:

```
ServiceBroker# 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 VDSM:

```
service cms restart
```

On the SB:

```
service {service-broker | cms | service-monitor}
```

## Syntax Description

<b>cms</b>	Specifies CMS services.
<b>service-broker</b>	Specifies Service Broker services.
<b>service-monitor</b>	Specifies Service Monitor services.

## Defaults

None

## Command Modes

EXEC configuration mode.

## Examples

The following example shows how to restart service-broker service:

```
ServiceBroker# service service-broker restart
The service service broker has been restarted successfully!
ServiceBroker#
```

# setup

To configure basic configuration settings (general settings, device network settings, and disk configuration) on the SB 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.

---

**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 SB running the VDS-SB software:

```
ServiceBroker# 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 Default** None

**Command Modes** EXEC configuration mode.

**Usage Guidelines** [Table 3-2](#) describes the fields shown in the **show aaa commands** command display.

*Table 3-2 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 3-2** *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 3-3](#) describes the fields shown in the **show aaa enable** command display.

**Table 3-3** *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 3-4](#) describes the fields shown in the **show aaa exec** command display.

**Table 3-4** *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 3-5 describes the fields shown in the **show aaa login** command display.

Table 3-5 *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 3-6 describes the fields shown in the **show aaa system** command display.

Table 3-6 *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
<b>aaa</b>	Configures accounting, authentication and authorization methods.
<b>show aaa</b>	Displays the accounting, authentication and authorization configuration.
<b>show statistics aaa</b>	Displays accounting, authentication and authorization statistics.

# show access-lists

To display the access control list (ACL) configuration, use the **show access-lists** command in EXEC configuration mode.

**show access-lists**

**Syntax Description** This command has no arguments or keywords.

**Command Default** None

**Command Modes** EXEC configuration mode.

**Usage Guidelines** [Table 3-7](#) describes the fields shown in the **show access-lists 300** display.

*Table 3-7 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
	<b>access-lists</b>	Configures access control list entries.

## 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		
<b>critical</b>	(Optional)	Displays critical alarm information.
<b>detail</b>	(Optional)	Displays detailed information for each alarm.
<b>support</b>	(Optional)	Displays additional information about each alarm.
<b>history</b>	(Optional)	Displays information about the history of various alarms.
<i>start_num</i>	(Optional)	Alarm number that appears first in the alarm history (1 to 100).
<i>end_num</i>	(Optional)	Alarm number that appears last in the alarm history (1 to 100).
<b>major</b>	(Optional)	Displays information about major alarms.
<b>minor</b>	(Optional)	Displays information about minor alarms.
<b>status</b>	(Optional)	Displays the status of various alarms and alarm overload settings.

**Defaults** None

**Command Modes** EXEC configuration mode.

**Usage Guidelines** The Node Health Manager enables VDS-SB 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 SB. 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 SB. These alarms are referred to as VDS-SB software alarms.

The VDS-SB software uses SNMP to report error conditions by generating SNMP traps. In the VDS-SB software, the following SB applications can generate an VDS-SB 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 VDS-SB software are as follows:

- Critical—Alarms that affect the existing traffic through the SB and are considered fatal (the SB 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 VDS-SB 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 VDS-SB software on the SB. The VDS-SB 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 SB'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 Broker, the protocol engine raises an alarm and sends a `threshold exceeded` notification to the Service Broker. Any new requests for that protocol engine are not routed to that Service Broker. Service Broker

**Note**

This feature only applies to the Windows Media Streaming engine, the Flash Media Streaming engine, and the Movie Streamer engine.

Table 3-8 describes the fields shown in the **show alarms history** display.

**Table 3-8** *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 <code>disk_failed</code> , 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 3-9 describes the fields shown in the **show alarms status** display.

**Table 3-9** *show alarms status Field Descriptions*

<b>Field</b>	<b>Description</b>
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**

<b>Command</b>	<b>Description</b>
<b>alarm</b>	Configure alarms.
<b>snmp-server enable traps</b>	Enables the SB 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.

**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 3-10](#) describes the fields shown in the **show arp** display.

*Table 3-10 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

<b>Syntax Description</b>	<b>user</b>	Displays the authentication configuration for the user login to the system.
---------------------------	-------------	---

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	EXEC configuration mode.
----------------------	--------------------------

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>clear</b>	Clears the HTTP object cache, the hardware interface, statistics, archive working transaction logs, and other settings.

# 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.

**Defaults** None

**Command Modes** EXEC configuration mode.

**Usage Guidelines** [Table 3-11](#) describes the fields shown in the **show banner** display.

*Table 3-11 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
	<b>banner</b>	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**]

<b>Syntax Description</b>	<b>movie-streamer</b>	(Optional) Displays the Movie Streamer bit rate settings.
	<b>wmt</b>	(Optional) Displays Windows Media Technology (WMT) bit rate settings.

**Defaults** None

**Command Modes** EXEC configuration mode.

**Usage Guidelines** [Table 3-12](#) describes the fields shown in the **show bitrate** display.

*Table 3-12 show bitrate Field Descriptions*

Field	Description
Module	Types of application servers for which the bit rate is displayed: <ul style="list-style-type: none"> <li>• <b>wmt outgoing</b> is the maximum bit rate per WMT stream that can be served by the SB.</li> <li>• <b>wmt incoming</b> is the maximum bit rate per WMT stream that can be received by the SB.</li> <li>• <b>movie-streamer outgoing</b> is the maximum bit rate per streamer that can be served by the SB.</li> <li>• <b>movie-streamer incoming</b> is the maximum bit rate per streamer that can be received by the SB.</li> </ul>
Default Bitrate Kbps	Bit rate associated with the application servers when the bit rate has not been configured on the SB.
Configured Bitrate Kbps	Bit rate configured on the SB in kilobits per second.

Related Commands	Command	Description
	<b>bitrate</b>	Configures the maximum pacing bit rate for large files for the Movie Streamer and separately configures WMT bit-rate settings.

# 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
<b>detail</b>	(Optional) Displays detailed information; indicates the Network Timing Protocol (NTP) clock source and the current summer time setting (if any).
<b>standard-timezones</b>	(Optional) Displays information about the standard time zones.
<b>all</b>	Displays all the standard time zones (approximately 1500 time zones). Each time zone is listed on a separate line.
<b>details</b>	Displays detailed information for the specified time zone.
<i>timezone</i>	Name of the time zone.
<b>regions</b>	Displays the region name of all the standard time zones. All 1500 time zones are organized into directories by region.
<b>zones</b>	Displays the name of every time zone that is within the specified region.
<i>region_name</i>	Name of the region.

**Defaults** None

**Command Modes** EXEC configuration mode.

**Usage Guidelines** The VDS-SB 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 3-13](#) describes the field in the **show clock** display.

**Table 3-13** *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 3-14 describes the fields shown in the **show clock detail** display.

**Table 3-14** *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.

```
ServiceBroker # 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.

```
ServiceBroker # 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).

```
ServiceBroker# 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).

```
ServiceBroker # 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
<b>clock (EXEC)</b>	Sets or clears clock functions or updates the calendar.
<b>clock (Global configuration)</b>	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		
<b>database</b>		Displays embedded database maintenance information.
<b>content</b>		Writes the database content to a file.
<b>dump</b>		Dumps all database content to a text file.
<i>filename</i>		Name of the file to be saved under local1 directory.
<b>text</b>		Writes the database content to a file in text format.
<b>xml</b>		Writes the database content to a file in XML format.
<b>maintenance</b>		Shows the current database maintenance status.
<b>detail</b>		(Optional) Displays database maintenance details and errors.
<b>info</b>		Displays CMS application information.
<b>processes</b>		Displays CMS application processes.

**Defaults** None

**Command Modes** EXEC configuration mode.

**Usage Guidelines** [Table 3-15](#) describes the fields shown in the VDSM **show cms info** display.

*Table 3-15 show cms Field Descriptions for the VDSM*

Field	Description
<b>CDN information</b>	
Model	Model name of the device.
Node Id	Unique identifier given to the device by the VDSM at registration, which is used to manage the device.
Device Mode	Configured mode of device used during registration.
Current VDSM role	Role of the current VDSM: Primary or Standby.
<b>CMS services information</b>	
Service cms_httpd is running	Status of the cms_httpd management service (running or not running). This field is specific to the VDSM only.
Service cms_VDSM is running	Status of the cms_VDSM management service (running or not running). This field is specific to the VDSM only.

Table 3-16 describes the fields shown in the SB **show cms info** display.

**Table 3-16** *show cms Field Descriptions for the SB*

Field	Description
<b>CDN information</b>	
Model	Model name of the device.
Node Id	Unique identifier given to the device by the VDSM at registration, which is used to manage the device.
Device Mode	Configured mode of device used during registration.
Current VDSM address	Address of the VDSM as currently configured in the <b>vdsml ip</b> command in Global configuration mode. This address may differ from the registered address if a standby VDSM is managing the device instead of the primary VDSM with which the device is registered.
Registered with VDSM	Address of the VDSM with which the device is registered.
Status	Connection status of the device to the VDSM. 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 VDSM for updates.

The following example writes the database content to a file in text format:

```
VDSM# 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:

```
VDSM# 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 SB:

```
ServiceBroker# 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
ServiceBroker#
```

#### Related Commands

Command	Description
<b>cms (EXEC)</b>	Configures the CMS-embedded database parameters.
<b>cms (global)</b>	Schedules maintenance and enables the CMS on a given node.

# show debugging

To display the state of each debugging option, use the **show debugging** user command in user EXEC configuration mode.

## show debugging

**Syntax Description** This command has no arguments or keywords.

**Command Default** None

**Command Modes** User EXEC configuration mode.

**Examples** The following is sample output from the **show debugging** command:

```
ServiceRouter# show debugging
Debug web-engine is set to trace
Debug capturecontroller is set to trace
ServiceRouter#
```

Related Commands	Command	Description
	<b>debug</b>	Monitors and records caching application functions.
	<b>undebug</b>	Disables debugging functions.

# 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
<b>configured</b>	Displays the configured device mode.
<b>current</b>	Displays the current device mode.

**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 VDS-SB 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 to an SB using the **device mode** command:

```
Acmehost# show device-mode current
Current device mode: service-broker
Acmehost# show device-mode configured
Configured device mode: service-broker
Acmehost(config)# device mode service-broker
The new configuration will take effect after a reload
Acmehost(config)# exit
Acmehost# show device-mode current
Current device mode: service-broker
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-broker
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-broker
!
```

## ■ show device-mode

```

hostname Acmehost
..

Acmehost# show device-mode configured
Configured device mode: service-broker
Acmehost# show device-mode current
Current device mode: service-broker

```

Related Commands	Command	Description
	<b>device</b>	Configures the mode of operation on a device as a VDSM, or SB.

# 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
<b>current</b>	(Optional) Displays currently effective configurations.
<b>details</b>	(Optional) Displays currently effective configurations with more details.
<b>error-handling</b>	(Optional) Displays the disk error-handling statistics.
<b>details</b>	(Optional) Displays the detail disk and sector errors.
<b>raid-state</b>	(Optional) Displays the volume and progress information for the RAID disks.
<b>SMART-info</b>	(Optional) Displays hard drive diagnostic information and information about impending disk failures.
<b>details</b>	(Optional) Displays SMART disk monitoring info with more details.

**Defaults** None

**Command Modes** EXEC configuration mode.

**Usage Guidelines** The **show disks** command displays the names of the disks currently attached to the SB.

[Table 3-17](#) describes the fields shown in the **show disks details** display.

*Table 3-17 show disks details Field Descriptions*

Field	Description
disk00	Availability of the disk: Present, Not present or Not responding, Not used, or (*). <b>Note</b> 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 SB 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 3-18](#) describes the fields shown in the **show disks error-handling details** display.

**Table 3-18** *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 VDS-SB 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 VDS-SB 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 3-19](#) describes some typical fields in the **show disks SMART-info** display.

**Table 3-19** *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 3-19 *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:

```
ServiceBroker# 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:

```
ServiceBroker# 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 SBs (Service Broker A and Service Broker B). These two SBs contain hard disks that were manufactured by different vendors.

```
ServiceBroker# 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:

```

ServiceBroker# #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
<b>disk</b> (EXEC)	Configures disks and allocates disk space for devices using VDS-SB software.

# 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.

**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 VDS-SB software that runs on the device after reload.



### Note

If you update the VDS-SB software on an SB, 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:

```
ServiceBroker# show flash
VDS-SB software version (disk-based code): VDS-SB-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 3-20 describes the fields shown in the **show flash** display.

**Table 3-20** show flash Field Descriptions

Field	Description
VDS-SB software version (disk-based code)	VDS-SB software version and build number that is running on the device.
<b>System image on flash:</b>	
Version	Version and build number of the software that is stored in flash memory.
<b>System flash directory:</b>	

Table 3-20 *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
<b>show version</b>	Displays the version information about the software.

# 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.

---

**Defaults** None

---

**Command Modes** EXEC configuration mode.

---

**Examples** The following example shows how to display the caching configuration of FTP:

```
ServiceBroker# 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.
```

---

Related Commands	Command	Description
	ftp	Enables FTP services.

---

# show geo-location-server

It displays information about primary and secondary Geo location server [ip address and port configured].

If Geo server monitoring is enabled/disabled. By default it is enabled. Geo monitoring polling interval is configured in seconds. The status of the Geo location server will be checked at each poll-interval. Default is 60 sec. Geo location server timeout - time after which the server will be treated as inactive. Default is 1 sec.

## show geo-location-server

---

**Syntax Description** This command has no arguments or keywords.

---

**Command Default** None

---

**Command Modes** EXEC configuration mode.

---

**Examples** The following example shows how to display information about primary and secondary Geo location server

```
ServiceBroker# show geo-location-server

Primary geo location server 1.1.1.3 7000
Secondary geo location server 1.1.1.2 7000
Geo Location server monitoring is enabled
Geo Location server poll rate 30 seconds
Geo Location server timeout 5 seconds
```

# show geo-location-service

It displays if location service is enabled/disabled, location cache timeout and max location cache entries.

**show geo-location-service**

---

**Syntax Description** This command has no arguments or keywords.

---

**Command Default** None

---

**Command Modes** EXEC configuration mode.

---

**Examples** The following example displays if location service is enabled or disabled.

```
ServiceBroker# show geo-location-service

Location based service is enabled
Location cache timeout 600000 seconds
Location cache max entries 10000
```

# 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
<b>all</b>	(Optional) Displays all hardware class information.
<b>core</b>	(Optional) Displays core hardware information.
<b>cpuinfo</b>	(Optional) Displays CPU information.
<b>dmi</b>	(Optional) Displays DMI <sup>1</sup> .
<b>all</b>	(Optional) Displays all DMI information.
<b>baseboard</b>	(Optional) Displays motherboard information.
<b>bios</b>	(Optional) Displays BIOS information.
<b>cache</b>	(Optional) Displays processor cache information.
<b>chassis</b>	(Optional) Displays chassis information.
<b>connector</b>	(Optional) Displays connector information.
<b>memory</b>	(Optional) Displays physical memory information.
<b>processor</b>	(Optional) Displays processor information.
<b>slot</b>	(Optional) Displays PCI slot information.
<b>system</b>	(Optional) Displays system information.
<b>mapping</b>	(Optional) Shows mapping between Cisco and Linux hardware names.
<b>disk</b>	Maps Cisco disk name to Linux device name.
<i>diskname</i>	Name of the disk (disk00).
<b>interface</b>	Maps Cisco interface name to Linux device name.
<b>all</b>	Displays all interface information.
<b>GigabitEthernet</b>	Selects a 1G ethernet interface.
<i>slot/port_num</i>	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 (/).
<b>TenGigabitEthernet</b>	Selects a 10G ethernet interface.
<b>meminfo</b>	(Optional) Displays RAM information.
<b>pci</b>	(Optional) Displays PCI information.
<b>details</b>	(Optional) Show output with PCI addresses and names.
<b>drivers</b>	(Optional) Identify driver names and availability.
<b>ids</b>	(Optional) Show PCI vendor and device codes.
<b>tree</b>	(Optional) Show a tree-like diagram containing all buses, bridges and devices.

1. Desktop Management Interface

---

**show hardware**


---

**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 3-21](#) describes the fields shown in the **show hardware** display.

*Table 3-21          show hardware Field Descriptions*

<b>Field</b>	<b>Description</b>
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.
<b>Cookie info</b>	
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.
<b>List of all disk drives</b>	
Physical disk information	Lists the disks by number.

Table 3-21 *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.
<b>Mounted filesystems</b>	
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.
<b>Memory Information</b>	
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 3-21 *show hardware Field Descriptions (continued)*

Field	Description
SUnreclaim	
KernelStack	
PageTables	
NFS_Unstable	
Bounce	
WritebackTmp	
CommitLimit	
Committed_AS	
VmallocTotal	
VmallocUsed	
VmallocChunk	
DirectMap4k	
DirectMap2M	
<b>PCI Information</b>	

**Examples**

The following example shows how to display the core hardware information:

```
ServiceBroker# show hardware core
VDS Service Broker Software (VDS-SB)
Copyright (c) 1999-2011 by Cisco Systems, Inc.
VDS Service Broker Software Release 2.6.0 (build
b460 Aug 28 2011)
Version: cde220-2g2-DEVELOPMENT[vcn-build1:/auto/v
cn-ul/vosis_release_builds/vosis_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: 9999999999
Model Type:
SerialNumber (raw): 57 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:

```

ServiceBroker# show hardware dmi
----- DMI Information -----
# dmidecode 2.9
SMBIOS 2.5 present.
70 structures occupying 2793 bytes.
Table at 0xCF66000.

Handle 0x0000, DMI type 0, 24 bytes
BIOS Information
  Vendor: Phoenix Technologies LTD
  Version: 1.2a
  Release Date: 04/09/2009
  Address: 0xE3DD0

```

■ **show hardware**

```

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
ServiceBroker#

```

Related Commands	Command	Description
	<b>show version</b>	Displays version information about the SB software.

# show hosts

To view the hosts on your SB, use the **show hosts** command in EXEC configuration mode.

## show hosts

**Syntax Description** This command has no arguments or keywords.

**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 3-22](#) describes the fields shown in the **show hosts** display.

*Table 3-22 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 <sup>1</sup> name server or servers.
<b>Host Table</b>	
hostname	FQDN <sup>2</sup> (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 <b>host</b> 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 | 3 | 4 } | standby
               group_num | TenGigabitEthernet slot/port}
```

Syntax Description		
<b>all</b>		Displays information for all interfaces.
<b>GigabitEthernet</b>		Displays information for the Gigabit Ethernet device.
<i>slot/port</i>		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 (/).
<b>PortChannel</b>		Displays information for the Ethernet channel of the device.
<b>1</b>		Sets the Ethernet channel interface number to 1.
<b>lACP</b>		(Optional) Displays the LACP port channel status.
<b>2</b>		Sets the Ethernet channel interface number to 2.
<b>3</b>		Sets the Ethernet channel interface number to 3.
<b>4</b>		Sets the Ethernet channel interface number to 4.
<b>standby</b>		Displays information for the standby group for the interface.
<i>group_num</i>		Group number for the selected interface. The group number range is 1 to 4.
<b>TenGigabitEthernet</b>		Displays information for the Ten Gigabit Ethernet device.
<i>slot/port</i>		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 (/).

**Defaults** None

**Command Modes** EXEC configuration mode.

**Usage Guidelines** [Table 3-23](#) describes the fields shown in the **show interface GigabitEthernet** display.

*Table 3-23 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.

Table 3-23 *show interface GigabitEthernet Field Descriptions (continued)*

Field	Description
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.
Flags	Interface status indicators. Values include Up, Broadcast, Running, and Multicast.
Mode	Setting, transmission mode, and transmission for this interface.

Table 3-24 describes the fields shown in the **show interface PortChannel** display.

Table 3-24 *show interface PortChannel Field Descriptions*

Field	Description
Description	Description of the device, as configured by using the <b>description</b> keyword of the <b>interface</b> 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.
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.

Table 3-24 *show interface PortChannel Field Descriptions (continued)*

Field	Description
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.
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 3-25 describes the fields shown in the **show interface standby** display.

Table 3-25 *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 <b>description</b> keyword of the <b>interface</b> command in Global configuration mode.

Table 3-25 *show interface standby Field Descriptions (continued)*

Field	Description
IP address, netmask	IP address and netmask of the standby group.
Member interfaces	Member interfaces of the standby group. Shows which physical interfaces are part of the standby group. Shows the interface definition, such as GigabitEthernet 1/0.
Active interface	Interfaces that are currently active in the standby group.

Table 3-26 describes the fields shown in the **show interface TenGigabitEthernet** display.

Table 3-26 *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.
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.

**show interface**

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>interface</b>	Configures a Gigabit Ethernet or port channel interface.
	<b>lACP</b>	Turns on LACP.
	<b>show lACP</b>	Displays LACP information.
	<b>show running-config</b>	Displays the current running configuration information on the terminal.
	<b>show startup-config</b>	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.

---

**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 SB. Typically, Cisco SBs 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 SB nonvolatile memory. Each SB 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 SB'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 SB models, you can use the **show inventory** command in EXEC configuration mode to display the SB's UDI. On older SB models, use the **show tech-support** command in EXEC configuration mode to display the SB's UDI.

---

**Examples** The following example shows the inventory information for one of the newer SB models (SB-565):

```
ServiceBroker# show inventory
PID: SB-565-K9 VID: 0 SN: serial_number
```

In the preceding example, *serial number* is the serial number of the SB. The version ID is displayed as "0" because the version number is not available.

[Table 3-27](#) describes the fields shown in the **show inventory** display.

Table 3-27 *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 SB model:

```
ServiceBroker# show inventory
Please look at 'sh tech-support' for information!
ServiceBroker# show tech-support
```

**Related Commands**

Command	Description
<b>show tech-support</b>	Displays system information necessary for Cisco Technical Support to assist you with your SB.

# show ip

To display the, use the **show ip** command in user EXEC configuration mode.

## show ip

Syntax	Description
<i>ip_address</i>	(Optional) IP address entered to filter the output to display only a particular host in the BGP routing table.
<i>prefix</i>	(Optional) Prefix entered to filter the output to display only a particular network in the BGP routing table.
<i>prefix_length</i>	(Optional) Specifies the prefix length.

**Command Default** 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
<b>clear ip bgp</b>	Clears entries in the BGP route table.
<b>router bgp</b>	Configures a BGP routing process.

---

# 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.

**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:

```
ServiceBroker# 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:

```
ServiceBroker# 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
```

## show lacp

```
GigabitEthernet 5/0      up      up      bndl      21
GigabitEthernet 6/0      up      up      bndl      21
```

ServiceBroker# **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
<b>lacp</b>	Turns on Link Aggregation Control Protocol (LACP).
<b>show interface portchannel 1 lacp</b>	Displays the link status for the port channel.

# show logging

Command	Description
<b>lacp</b>	Turns on Link Aggregation Control Protocol (LACP).
<b>show interface portchannel 1 lacp</b>	Displays the link status for the port channel.

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.

**Defaults** None

**Command Modes** EXEC configuration mode.

**Usage Guidelines** The following is an example of a syslog message for proxy mode native FTP support:

```
SB-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 VDS-SB network, you can use the system message log in the VDSM GUI. The VDSM logs only severity level critical or higher messages from registered nodes. Also, the VDSM 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, SB, are not related to the messages logged in the system log file on the sysfs partition on the VDSM as /local1/syslog.txt.

The syslog.txt file on the VDSM contains information about events that have occurred on the VDSM 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 VDSM because the problem never occurred on the VDSM but only on the registered node. However, this error message is displayed in the system message log for device the SB device.

**Examples**

The following example shows how to display the syslog host configuration on an SB:

```
ServiceBroker# 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
<b>clear</b>	Clears the HTTP object cache, the hardware interface, statistics, archive working transaction logs, and other settings.
<b>logging</b>	Configures system logging.

# show mount-option

To display the mount options, use the **show mount-option** command in EXEC configuration mode.

## show mount-option

**Syntax Description** This command has no arguments or keywords.

**Defaults** None

**Command Modes** EXEC configuration mode.

**Usage Guidelines** [Table 3-28](#) describes the fields shown in the **show mount-option** display.

*Table 3-28 show mount-option status Field Descriptions*

Field	Description
Read/Write	
ReadBlock Size	
WriteBlock Size	
Mount Timeout	
Retransmit	
Retry Minutes	

Related Commands	Command	Description
	<b>mount-option</b>	Configures the mount option profile for remote storage.

# show ntp

To display the Network Time Protocol (NTP) parameters, use the **show ntp** command in EXEC configuration mode.

## show ntp status

<b>Syntax Description</b>	<b>status</b>	Displays the NTP status.
---------------------------	---------------	--------------------------

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	EXEC configuration mode.
----------------------	--------------------------

<b>Usage Guidelines</b>	<a href="#">Table 3-29</a> describes the fields shown in the <b>show ntp status</b> display.
-------------------------	--

**Table 3-29** *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**

<b>Command</b>	<b>Description</b>
<b>clock</b>	Sets or clears clock functions or updates the calendar.
<b>ntp</b>	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		
<b>cpu</b>	(Optional)	Displays the CPU utilization.
<b>debug</b>	(Optional)	Displays the system call and signal traces for a specified process identifier (PID) to display system progress.
<i>pid</i>		Process identifier.
<b>memory</b>	(Optional)	Displays memory allocation processes.
<b>system</b>	(Optional)	Displays system load information in terms of updates.
<b>delay</b>	(Optional)	Specifies the delay between updates, in seconds. The range is from 1 to 60.
<i>delay_num</i>		Displays delays between updates, in seconds.
<b>count</b>	(Optional)	Specifies the number of updates that are displayed. The range is from 1 to 100.
<i>count_num</i>		Displays the number of updates displayed.

**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 **show process** command with keywords **system** and especially **debug**, unless it is absolutely necessary.

Table 3-30 describes the fields shown in the **show processes** displays.

**Table 3-30** *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 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.

**Defaults** None

**Command Modes** EXEC configuration mode.

**Usage Guidelines** [Table 3-31](#) describes the fields shown in the **show radius-server** display.

*Table 3-31 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 SBs 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 SB.
Key	Key used to encrypt and authenticate all communication between the RADIUS client (the SB) and the RADIUS server.
Timeout	Number of seconds that the SB waits for a response from the specified RADIUS Authentication Server before declaring a timeout.
Retransmit	Number of times that the SB 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 SB is to use for RADIUS authentication.

*Table 3-31 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
	<b>radius-server</b>	Configures RADIUS authentication parameters.

# 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 arguments or keywords.

---

**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:

```
ServiceBroker# show running-config
! VDS-SB version 2.6.0
!
device mode service-broker
!
!
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
```

## show running-config

```

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 $5$bVz2jck/$QYvCAKrBmq3YqM5Ik1vuGrXQACMelfON
dq3/siTpqV8
username admin privilege 15
!
snmp-server enable traps config
snmp-server enable traps service-broker 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
!
!

```

```

ftp enable
!
telnet enable
!
!
!
!
!
!
!
!
!
VDSM 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 VDS-SB configuration
ServiceBroker#

```

**Related Commands**

Command	Description
<b>configure</b>	Enters Global configuration mode.
<b>copy</b>	Copies the configuration or image data from a source to a destination.

## show service-broker

To display the Service Broker configuration, use the **show service-broker** command in EXEC configuration mode.

On the SB:

```
show service-broker { access-policy | bfqdn [all | domain [domain-name] [bfqdn-policy
[print-script | print-xml [filename]]] ] | cdn [all | name cdn-name [adaptation-policy
[print-script | print-xml [filename]]] ] | cdn-metric-provider [all | name
[metric-provider-name] | cdn-network [dump-file | ip-address] | cdn-selection-policy
[print-script | print-xml [filename]] ] | memory [javascript ] | service-broker-policy [
print-script [filename]] | status [ all | cdn cdn-name] }
```

Syntax	Description
<b>access-policy</b>	Displays Access-Policy configurations.
<b>bfqdn</b>	Displays Broker FQDN information.
<b>all</b>	(Optional) Displays all BFQDNs.
<b>domain</b>	(Optional) Displays BFQDN for a given broker.
<b>bfqdn-policy</b>	(Optional) Broker fqdn policy script.
<b>print-script</b>	(Optional) Print Script contents to File.
<b>print-xml</b>	(Optional) Print policies configured in VDSM UI as xml format.
<b>cdn</b>	Displays CDN Information.
<b>all</b>	(Optional) Display for all CDNs.
<b>name</b>	(Optional) Display for a given CDN name.
<b>adaptation-policy</b>	(Optional) CDN Adaptation-Policy script.
<b>cdn-metric-provider</b>	Displays CDN metric provider information.
<b>all</b>	(Optional) Display for all CDN metric providers.
<b>name</b>	(Optional) Display for a given CDN metric provider name.
<b>cdn-network</b>	Displays CDN network (OnNet and OffNet) configuration.
<b>dump-file</b>	Dump CDN network configuration to File.
<b>ip-address</b>	Displays CDN network for the Client IP-Address.
<b>cdn-selection-policy</b>	Displays CDN Selection Policy configuration.
<b>memory</b>	Diaplays Memory Usage statistics for Service Broker.
<b>javascript</b>	Displays Memory Usage statistics for javascript engine.
<b>service-broker-policy</b>	Displays Service Broker Policy configuration.
<b>status</b>	Displays Status of CDN.
<b>all</b>	Displays Status of all CDNs.
<b>cdn</b>	Displays for a given CDN.

**Defaults** None

**Command Modes** EXEC configuration mode.

**Usage Guidelines**

This command allows users to check the Service Broker-related configuration. Through this command, users can view the configured features of an SB, such as location-based parameters.

**Note**

The Load percentage displayed in the Average Device Load field when the **show service-broker service-monitor** command is executed on the SB is the maximum of the average disk load/average CPU load given both CPU and disk monitoring are enabled on the SB.

The memory usage is calculated in the **show service-broker 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.

**Note**

All the commands which output a filename, such as print-xml, print-script, and any others, are located in *local/local1* directory.

**Examples**

The following example shows the memory usage statistics of the service broker:

```
ServiceBroker# show service-broker memory
system bytes      = 347660288
in use bytes      = 347109504
max mmap regions =      189
max mmap bytes    = 345247744
```

The following example shows the memory usage statistics of the javascript engine:

```
ServiceBroker# show service-broker memory javascript
heap size limit      =      1535115264
total heap size      =      4083456
total heap size executable =      2097152
used heap size       =      1086048
```

## 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.
	<i>port_num</i>	(Optional) Displays up to eight port numbers. The port number range is from 1 to 65535.
	<b>summary</b>	Displays the services summary.

**Defaults** None

**Command Modes** EXEC configuration mode.

**Examples** The following example shows how to display the services information by the port number:

```
VDSM# 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:

VDSM# 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											
	VDSM_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		
	<b>alarm-history</b>	Displays SNMP alarm history information.
	<b>engineID</b>	Displays the local SNMP engine identifier.
	<b>group</b>	Displays SNMP groups.
	<b>stats</b>	Displays SNMP statistics.
	<b>user</b>	Displays SNMP users.

**Defaults** None

**Command Modes** EXEC configuration mode.

**Usage Guidelines** This command provides information on various SNMP variables and statistics on SNMP operations. [Table 3-32](#) describes the fields shown in the **snmp alarm-history** display.

*Table 3-32 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 VDS-SB device contain numeric alarm IDs.
ModuleID	Traps sent by a VDS-SB device contain numeric module IDs. See <a href="#">Table 3-34</a> to map module names to module IDs.
Category	Traps sent by an VDS-SB device contain numeric category IDs. See <a href="#">Table 3-34</a> to map category names to category IDs.
Descr	Description of the VDS-SB software alarm and the application that generated the alarm.

Table 3-33 describes the mapping of module names to module IDs.

**Table 3-33** 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 3-34 describes the mapping of category names to category IDs.

**Table 3-34** 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 3-35 describes the fields shown in the **show snmp stats** display.

**Table 3-35** 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 3-35** *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 3-36](#) describes the fields shown in the **show snmp engineID** display.

**Table 3-36** *show snmp engineID Field Descriptions*

Field	Description
Local SNMP Engine ID	String that identifies the copy of SNMP on the local device.

[Table 3-37](#) describes the fields shown in the **show snmp group** display.

**Table 3-37** *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 3-38](#) describes the fields shown in the **show snmp user** display.

Table 3-38 *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
<b>snmp-server community</b>	Configures the community access string to permit access to the SNMP.
<b>snmp-server contact</b>	Sets the system server contact (sysContact) string.
<b>snmp-server enable traps</b>	Enables the SE to send SNMP traps.
<b>snmp-server group</b>	Defines a user security model group.
<b>snmp-server host</b>	Specifies the recipient of a host SNMP trap operation.
<b>snmp-server location</b>	Sets the SNMP system location string.
<b>snmp-server notify inform</b>	Configures the SNMP notify inform request.
<b>snmp-server user</b>	Defines a user who can access the SNMP server.
<b>snmp-server view</b>	Defines a SNMP V2 MIB view.

## 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.

---

**Defaults** None

---

**Command Modes** EXEC configuration mode.

---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	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.

**Defaults** None

**Command Modes** EXEC configuration mode.

**Usage Guidelines** [Table 3-39](#) describes the fields shown in the **show standby** display.

*Table 3-39 show standby Field Descriptions*

Field	Description
Standby Group	Number that identifies the standby group.
Description	Description of the device, as configured by using the <b>description</b> option of the <b>interface</b> 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
<b>show interface</b>	Displays the hardware interface information.
<b>show running-config</b>	Displays the current running configuration information on the terminal.
<b>show startup-config</b>	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 arguments or keywords.

**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 SB:

```
ServiceBroker# show startup-config
! VDS-SB version 2.3.9
!
device mode service-broker
!
!
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
!
!
!
VDSM ip 4.0.8.10
cms enable
!
!
!
service-broker service-monitor threshold wmt 50
service-broker service-monitor number-of-samples wmt 5
service-broker service-monitor sample-period wmt 15
qos device-policy-service enable
!
!
cache content max-cached-entries 1000
! End of VDS-SB configuration

```

■ show startup-config

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>configure</b>	Enters Global configuration mode.
	<b>copy</b>	Copies the configuration or image data from a source to a destination.
	<b>show running-config</b>	Displays the current running configuration information on the terminal.

# show statistics

To display the SB statistics, use the **show statistics** command in EXEC configuration mode.

```
show statistics { aaa | authentication | fd | icmp| icmpv6 | ip | lsof | netstat | radius |
service-broker | services | snmp | tacacs | tcp | transaction-logs | udp }
```

On SB only:

```
show statistics service-broker {all | bfqdn [all | domain ] | cdn [ all | name ] | geo-location |
history | javascript | summary}}
```

Syntax	Description
<b>aaa</b>	Displays AAA statistics.
<b>all</b>	Displays all statistics.
<b>bfqdn</b>	Displays all Broker FQDN specific statistics.
<b>cdn</b>	Displays CDN specific statistics.
<b>authentication</b>	Displays User Authentication statistics.
<b>fd</b>	Displays File Descriptors Limits.
<b>icmp</b>	Displays ICMP statistics.
<b>icmpv6</b>	Displays ICMPV6 statistics.
<b>ip</b>	Displays IP statistics.
<b>lsof</b>	Displays List of Open File Descriptors.
<b>netstat</b>	Displays Internet Socket Connections.
<b>radius</b>	Displays Radius statistics.
<b>service-broker</b>	Displays Service Broker statistics.
<b>services</b>	Displays Services related statistics.
<b>snmp</b>	Displays SNMP statistics.
<b>tacacs</b>	Displays TACAS+ statistics
<b>tcp</b>	Displays TCP statistics.
<b>transaction-logs</b>	Displays Transaction log export statistics.
<b>udp</b>	Displays UDP statistics.
<b>geo-location</b>	Displays Geo Location specific statistics.
<b>history</b>	Displays statistics history.
<b>javascript</b>	Displays javascript statistics.
<b>summary</b>	Displays Summary statistics.

**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 3-40 describes the fields shown in the **show statistics access-lists 300** display.

*Table 3-40 show statistics access-lists 300 Field Descriptions*

Field	Description
<b>Access Control Lists Statistics</b>	
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
<b>clear</b>	Clears the HTTP object cache, the hardware interface, statistics, archive working transaction logs, and other settings.

## show statistics access-lists

To display SB access control list statistics, use the **show statistics access-lists** command in EXEC configuration mode.

### show statistics access-lists

**Syntax Description** This command has no arguments or keywords.

**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 3-41](#) describes the fields shown in the **show statistics access-lists 300** display.

*Table 3-41 show statistics access-lists 300 Field Descriptions*

Field	Description
<b>Access Control Lists Statistics</b>	
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.

Command	Description
<b>clear</b>	Clears the HTTP object cache, the hardware interface, statistics, archive working transaction logs, and other settings.

# 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 arguments or keywords.

**Defaults** None

**Command Modes** EXEC configuration mode.

**Usage Guidelines** [Table 3-42](#) describes the fields shown in the **show statistics admission** display.

*Table 3-42 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 3-42 *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 fd

To display file descriptors limit statistics, use the **show statistics netstat** command in EXEC configuration mode.

## show statistics fd

**Syntax Description** This command has no arguments or keywords.

**Defaults** None

**Command Modes** EXEC configuration mode.

**Usage Guidelines** [Table 3-43](#) describes the fields shown in the **show statistics fd** display.

*Table 3-43 show statistics netstat Field Descriptions*

Field	Description
Number of file descriptors in use	Displays the number of file descriptors currently in use.
Maximum number of file descriptions allowed	Displays the maximum number of file descriptions allowed at one time.
Percentage of file descriptions in use	Displays the percentage of file descriptions currently in use.

**Examples** The following is sample output from the **show statistics fd** command:

```
ServiceBroker# show statistics fd
Number of file descriptors in use           = 3600
Maximum number of file descriptions allowed = 262144
Percentage of file descriptions in use      = 1.37%
```

# show statistics icmp

To display SB 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.

**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 4-1](#).

*Table 4-1*      *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 4-1**      *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 4-2](#).

**Table 4-2**      *Errors*

Error	Type Field Value
Destination Unreachable	3
Source Quench	4
Redirect	5
Time Exceeded	11
Parameter Problems	12

[Table 4-3](#) describes the fields shown in the **show statistics icmp** display.

**Table 4-3**      *show statistics icmp Field Descriptions*

Field	Description
ICMP messages received	Total number of ICMP messages received by the SB.
ICMP messages receive failed	Total number of ICMP messages that were not received by the SB.
Destination unreachable	Number of destination-unreachable ICMP packets received by the SB. 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 4-3 *show statistics icmp Field Descriptions (continued)*

Field	Description
Timeout in transit	<p>Number of ICMP time-exceeded packets received by the SB. 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:</p> <ul style="list-style-type: none"> <li>• 0 = Time-To-Live Equals 0 During Transit</li> <li>• 1 = Time-To-Live Equals 0 During Reassembly</li> </ul> <p>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.</p>
Wrong parameters	<p>Number of ICMP packets with parameter problems received by the SB. 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.</p>
Source quenches	<p>Number of ICMP source-quench packets received by the SB. 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.</p>

Table 4-3 *show statistics icmp Field Descriptions (continued)*

Field	Description
Redirects	<p>Number of ICMP redirect packets received by the SB. 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.</p> <p>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.</p>
Echo requests	<p>Number of echo ICMP packets received by the SB. 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.</p> <p><b>Note</b> You should be suspicious when a large number of these packets are found on the network.</p>
Echo replies	<p>Number of echo-reply ICMP packets received by the SB. 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.</p> <p><b>Note</b> You should be suspicious when a large number of these packets are found on the network.</p>
Timestamp requests	<p>Number of ICMP time stamp request packets received by the SB. 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.</p> <p><b>Note</b> You should be suspicious when a large number of these packets are found on the network.</p>

Table 4-3 *show statistics icmp Field Descriptions (continued)*

Field	Description
Timestamp replies	Number of ICMP time stamp reply packets received by the SB. 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 SB. 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.  <b>Note</b> 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 SB. 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.  <b>Note</b> 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 SB.
ICMP messages send failed	Total number of ICMP messages that failed to be sent by the SB.
Destination unreachable	Number of destination-unreachable ICMP packets sent by the SB.
Timeout in transit	Number of ICMP time-exceeded packets sent by the SB.
Wrong parameters	Number of ICMP packets with parameter problems sent by the SB.
Source quenches	Number of ICMP source-quench packets sent by the SB.
Redirects	Number of ICMP redirect packets sent by the SB.
Echo requests	Number of echo ICMP packets sent by the SB.

**Table 4-3** *show statistics icmp Field Descriptions (continued)*

<b>Field</b>	<b>Description</b>
Echo replies	Number of echo-reply ICMP packets sent by the SB.
Timestamp requests	Number of ICMP time stamp request packets sent by the SB.
Timestamp replies	Number of ICMP time stamp reply packets sent by the SB.
Address mask requests	Number of ICMP address mask requests sent by the SB.
Address mask replies	Number of ICMP address mask replies sent by the SB.

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>clear statistics</b>	Clears the statistics settings.

# show statistics ip

To display the IP statistics, use the **show statistics ip** command in user EXEC configuration mode.

## show statistics ip

**Syntax Description** This command has no arguments or keywords.

**Defaults** None

**Command Modes** User EXEC configuration mode.

**Examples** The following is sample output from the **show statistics ip** command:

```
ServiceRouter# show statistics ip

IP statistics
-----
Total packets in           = 1408126
  with invalid header      = 0
  with invalid address     = 0
  forwarded                = 0
  unknown protocol        = 0
  discarded                = 0
  delivered                = 1408126
Total packets out         = 1500110
  dropped                  = 0
  dropped (no route)      = 0
Fragments dropped after timeout = 0
Reassemblies required    = 0
Packets reassembled      = 0
Packets reassemble failed = 0
Fragments received       = 0
Fragments failed         = 0
Fragments created        = 0

ServiceRouter#
```

[Table 4-4](#) describes the fields shown in the **show statistics ip** display.

**Table 4-4** *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 4-4 *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 SB 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 SB 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 4-4 *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
<b>clear statistics ip</b>	Clears IP statistics counters.
<b>ip</b>	Configures the IP.
<b>show ip routes</b>	Displays the IP routing table.

## show statistics lsof

To display the List of Open File (lsof) descriptors, use the **show statistics lsof** command in EXEC configuration mode.

### show statistics lsof

**Syntax Description** This command has no arguments or keywords.

**Defaults** None

**Command Modes** EXEC configuration mode.

**Examples** The following example shows to display the lsof descriptors:

```
ServiceEngine# show statistics lsof
COMMAND      PID      USER    FD      TYPE          DEVICE    SIZE    NODE
NAME
init          1       admin   cwd     DIR           1,0      1024    2
/
init          1       admin   rtd     DIR           1,0      1024    2
/
init          1       admin   txt     REG           1,0      45436   7488
/sbin/init
init          1       admin   mem     REG           1,0     1852502 6566
/lib/libc-2.13.so
init          1       admin   mem     REG           1,0     154528  2006
/lib/ld-2.13.so
init          1       admin   10u    FIFO          0,13          4069
/dev/initctl
kthreadd     2       admin   cwd     DIR           1,0      1024    2
/
kthreadd     2       admin   rtd     DIR           1,0      1024    2
/
kthreadd     2       admin   txt     unknown
/proc/2/exe
migration    3       admin   cwd     DIR           1,0      1024    2
/
migration    3       admin   rtd     DIR           1,0      1024    2
/

<Output truncated>
```

## show statistics netstat

To display SB 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.

**Defaults** None

**Command Modes** EXEC configuration mode.

**Usage Guidelines** [Table 4-5](#) describes the fields shown in the **show statistics netstat** display.

*Table 4-5 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 SB 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.

**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
<b>clear statistics</b>	Clears the statistics settings.
<b>radius-server</b>	Configures the RADIUS authentication.
<b>show radius-server</b>	Displays the RADIUS server information.

## show statistics services

To display SB services statistics, use the **show statistics services** command in EXEC configuration mode.

### show statistics services

**Syntax Description** This command has no arguments or keywords.

**Defaults** None

**Command Modes** EXEC configuration mode.

**Usage Guidelines** [Table 4-6](#) describes the fields shown in the **show statistics services** display.

*Table 4-6 show statistics services Field Descriptions*

Field	Description
Port Statistics	Service-related statistics for each port on the WAAS <sup>1</sup> device.
Port	Port number.
Total Connections	Number of total connections.

1. WAAS = Wide Area Application Service

Related Commands	Command	Description
	<b>show services</b>	Displays the services-related information.

## show statistics snmp

To display SB 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.

**Defaults** None

**Command Modes** EXEC configuration mode.

**Usage Guidelines** [Table 4-7](#) describes the fields shown in the **show statistics snmp** display.

*Table 4-7 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 4-7 *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
<b>show snmp</b>	Displays the SNMP parameters.
<b>snmp-server community</b>	Configures the community access string to permit access to the SNMP.
<b>snmp-server contact</b>	Sets the system server contact string.
<b>snmp-server enable</b>	Enables the SB to send SNMP traps.
<b>snmp-server group</b>	Defines a user security model group.
<b>snmp-server host</b>	Specifies the hosts to receive SNMP traps.
<b>snmp-server location</b>	Sets the SNMP system location string.
<b>snmp-server notify inform</b>	Configures the SNMP notify inform request.
<b>snmp-server user</b>	Defines a user who can access the SNMP engine.

## show statistics tacacs

To display Service Broker 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.

**Defaults** None

**Command Modes** User EXEC configuration mode.

**Usage Guidelines** The fields shown in the **show statistics tacacs** display for the Service Broker 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
	<b>clear tacacs</b>	Clears the TACACS+ settings.
	<b>show tacacs</b>	Displays TACACS+ authentication protocol configuration information.
	<b>tacacs</b>	Configures TACACS+ server parameters.

## show statistics tcp

To display SB 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.

**Defaults** None

**Command Modes** EXEC configuration mode.

**Usage Guidelines** [Table 4-8](#) describes the fields shown in the **show statistics tcp** display.

*Table 4-8 show statistics tcp Field Descriptions*

Field	Description
Server connection openings	Number of connections opened from the SB to the server.
Client connection openings	Number of connections opened from the client to the SB.
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 <sup>1</sup> received by the SB.
Connection resets sent	Number of RSTs sent by the SB.
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 4-8 *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 SB from the server.
Server segments sent	Number of TCP segments sent by the SB to the server.
Server segments retransmitted	Number of TCP segments retransmitted by the SB from the server.
Client segments received	Number of TCP segments received by the SB from the client.
Client segments sent	Number of TCP segments sent by the SB to the server.
Client segments retransmitted	Number of TCP segments retransmitted by the SB to the client.
Sync cookies sent	Number of SYN <sup>2</sup> cookies sent by the SB. 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 SB. 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 SB. 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 SB accepted the connection.
Prune message called	Number of calls that the SB 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 4-8 *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 <sup>3</sup> not sent because they were meant for the SB.
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 <sup>4</sup> 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 SB.
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 4-8 *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 <sup>5</sup> 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 <i>additive increase and multiplicative decrease</i> . 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 SB 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 4-8 *show statistics tcp* Field Descriptions (continued)

Field	Description
TCP SACK renegeing	<p>Number of times that the SB 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.</p> <p>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.</p>
TCP FACK reorders	<p>Number of FACK<sup>6</sup> 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.</p>
TCP SACK reorders	Number of SACK <sup>7</sup> 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 <sup>8</sup> 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 4-8 *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 <sup>9</sup> shrunk because the SB 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 4-8 *show statistics tcp Field Descriptions (continued)*

Field	Description
TCP forward retransmissions	<p>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:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Number of retransmissions configured in maximum retransmissions per packet is reached.</li> </ul>
TCP slowstart retransmissions	<p>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.)</p>
TCP Timeouts	Number of times that a TCP timeout occurred.
TCP Reno recovery fail	<p>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.</p>
TCP Sack recovery fail	<p>Number of times that the SB 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.</p>
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 4-8 *show statistics tcp* Field Descriptions (continued)

Field	Description
TCP DSACK old packets sent	Number of D-SACKs sent by the SB. 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 SB. 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 SB. 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 SB. 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 4-8 *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
<b>clear statistics</b>	Clears the statistics settings.

# show statistics transaction-logs

To display SB 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.

**Defaults** None

**Command Modes** EXEC configuration mode.

**Usage Guidelines** To display the transaction log export statistics, you must first configure the FTP server.

[Table 4-9](#) describes the fields shown in the **show statistics transaction-logs** display.

**Table 4-9** *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 SB failed to open a connection to the FTP export server.
Initial Put Failures	Number of times that the SB 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 SB failed to open a connection to the FTP export server on a retry.
Retry Put Failures	Number of times that the SB failed to transfer a file to the FTP export server on a retry.
Authentication Failures	Number of times that the SB failed to authenticate with the FTP export server. This situation might occur if the SB is misconfigured with the wrong password for the FTP server or the password on the FTP server has been changed since the SB was configured.
Invalid Server Directory Failures	Number of times the SB failed to direct traffic to the correct server directory.

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>clear transaction-log</b>	Clears the working transaction logs settings.
<b>show transaction-logging</b>	Displays the transaction log configuration settings and a list of archived transaction log files.
<b>transaction-log force</b>	Forces the archive or export of the transaction log.

## show statistics udp

To display SB 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.

**Defaults** None

**Command Modes** EXEC configuration mode.

**Usage Guidelines** [Table 4-10](#) describes the fields shown in the **show statistics udp** display.

*Table 4-10 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 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.

**Defaults** None

**Command Modes** EXEC configuration mode.

**Usage Guidelines** The **show tacacs** command displays the TACACS+ configuration for the Service Broker. [Table 4-11](#) describes the fields shown in the **show tacacs** display.

*Table 4-11 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 Brokers 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 Broker.
Key	Secret key that the Service Broker 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 Broker waits for a response from the specified TACACS+ Authentication Server before declaring a timeout.
Retransmit	Number of times that the Service Broker 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 <sup>1</sup> is the mechanism for password authentication.

**Table 4-11** *show tacacs Field Descriptions (continued)*

<b>Field</b>	<b>Description</b>
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**

<b>Command</b>	<b>Description</b>
<b>clear tacacs</b>	Clears the TACACS+ settings.
<b>show statistics tacacs</b>	Displays the SB TACACS+ authentication and authorization statistics.
<b>tacacs</b>	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 {authentication | cms | kernel } | authentication }
```

Syntax Description		
<b>list-files</b>	(Optional)	Displays the list of files under a directory.
<i>directory_name</i>		Directory name (use absolute path, such as /local1/logs).
<b>recursive</b>		Specifies to include files in recursive sub-directories.
<b>page</b>	(Optional)	Specifies the pages through the output.
<b>service</b>	(Optional)	Displays technical support information specific to a service.
<b>authentication</b>		Displays technical support information related to HTTP authentication.
<b>cms</b>		Displays technical support information related to CMS.
<b>kernel</b>		Displays technical support information related to the kernel.

**Defaults** None

**Command Modes** EXEC configuration mode.

**Usage Guidelines** Use this command to view system information necessary for TAC to assist you with your SB. We recommend that you log the output to a disk file. Use the streaming option to view information specific to the streaming feature.

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

**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:

```
ServiceBroker# show tech-support
```

```
CPU Usage:
```

```
cpu: 0.39% User, 0.42% System, 0.33% User(nice), 98.86% Idle
cpu0: 0.39% User, 0.42% System, 0.33% User(nice), 98.86% Idle
```

```
-----
PID  STATE PRI  User T  SYS T      COMMAND
-----
   1   S    0   4386 1706 (init)
   2   S    0     0  0 (keventd)
   3   S   19     0  0 (ksoftirqd_CPU0)
   4   S    0     0  0 (kswapd)
   5   S    0     0  0 (bdflood)
   6   S    0     0  0 (kupdated)
   7   S    0     0  0 (scsi_ah_0)
  45   S    0   4733 4114 (nodemgr)
  46   S    0     0  0 (syslogd)
  47   R    0    83  65 (dataserver)
 920   S    0     0  0 (login)
1207   S    0     0  0 (parser_server)
1208   S    0     0  0 (eval_timer_man)
1211   S    0    46  1 (parser_server)
1443   S    0     0  0 (overload)
1444   S    0     0  0 (standby)
1445   S    0    13  29 (cache)
1446   S    0     0  0 (proxy_poll)
1447   S    0     0  0 (snmpcd)
1448   S    0     0  0 (http_authmod)
1458   S    0     0  0 (http_authmod)
1465   S    0     0  0 (http_authmod)
1466   S    0     0  0 (http_authmod)
1467   S    0     0  0 (http_authmod)
1537   S    0     0  0 (cache)
1538   S    0     0  0 (unified_log)
1540   S    0     0  1 (webserver)
1541   S    0     2  2 (mcm)
1542   S    0     0  0 (cache)
1543   S    0     0  0 (cache)
1550   S    0     0  0 (cache)
1551   S    0     0  0 (cache)
1556   S    0     0  0 (cache)
1567   S    0     0  0 (mcm)
1568   S    0     0  0 (mcm)
1629   S    0  18982 4140 (crond)
1936   S    0   1669  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_man)
1211	S	0	0.3	4980736	847	(parser_server)
1443	S	0	0.0	1548288	154	(overload)
1444	S	0	0.0	1724416	161	(standby)
1445	S	0	5.9	65646592	15266	(cache)
1446	S	0	0.0	1957888	173	(proxy_poll)
1447	S	0	0.1	2097152	290	(snmpcd)
1448	S	0	0.0	1757184	205	(http_authmod)
1458	S	0	0.0	1757184	205	(http_authmod)
1465	S	0	0.0	1757184	205	(http_authmod)
1466	S	0	0.0	1757184	205	(http_authmod)
1467	S	0	0.0	1757184	205	(http_authmod)
1537	S	0	5.9	65646592	15266	(cache)
1538	S	0	0.0	1789952	169	(unified_log)
1540	S	0	0.4	10817536	1164	(webserver)
1541	S	0	0.0	2150400	251	(mcm)
1542	S	0	5.9	65646592	15266	(cache)
1543	S	0	5.9	65646592	15266	(cache)
1550	S	0	5.9	65646592	15266	(cache)
1551	S	0	5.9	65646592	15266	(cache)

```

1556      S      0 5.9 65646592      15266 (cache)
1567      S      0 0.0 2150400      251 (mcm)
1568      S      0 0.0 2150400      251 (mcm)
1629      S      0 0.0 1187840      137 (crond)
1936      S      0 0.6 7532544      1605 (bootnet)
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.

---

**Defaults** Enabled.

---

**Command Modes** EXEC configuration mode.

---

**Examples** The following example shows how to display the Telnet service details:

```
ServiceBroker# show telnet
telnet service is enabled
```

---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>exec-timeout</b>	Configures the length of time that an inactive Telnet or SSH session remains open.
	<b>telnet enable</b>	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.

**Defaults** None

**Command Modes** EXEC configuration mode.

**Usage Guidelines** To display information about the current configuration of transaction logging on an SB, 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 SB:

```
ServiceBroker# show transaction-logging
Transaction log configuration:
-----
Logging is enabled.
Archive interval: 1800 seconds
Maximum size of archive file: 2000000 KB
Maximum number of archive files: 50 files
Log File format is apache.
Windows domain is not logged with the authenticated username

Exporting files to ftp servers is enabled.
File compression is disabled.
Export interval: 30 minutes

server          type  username      directory
10.77.153.110   ftp   root          /var/ftp/test

WMT MMS Caching Proxy/Server Transaction Log File Info
  Working Log file - size : 556
                   age: 483497
  Archive Log file - mms_export_3.1.18.8_20090522_074807      size: 556

WMT MMS Caching Proxy/Server Transaction Log File Info (WMS-90 format)
  Working Log file - size : 665
                   age: 483497
  Archive Log file - mms_export_wms_90_3.1.18.8_20090522_074807 size: 665

WMT MMS Caching Proxy/Server Transaction Log File Info (Ext. WMS-90 format)
  Working Log file - size : 702
```

```

    age: 483497
Archive Log file - mms_export_e_wms_90_3.1.18.8_20090522_074807    size: 70
2

WMT MMS Caching Proxy/Server Transaction Log File Info (Ext. WMS-41 format)
Working Log file - size : 584
    age: 483497
Archive Log file - mms_export_e_wms_41_3.1.18.8_20090522_074807    size: 58
4

A&D Transaction Log File Info
Working Log file - size : 138
    age: 483497
Archive Log file - acqdist_3.1.18.8_20090522_074807    size: 138
Movie Streamer Transaction Log File Info
Working Log file - size : 488
    age: 482196
Archive Log file - movie-streamer_3.1.18.8_20090522_062602    size: 648
Archive Log file - movie-streamer_3.1.18.8_20090522_064309    size: 805
Archive Log file - movie-streamer_3.1.18.8_20090522_065857    size: 645
Archive Log file - movie-streamer_3.1.18.8_20090522_070038    size: 648
Archive Log file - movie-streamer_3.1.18.8_20090522_074807    size: 645
Archive Log file - movie-streamer_3.1.18.8_20090522_080016    size: 648
Archive Log file - movie-streamer_3.1.18.8_20090523_030829    size: 645
ICAP Transaction Log File Info
Working Log file - size : 61
    age: 483496
Archive Log file - icap_3.1.18.8_20090522_074807    size: 61

Web Engine Transaction Log File Info - Apache format
Working Log file - size : 86
    age: 483497
Archive Log file - we_accesslog_apache_3.1.18.8_20090522_074807    size: 82

Web Engine Transaction Log File Info - CLF format
Working Log file - size : 3
    age: 483497
Archive Log file - we_accesslog_clf_3.1.18.8_20090522_074807    size: 3

Web Engine Transaction Log File Info - Extended Squid format
Working Log file - size : 102
    age: 483497
Archive Log file - we_accesslog_extsqu_3.1.18.8_20090522_074807    size: 10
2

Cached Content Log File Info
Working Log file - size : 41
    age: 483496
Archive Log file - cache_content_3.1.18.8_20090522_074807    size: 41

Flash Media Streaming Access Transaction Log File Info
Working Log file - size : 36
    age: 482196
Archive Log file - fms_access_3.1.18.8_20090522_062602    size: 650
Archive Log file - fms_access_3.1.18.8_20090522_064309    size: 509
Archive Log file - fms_access_3.1.18.8_20090522_065857    size: 650
Archive Log file - fms_access_3.1.18.8_20090522_074807    size: 509
Archive Log file - fms_access_3.1.18.8_20090522_080016    size: 509
Archive Log file - fms_access_3.1.18.8_20090523_030830    size: 650

Flash Media Streaming Authorization Transaction Log File Info
Working Log file - size : 43
    age: 482196
Archive Log file - fms_auth_3.1.18.8_20090522_062602    size: 4826

```

## show transaction-logging

```

Archive Log file - fms_auth_3.1.18.8_20090522_063036 size: 281
Archive Log file - fms_auth_3.1.18.8_20090522_064309 size: 596
Archive Log file - fms_auth_3.1.18.8_20090522_065857 size: 4789
Archive Log file - fms_auth_3.1.18.8_20090522_070038 size: 277
Archive Log file - fms_auth_3.1.18.8_20090522_074807 size: 596
Archive Log file - fms_auth_3.1.18.8_20090523_030830 size: 4790

```

### Authserver Transaction Log File Info

```

Working Log file - size : 108
                  age: 483496
Archive Log file - authsvr_3.1.18.8_20090522_065857 size: 108

```

ServiceBroker#

The following example shows how to display information about the current configuration of transaction logging on an SB:

ServiceBroker# **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 Broker Log File Info

```

Working Log file - size : 96
                  age: 169813
Archive Log file - service_broker_3.1.14.70_20090421_222006 size: 256
Archive Log file - service_broker_3.1.14.70_20090422_020038 size: 223
Archive Log file - service_broker_3.1.14.70_20090422_210022 size: 351
Archive Log file - service_broker_3.1.14.70_20090423_020006 size: 1248
Archive Log file - service_broker_3.1.14.70_20090423_210021 size: 456
Archive Log file - service_broker_3.1.14.70_20090521_000218 size: 402
Archive Log file - service_broker_3.1.14.70_20090521_014815 size: 243
Archive Log file - service_broker_3.1.14.70_20090521_015020 size: 225
Archive Log file - service_broker_3.1.14.70_20090521_015227 size: 243
Archive Log file - service_broker_3.1.14.70_20090521_015417 size: 272
Archive Log file - service_broker_3.1.14.70_20090521_015601 size: 390
Archive Log file - service_broker_3.1.14.70_20090521_015816 size: 243
Archive Log file - service_broker_3.1.14.70_20090521_020033 size: 243
Archive Log file - service_broker_3.1.14.70_20090521_020249 size: 143
Archive Log file - service_broker_3.1.14.70_20090521_032633 size: 168
Archive Log file - service_broker_3.1.14.70_20090526_025027 size: 143
Archive Log file - service_broker_3.1.14.70_20090526_030002 size: 176
Archive Log file - service_broker_3.1.14.70_20090526_030226 size: 250
Archive Log file - service_broker_3.1.14.70_20090526_052206 size: 250
Archive Log file - service_broker_3.1.14.70_20090526_052413 size: 143
Archive Log file - service_broker_3.1.14.70_20090526_200213 size: 168
Archive Log file - service_broker_3.1.14.70_20090526_200413 size: 481
Archive Log file - service_broker_3.1.14.70_20090526_200645 size: 173
Archive Log file - service_broker_3.1.14.70_20090526_201010 size: 250

```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>clear transaction-log</b>	Clears the working transaction log settings.
	<b>show statistics transaction-logs</b>	Displays the SB transaction log export statistics.
	<b>transaction-log force</b>	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.

**Defaults** None

**Command Modes** EXEC configuration mode.

**Examples** The following example shows how to display the URL signature information:

```
key-id-owner  key-id-number  key  public-key  private-key  symmetric-key
-----
                1                1          ****          ****          ****
```

# 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

<b>uid</b>	Displays the user's identification number.
<i>num</i>	Identification number. The range is from 0 to 65535.
<b>username</b>	Displays the name of user.
<i>name</i>	Name of the user.

## Defaults

None

## Command Modes

EXEC configuration mode.

## Usage Guidelines

[Table 4-12](#) describes the fields shown in the **show user** display.

*Table 4-12 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
<b>clear user</b>	Clears the user settings.
<b>show users</b>	Displays the specified users.
<b>username</b>	Establishes the username authentication.

# show users

To display users, use the **show users** command in EXEC configuration mode.

## **show users administrative**

<b>Syntax Description</b>	<b>administrative</b>	Lists users with administrative privileges.
---------------------------	-----------------------	---

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	EXEC configuration mode.
----------------------	--------------------------

**Examples** The following example shows how to display the list of users with administrative privileges:

```
ServiceBroker# show users administrative
                UID USERNAME
                0 admin
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>clear user</b>	Clears the user settings.
	<b>show user</b>	Displays the user identification number and username information for a particular user.
	<b>username</b>	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

<b>Syntax Description</b>	<b>pending</b>	Displays the version for pending upgraded image.
<b>Defaults</b>	None	
<b>Command Modes</b>	EXEC configuration mode.	
<b>Usage Guidelines</b>	Table 4-13 describes the fields shown in the <b>show version</b> display.	

*Table 4-13 show version Field Descriptions*

Field	Description
Version	VDS-SB 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 VDS-SB software on an SB, 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:

```
ServiceBroker# show version
VDS Service Broker Software
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/vosis_release_builds/vosis_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.
```

## ■ show version

```
ServiceBroker#
```

The following example shows how to display the pending software version:

```
ServiceBroker# show version pending  
Pending version is VDS-SB 3.0.0-b360, built on 05:17:52 Jun 19 2011 by ipvbuild  
It will take effect after reload  
ServiceBroker#
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show flash</b>	Displays the flash memory version and usage information.

---

# 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.

**Defaults** None

**Command Modes** Interface configuration (config-if) mode.

**Usage Guidelines** See the [“interface” section on page 2-85](#) for alternative mechanism.

**Examples** The following example shows how to shut down an interface configured on an SB:

```
ServiceBroker(config-if)# shutdown
```

Related Commands	Command	Description
	<b>interface</b>	Configures a Gigabit Ethernet or port channel interface.
	<b>show interface</b>	Displays the hardware interface information.
	<b>show running-config</b>	Displays the current operating configuration.
	<b>show startup-config</b>	Displays the startup configuration.

## shutdown (EXEC Configuration)

To shut down the SB or VDSM, use the **shutdown** command in EXEC configuration mode.

**shutdown [poweroff]**

<b>Syntax Description</b>	<b>poweroff</b> (Optional) Turns off the power after closing all applications and the operating system.
<b>Defaults</b>	None
<b>Command Modes</b>	EXEC configuration mode.
<b>Usage Guidelines</b>	<p>A controlled shutdown refers to the process of properly shutting down an SB 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 SB but the power is still on. Controlled shutdowns of an SB can help you minimize the downtime when the SB is being serviced.</p> <p>The <b>shutdown</b> command enables you to shut down and optionally power off an SB:</p> <ul style="list-style-type: none"> <li>• <i>Shutdown</i> means that all application activities (applications and operating system) are stopped, but the power is still on. This shutdown is similar to the Linux <b>halt</b> command.</li> <li>• <i>Shutdown poweroff</i> means that the SB is powered down by the VDS-SB 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.</li> </ul>
 <b>Caution</b>	If you do not perform a controlled shutdown, the SB file system can be corrupted. It also takes longer to reboot the SB if the SB is not properly shut down.
 <b>Note</b>	You cannot power on SBs again through software after a software poweroff operation. You must press the power button once on these SBs to bring these SBs back online.
	<p>The <b>shutdown</b> command facilitates a proper shutdown for SBs, or VDSMs. Where the <b>shutdown</b> command is supported on all content networking hardware models, the <b>shutdown poweroff</b> command is supported only on those models that support ACPI.</p>

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 SB using a console to display the following menu:

```
ServiceBroker# 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 Broker 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 4-14](#) describes the shutdown and shutdown power-off operations for SBs.

Table 4-14 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 SB	ServiceBroker# <b>shutdown</b>	ServiceBroker# <b>shutdown poweroff</b>
User intervention to bring SB back online	To bring an SB that has an on/off switch on the back online after a shutdown operation, flip the on/off switch twice.  To bring an SB 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 SB back online.
File system check	Is not performed after you turn the power on again and reboot the SB.	Is not performed after you turn the power on again and reboot the SB.

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 SB.

To perform a shutdown on an SB, enter the **shutdown** command as follows:

```
ServiceBroker# 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 SB:

```
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 VDS-SB 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 4-15** *show statistics wmt all Field Descriptions*

Field	Description
<b>Unicast Requests Statistics</b>	
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.
<b>By Type of Content</b>	
Live content	Number of live content requests received.
On-Demand Content	Number of on-demand content requests received.
<b>By Transport Protocol</b>	
HTTP	Number of HTTP requests received.
RTSPT	Number of RTSPT requests received.
RTSPU	Number of RTSPU requests received.
<b>Unicast Savings Statistics</b>	
Total bytes saved	Total number of bytes saved.
<b>By Source of Content</b>	
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.
<b>CDN-Related WMT Requests</b>	
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 4-15 *show statistics wmt all Field Descriptions (continued)*

Field	Description
CDN Content Errors	Number of CDN content request errors.
<b>Fast Streaming-related WMT Requests</b>	
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.
<b>Authenticated Requests</b>	
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.
<b>Unicast Bytes Statistics</b>	
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.
<b>Unicast Savings Statistics</b>	
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 4-15 *show statistics wmt all Field Descriptions (continued)*

Field	Description
<b>Caching</b>	
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.
<b>Usage Summary</b>	
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.
<b>Error Statistics</b>	
Total request errors	Total number of request errors.
Errors generated by this box	Number of request errors generated by this device.

Table 4-15 *show statistics wmt all Field Descriptions (continued)*

Field	Description
Errors generated by remote servers	Number of request errors generated by remote servers.
<b>Other Statistics</b>	
Authentication Retries from Clients	Number of authentication retries from clients.
<b>WMT Rule Template Statistics</b>	
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.
<b>Multicast Statistics</b>	
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 SB, press and hold the power button on the SB, 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 SB CLI, enter the **shutdown poweroff** command as follows:

```
ServiceBroker# 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:

```
ServiceBroker1# 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 SB:

```
ServiceBroker2# shutdown poweroff  
System configuration has been modified. Save? [ yes ] :yes  
Device can not be powered on again through software after poweroff.  
Proceed with poweroff? [ confirm ]  
Shutting down all services, will timeout in 15 minutes.  
poweroff in progress ..Power down.
```

# snmp-server community

To configure the community access string to permit access to the Simple Network Management Protocol (SNMP), use the **snmp-server community** command in Global configuration mode. To remove the specified community string, use the **no** form of this command.

**snmp-server community** *community\_string* [**group** *group\_name* | **rw**]

**no snmp-server community** *community\_string* [**group** *group\_name* | **rw**]

## Syntax Description

<i>community_string</i>	Community string that acts like a password and permits access to SNMP.
<b>group</b>	(Optional) Specifies the group to which this community name belongs.
<i>group_name</i>	(Optional) Name of the group.
<b>rw</b>	(Optional) Specifies read-write access with this community string.

## Defaults

An SNMP community string permits read-only access to all MIB objects.

A community string is assigned to the Secure Domain Router (SDR) owner.

## Command Modes

Global configuration (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:

```
ServiceBroker(config)# snmp-server community comaccess rw
```

The following example shows how to remove the community comaccess:

```
ServiceBroker(config)# no snmp-server community comaccess
```

## Related Commands

Command	Description
<b>snmp-server view</b>	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	<i>line</i>	Identification of the contact person for this managed node.
--------------------	-------------	---

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:
----------	---

```
ServiceBroker(config)# snmp-server contact Dial System Operator at beeper # 27345
```

Examples	The following example shows how to reset the system contact string:
----------	---

```
ServiceBroker(config)# no snmp-server contact
```

Related Commands	Command	Description
	<b>show snmp</b>	Displays the SNMP parameters.
	<b>snmp-server community</b>	Configures the community access string to permit access to the SNMP.
	<b>snmp-server enable traps</b>	Enables the SB to send SNMP traps.
	<b>snmp-server group</b>	Defines a user security model group.
	<b>snmp-server host</b>	Specifies the hosts to receive SNMP traps.
	<b>snmp-server location</b>	Sets the SNMP system location string.
	<b>snmp-server notify inform</b>	Configures the SNMP notify inform request.
	<b>snmp-server user</b>	Defines a user who can access the SNMP engine.
	<b>snmp-server view</b>	Defines a SNMPv2 MIB view.

## snmp-server enable traps

To enable the SB 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-broker [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-broker [disk-fail | disk-read |
disk-write | transaction-log] | snmp [authentication | cold-start]]
```

Syntax	Description
<b>alarm</b>	(Optional) Enables SB alarm traps.
<b>clear-critical</b>	(Optional) Enables the clear-critical alarm trap.
<b>clear-major</b>	(Optional) Enables the clear-major alarm trap.
<b>clear-minor</b>	(Optional) Enables the clear-minor alarm trap.
<b>raise-critical</b>	(Optional) Enables the raise-critical alarm trap.
<b>raise-major</b>	(Optional) Enables the raise-major alarm trap.
<b>raise-minor</b>	(Optional) Enables the raise-minor alarm trap.
<b>config</b>	(Optional) Enables CiscoConfigManEvent traps.
<b>entity</b>	(Optional) Enables SNMP entity traps.
<b>event</b>	(Optional) Enables Event MIB traps.
<b>service-broker</b>	(Optional) Enables SNMP SB traps.
<b>disk-fail</b>	(Optional) Enables the disk failure error trap.
<b>disk-read</b>	(Optional) Enables the disk read error trap.
<b>disk-write</b>	(Optional) Enables the disk write error trap.
<b>transaction-log</b>	(Optional) Enables the transaction log write error trap.
<b>snmp</b>	(Optional) Enables SNMP-specific traps.
<b>authentication</b>	(Optional) Enables the authentication trap.
<b>cold-start</b>	(Optional) Enables the cold-start trap.

### Defaults

This command is disabled by default. No traps are enabled.

### Command Modes

Global configuration (config) mode.

### Usage Guidelines

You can configure an SB to generate an SNMP trap for a specific alarm condition. You can configure the generation of SNMP alarm traps on SBs based on the following:

- Severity of the alarm (critical, major, or minor)
- Action (the alarm is raised or cleared)

Cisco VDS Service Broker 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 SB 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 SB 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 SB to send all traps to the host 172.31.2.160 using the community string public:

```
ServiceBroker(config)# snmp-server enable traps
ServiceBroker(config)# snmp-server host 172.31.2.160 public
```

The following example disables all traps:

```
ServiceBroker(config)# no snmp-server enable traps
```

**Related Commands**

Command	Description
<b>show snmp</b>	Displays the SNMP parameters.
<b>snmp-server community</b>	Configures the community access string to permit access to the SNMP.
<b>snmp-server contact</b>	Sets the system server contact string.
<b>snmp-server group</b>	Defines a user security model group.
<b>snmp-server host</b>	Specifies the hosts to receive SNMP traps.
<b>snmp-server location</b>	Sets the SNMP system location string.
<b>snmp-server notify inform</b>	Configures the SNMP notify inform request.
<b>snmp-server user</b>	Defines a user who can access the SNMP engine.
<b>snmp-server view</b>	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		
<i>name</i>		Name of the SNMP group. Supports up to a maximum of 64 characters.
<b>v1</b>		Specifies the group using the Version 1 Security Model.
<b>notify</b>		(Optional) Specifies a notify view for the group that enables you to specify a notify, inform, or trap.
<i>name</i>		Notify view name. Supports up to a maximum of 64 characters.
<b>read</b>		(Optional) Specifies a read view for the group that enables you only to view the contents of the agent.
<i>name</i>		Read view name. Supports up to a maximum of 64 characters.
<b>write</b>		(Optional) Specifies a write view for the group that enables you to enter data and configure the contents of the agent.
<i>name</i>		Write view name. Supports up to a maximum of 64 characters.
<b>v2c</b>		Specifies the group using the Version 2c Security Model.
<b>v3</b>		Specifies the group using the User Security Model (SNMPv3).
<b>auth</b>		Specifies the group using the AuthNoPriv Security Level.
<b>noauth</b>		Specifies the group using the noAuthNoPriv Security Level.
<b>priv</b>		Specifies the group using the AuthPriv Security Level.

**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 VDS Service Broker 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 SBs 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 SB'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 SB:

```
ServiceBroker(config)# snmp-server group acme v1 notify mymib
```

**Related Commands**

Command	Description
<b>show snmp</b>	Displays the SNMP parameters.
<b>snmp-server community</b>	Configures the community access string to permit access to the SNMP.
<b>snmp-server contact</b>	Sets the system server contact string.
<b>snmp-server enable traps</b>	Enables the SB to send SNMP traps.
<b>snmp-server host</b>	Specifies the hosts to receive SNMP traps.
<b>snmp-server location</b>	Sets the SNMP system location string.
<b>snmp-server notify inform</b>	Configures the SNMP notify inform request.
<b>snmp-server user</b>	Defines a user who can access the SNMP engine.
<b>snmp-server view</b>	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		
<i>hostname</i>	Hostname of the SNMP trap host that is sent in the SNMP trap messages from the SB.	
<i>ip_address</i>	IP address of the SNMP trap host that is sent in the SNMP trap messages from the SB.	
<i>communitystring</i>	Password-like community string sent in the SNMP trap messages from the SB. You can enter a maximum of 64 characters.	
<b>v2c</b>	(Optional) Specifies the Version 2c Security Model.	
<b>retry</b>	(Optional) Sets the count for the number of retries for the inform request. (The default is 2 tries.)	
<i>number</i>	Number of retries for the inform request. The range is from 1 to 10.	
<b>timeout</b>	(Optional) Sets the timeout for the inform request. The default is 15 seconds.	
<i>seconds</i>	Timeout value, in seconds. The range is from 1 to 1000.	
<b>v3</b>	(Optional) Specifies the User Security Model (SNMPv3).	
<b>auth</b>	Sends notification using the AuthNoPriv Security Level.	
<b>noauth</b>	Sends notification using the noAuthNoPriv Security Level.	
<b>priv</b>	Sends notification using the AuthPriv Security Level.	

### Defaults

This command is disabled by default. No traps are sent. The version of the SNMP protocol used to send the traps is SNMP Version 1.

**retry number:** 2

**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. Inform requests are more likely to reach their intended destination.

However, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in the memory until a response is received or the request times out. Also, traps are sent only once, while an inform may be retried several times. The retries increase traffic and contribute to a higher overhead on the network.

If you do not enter an **snmp-server host** command, no notifications are sent. To configure the SB 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:

```
ServiceBroker(config)# snmp-server enable traps
ServiceBroker(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:

```
ServiceBroker(config)# no snmp-server host 172.16.2.160
```

#### Related Commands

Command	Description
<b>show snmp</b>	Displays the SNMP parameters.
<b>snmp-server community</b>	Configures the community access string to permit access to the SNMP.
<b>snmp-server contact</b>	Sets the system server contact string.
<b>snmp-server enable traps</b>	Enables the SB to send SNMP traps.
<b>snmp-server group</b>	Defines a user security model group.
<b>snmp-server location</b>	Sets the SNMP system location string
<b>snmp-server notify inform</b>	Configures the SNMP notify inform request.
<b>snmp-server user</b>	Defines a user who can access the SNMP engine.
<b>snmp-server view</b>	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	<i>line</i>	String that describes the physical location of this node.
--------------------	-------------	---

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 <b>show snmp</b> command.
------------------	---

Examples	The following example shows how to configure a system location string:
----------	--

```
ServiceBroker(config)# snmp-server location Building 3/Room 214
```

Related Commands	Command	Description
	<b>show snmp</b>	Displays the SNMP parameters.
	<b>snmp-server community</b>	Configures the community access string to permit access to the SNMP.
	<b>snmp-server contact</b>	Sets the system server contact string.
	<b>snmp-server enable traps</b>	Enables the SB to send SNMP traps.
	<b>snmp-server group</b>	Defines a user security model group.
	<b>snmp-server host</b>	Specifies the hosts to receive SNMP traps.
	<b>snmp-server notify inform</b>	Configures the SNMP notify inform request.
	<b>snmp-server user</b>	Defines a user who can access the SNMP engine.
	<b>snmp-server view</b>	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.

---

**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 SBs to send inform requests to SNMP managers. SBs can send notifications to SNMP managers when particular events occur. For example, an agent SB might send a message to a manager when the agent SB 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 SB 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 SB 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 SB:

```
ServiceBroker(config)# snmp-server notify inform
```

**Related Commands**

Command	Description
<b>show snmp</b>	Displays the SNMP parameters.
<b>snmp-server community</b>	Configures the community access string to permit access to the SNMP.
<b>snmp-server contact</b>	Sets the system server contact string.
<b>snmp-server enable traps</b>	Enables the SB to send SNMP traps.
<b>snmp-server group</b>	Defines a user security model group.
<b>snmp-server host</b>	Specifies the hosts to receive SNMP traps.
<b>snmp-server location</b>	Sets the SNMP system location string.
<b>snmp-server user</b>	Defines a user who can access the SNMP engine.
<b>snmp-server view</b>	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
<i>name</i>	Name of the SNMP user. Use letters, numbers, dashes, and underscores, but no blanks. This is the name of the user on the SNMP host who wants to communicate with the SNMP agent on the SB. You can enter a maximum of 64 characters.
<i>group</i>	Name of the group to which the SNMP user belongs. You can enter a maximum of 64 characters.
<b>auth</b>	(Optional) Configures user authentication parameters.
<b>md5</b>	Configures the Hashed-Based Message Authentication Code Message Digest 5 (HMAC MD5) authentication algorithm.
<i>password</i>	HMAC MD5 user authentication password.
<b>priv</b>	(Optional) Configures authentication parameters for the packet.
<i>password</i>	HMAC MD5 user private password. You can enter a maximum of 256 characters.
<b>sha</b>	Configures the HMAC Secure Hash Algorithm (SHA) authentication algorithm.
<i>password</i>	HMAC SHA authentication password. You can enter a maximum of 256 characters.
<b>remote</b>	(Optional) Specifies the engine identity of the remote SNMP entity to which the user belongs.
<i>octet_string</i>	Globally unique identifier for a remote SNMP entity (for example, the SNMP network management station) for at least one of the SNMP users.

**Defaults** 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 SBs:

- If SNMPv3 is going to be used for SNMP requests, define at least one SNMPv3 user account on the SB for the SB 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 SB. 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 SB. 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 SB does not perform authentication on SNMP requests from this user.

```
ServiceBroker(config)# snmp-server user acme admin
```

**Related Commands**

Command	Description
<b>show snmp</b>	Displays the SNMP parameters.
<b>snmp-server community</b>	Configures the community access string to permit access to the SNMP.
<b>snmp-server contact</b>	Sets the system server contact string.
<b>snmp-server enable traps</b>	Enables the SB to send SNMP traps.
<b>snmp-server group</b>	Defines a user security model group.
<b>snmp-server host</b>	Specifies the hosts to receive SNMP traps.
<b>snmp-server location</b>	Sets the SNMP system location string.
<b>snmp-server notify inform</b>	Configures the SNMP notify inform request.
<b>snmp-server view</b>	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.
	<b>excluded</b>	Excludes the MIB family from the view.
	<b>included</b>	Includes the MIB family from the view.

**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:

```
ServiceBroker(config)# snmp-server view contentview ciscoServiceBrokerMIB 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:

```
ServiceBroker(config)# snmp-server view phred system included
ServiceBroker(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:

```
ServiceBroker(config)# snmp-server view agon system included
ServiceBroker(config)# snmp-server view agon system.7 excluded
```

## Related Commands

Command	Description
<b>show snmp</b>	Displays the SNMP parameters.
<b>snmp-server community</b>	Configures the community access string to permit access to the SNMP.
<b>snmp-server contact</b>	Sets the system server contact string.
<b>snmp-server enable traps</b>	Enables the SB to send SNMP traps.
<b>snmp-server group</b>	Defines a user security model group.
<b>snmp-server host</b>	Specifies the hosts to receive SNMP traps.
<b>snmp-server location</b>	Sets the SNMP system location string.
<b>snmp-server notify inform</b>	Configures the SNMP notify inform request.
<b>snmp-server user</b>	Defines a user who can access the SNMP engine.

## SS

To dump socket statistics, use the **ss** command in EXEC configuration mode.

*ss line*

<b>Syntax Description</b>	<i>line</i> ss connection information, -h to get help.
---------------------------	--

<b>Command Defaults</b>	None
-------------------------	------

<b>Command Modes</b>	EXEC configuration.
----------------------	---------------------

<b>Usage Guidelines</b>	The <b>ss</b> utility is used to dump socket statistics. It shows information similar to the <b>netstat</b> 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.

```
ServiceBroker# 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
  -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:

```
ServiceBroker# ss -t -a
```

The following command shows how to display all UDP sockets:

```
ServiceBroker# ss -u -a
```

The following command shows how to display all established SSH connections and display the timer information:

```
ServiceBroker# 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:

```
ServiceBroker# ss -o state established '(dport = :http or sport = :http)'
```

### Related Commands

Command	Description
<b>gulp</b>	Captures lossless gigabit packets and writes them to disk.
<b>netmon</b>	Displays the transmit and receive activity on an interface.
<b>netstatr</b>	Displays the rate of change of netstat statistics.
<b>tcpmon</b>	Searches all TCP connections.

# ssh-key-generate

To generate the SSH host key, use the **ssh-key-generate** command in Global configuration mode. To disable the SSH key, use the **no** form of this command.

**ssh-key-generate** [**key-length** *num*]

**no ssh-key-generate** [**key-length** *num*]

Syntax Description	key-length	Configures the length of SSH key.
	<i>num</i>	Specifies the number of bits in the SSH key to create.

**Defaults** **key-length** *bits*: 2048

**Command Modes** Global configuration (config) mode.

**Usage Guidelines** SSH enables login access to the SB 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 VDS-SB 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 SB, SFTP support is not available.

**Examples** The following example shows how to generate an SSH host key on an SB:

```
ServiceBroker(config)# ssh-key-generate key-length 2048
```

The following example disables the ssh host key:

```
ServiceBroker(config)# no ssh-key-generate key-length 2048
```

Related Commands	Command	Description
	<b>show ssh</b>	Displays the SSH status and configuration.

# 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		
<b>enable</b>		Enables the SSH feature.
<b>timeout</b>		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.
	<b>Note</b>	If you have established an SSH connection to the SB but have not entered the username when prompted at the login prompt, the connection is terminated by the SB even after successful login if the grace period expires.
	<i>seconds</i>	SSH login grace time value, in seconds. The range is from 1 to 99999. The default is 300.
<b>version</b>		Configures the SSH version to be supported on the SB.
<b>1</b>		Specifies that SSH Version 1 is supported on the SB.
<b>2</b>		Specifies that SSH Version 2 is supported on the SB.

## 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 SB 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 VDS-SB 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 SB, 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 VDS-SB software enables support for both SSH Version 1 and SSH Version 2 on the SB. If you want the SB 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 SB, 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 SB. Use the **no sshd enable** command in Global configuration mode to disable SSH on the SB.

**Examples**

The following example shows how to enable the SSH daemon and configure the number of allowable password guesses and timeout for the SB:

```
ServiceBroker(config)# sshd enable
ServiceBroker(config)# sshd password-guesses 4
ServiceBroker(config)# sshd timeout 20
```

The following example disables the support for SSH Version 1 in the SB:

```
ServiceBroker(config)# no sshd version 1
```

**Related Commands**

Command	Description
<b>show ssh</b>	Displays the SSH status and configuration.

# sysreport

To save the sysreport to a user-specified file, use the **sysreport** privilege command in EXEC configuration mode.

```
sysreport { authentication [date-range start_date end_date | filename] | cms [date-range
start_date end_date | filename] | dns | ftp | http | icap }
```

Syntax Description		
<b>authentication</b>		Generates sysreport information related to http authentication.
<b>cms</b>		Generates sysreport information related to Centralized Management System (CMS).
<b>dns</b>		Generates sysreport information related to Domain Name Server (DNS).
<b>ftp</b>		Generates sysreport information related to FTP.
<b>http</b>		Generates sysreport information related to HTTP.
<b>icap</b>		Generates sysreport information related to ICAP

**Defaults** None

**Command Modes** Privilege EXEC configuration mode.

**Examples** The following example saves the sysreport for WMT to a user-specified file:

```
ServiceBroker# 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

<b>host</b>	Sets a server address.
<i>hostname</i>	Hostname of the TACACS+ server.
<i>ip_address</i>	IP address of the TACACS+ server.
<b>primary</b>	(Optional) Sets the server as the primary server.
<b>key</b>	Sets the security word.
<i>keyword</i>	Keyword. An empty string is the default.
<b>password ascii</b>	Specifies ASCII as the TACACS+ password type.
<b>retransmit</b>	Sets the number of times that requests are retransmitted to a server.
<i>retries</i>	Number of retry attempts allowed. The range is from 1 to 3. The default is 2.
<b>timeout</b>	Sets the number of seconds to wait before a request to a server is timed out.
<i>seconds</i>	Timeout, in seconds. The range is from 1 to 20. The default is 5.

## 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:

```
ServiceBroker(config)# authentication login tacacs enable
ServiceBroker(config)# authentication configuration tacacs enable
```

HTTP request authentication is independent of user authentication options and must be disabled with the following separate commands:

```
ServiceBroker(config)# no authentication login tacacs enable
ServiceBroker(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 Broker 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 Broker 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 Broker 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 Broker, 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 Broker. 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:

```
ServiceBroker(config)# tacacs key human789
```

The following example shows how to configure the host named spearhead as the primary TACACS+ server:

```
ServiceBroker(config)# tacacs host spearhead primary
```

The following example shows how to set the timeout interval for the TACACS+ server:

```
ServiceBroker(config)# tacacs timeout 10
```

The following example shows how to set the number of times that authentication requests are retried (retransmitted) after a timeout:

```
ServiceBroker(config)# tacacs retransmit 5
```

The following example shows the password type to be PAP by default:

```
ServiceBroker# 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
ServiceBroker#
```

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:

```
ServiceBroker(config)# tacacs password ascii
ServiceBroker(config)# exit
ServiceBroker# 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
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show authentication</b>	Displays the authentication configuration.
	<b>show statistics tacacs</b>	Displays the Service Broker TACACS+ authentication and authorization statistics.
	<b>show tacacs</b>	Displays TACACS+ authentication protocol configuration information.

# tcpdump

To dump the network traffic, use the **tcpdump** command in EXEC configuration mode.

**tcpdump** [*LINE*]

<b>Syntax Description</b>	<i>LINE</i> (Optional) Dump options.
<b>Defaults</b>	None
<b>Command Modes</b>	EXEC configuration mode.
<b>Usage Guidelines</b>	Use the <b>tcpdump</b> command to gather a sniffer trace on the SB, or VDSM for troubleshooting when asked to gather the data by the Cisco Technical Support. This utility is very similar to the Linux or UNIX <b>tcpdump</b> command.

The **tcpdump** command allows an administrator (must be an admin user) to capture packets from the Ethernet. On the SB 500 series, the interface names are GigabitEthernet 1/0 and GigabitEthernet 2/0. On all VDS-SB 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 SB:

```
ServiceBroker# 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 SB to a PC so that the file can be viewed by a sniffer decoder.

```
ftp <ip address of the SB>
```

```
!--- 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 VDS-SB 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:

```
ServiceBroker# 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 ServiceBroker.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 > ServiceBroker.cisco.com: icmp 36: 172.19.226.63 udp
port 2048 unreachable
12:45:43.019327 IP ServiceBroker.cisco.com.10015 > dns-sj2.cisco.com.domain: 49828+ [ |
domain ]
12:45:43.021158 IP dns-sj2.cisco.com.domain > ServiceBroker.cisco.com.10015: 49828
NXDomain* [ | domain ]
12:45:43.021942 IP ServiceBroker.cisco.com.10015 > dns-sj2.cisco.com.domain: 49829+ [ |
domain ]
12:45:43.023799 IP dns-sj2.cisco.com.domain > ServiceBroker.cisco.com.10015: 49829
NXDomain* [ | domain ]
12:45:43.024240 IP ServiceBroker.cisco.com.10015 > dns-sj2.cisco.com.domain: 49830+ [ |
domain ]
12:45:43.026164 IP dns-sj2.cisco.com.domain > ServiceBroker.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 > ServiceBroker.cisco.com.ssh: . ack 112 win 64351
12:45:42.831490 IP ServiceBroker.cisco.com.ssh > 10.77.140.97.4314: . 112:1444(1332) ack 1
win 15232
12:45:42.831504 IP ServiceBroker.cisco.com.ssh > 10.77.140.97.4314: P 1444:1568(124) ack 1
win 15232
12:45:42.831741 IP ServiceBroker.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 > ServiceBroker.cisco.com.ssh: . ack 1568 win 65535
12:45:43.046248 IP ServiceBroker.cisco.com.ssh > 10.77.140.97.4314: P 1696:2128(432) ack 1
win 15232
12:45:43.046469 IP ServiceBroker.cisco.com.ssh > 10.77.140.97.4314: P 2128:2256(128) ack 1
win 15232
12:45:43.046616 IP ServiceBroker.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 > ServiceBroker.cisco.com.ssh: . ack 1696 win 65407
12:45:43.199784 IP ServiceBroker.cisco.com.ssh > 10.77.140.97.4314: P 2400:2864(464) ack 1
win 15232
12:45:43.199998 IP ServiceBroker.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 > ServiceBroker.cisco.com.ssh: . ack 2400 win 64703
12:45:43.260064 IP ServiceBroker.cisco.com.ssh > 10.77.140.97.4314: P 2992:3280(288) ack 1
win 15232
12:45:43.260335 IP ServiceBroker.cisco.com.ssh > 10.77.140.97.4314: P 3280:3408(128) ack 1
win 15232
12:45:43.260482 IP ServiceBroker.cisco.com.ssh > 10.77.140.97.4314: P 3408:3552(144) ack 1
win 15232
12:45:43.260621 IP ServiceBroker.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 > ServiceBroker.cisco.com.ssh: . ack 2992 win 65535
12:45:43.413389 IP ServiceBroker.cisco.com.ssh > 10.77.140.97.4314: P 3696:3984(288) ack 1
win 15232
12:45:43.413597 IP ServiceBroker.cisco.com.ssh > 10.77.140.97.4314: P 3984:4112(128) ack 1
win 15232
12:45:43.413741 IP ServiceBroker.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 > ServiceBroker.cisco.com.ssh: . ack 3552 win 64975
12:45:43.473659 IP ServiceBroker.cisco.com.ssh > 10.77.140.97.4314: P 4256:4544(288) ack 1
win 15232
12:45:43.473853 IP ServiceBroker.cisco.com.ssh > 10.77.140.97.4314: P 4544:4672(128) ack 1
win 15232
12:45:43.473994 IP ServiceBroker.cisco.com.ssh > 10.77.140.97.4314: P 4672:4816(144) ack 1
win 15232
12:45:43.474132 IP ServiceBroker.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 > ServiceBroker.cisco.com.ssh: P 1:81(80) ack 3696
win 64831
12:45:43.484167 IP ServiceBroker.cisco.com.ssh > 10.77.140.97.4314: P 4960:5248(288) ack
81 win 15232
12:45:43.484424 IP ServiceBroker.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 > ServiceBroker.cisco.com.ssh: . ack 4112 win 64415
12:45:43.627204 IP ServiceBroker.cisco.com.ssh > 10.77.140.97.4314: P 5392:5680(288) ack
81 win 15232
12:45:43.627439 IP ServiceBroker.cisco.com.ssh > 10.77.140.97.4314: P 5680:5808(128) ack
81 win 15232
12:45:43.627586 IP ServiceBroker.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 > ServiceBroker.cisco.com.ssh: . ack 4544 win 65535
12:45:43.688316 IP ServiceBroker.cisco.com.ssh > 10.77.140.97.4314: P 5952:6240(288) ack
81 win 15232
12:45:43.688495 IP ServiceBroker.cisco.com.ssh > 10.77.140.97.4314: P 6240:6368(128) ack
81 win 15232
12:45:43.688638 IP ServiceBroker.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 > ServiceBroker.cisco.com.ssh: . ack 4960 win 65119
12:45:43.689046 IP ServiceBroker.cisco.com.ssh > 10.77.140.97.4314: P 6512:6800(288) ack
81 win 15232
12:45:43.689170 IP ServiceBroker.cisco.com.ssh > 10.77.140.97.4314: P 6800:6928(128) ack
81 win 15232
12:45:43.689309 IP ServiceBroker.cisco.com.ssh > 10.77.140.97.4314: P 6928:7072(144) ack
81 win 15232
12:45:43.689447 IP ServiceBroker.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 > ServiceBroker.cisco.com.ssh: . ack 5392 win 64687
12:45:43.698437 IP ServiceBroker.cisco.com.ssh > 10.77.140.97.4314: P 7216:7504(288) ack
81 win 15232
12:45:43.698599 IP ServiceBroker.cisco.com.ssh > 10.77.140.97.4314: P 7504:7632(128) ack
81 win 15232
12:45:43.698740 IP ServiceBroker.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 > ServiceBroker.cisco.com.ssh: . ack 5808 win 64271
12:45:43.840622 IP ServiceBroker.cisco.com.ssh > 10.77.140.97.4314: P 7776:8064(288) ack
81 win 15232
```

```

12:45:43.840819 IP ServiceBroker.cisco.com.ssh > 10.77.140.97.4314: P 8064:8192(128) ack
81 win 15232
12:45:43.840962 IP ServiceBroker.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 > ServiceBroker.cisco.com.ssh: . ack 6368 win 65535
12:45:43.901938 IP ServiceBroker.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 > ServiceBroker.cisco.com.ssh: . ack 6928 win 64975
12:45:43.901910 IP 10.77.140.97.4314 > ServiceBroker.cisco.com.ssh: . ack 7216 win 64687
12:45:43.902137 IP ServiceBroker.cisco.com.ssh > 10.77.140.97.4314: P 8624:8752(128) ack
81 win 15232
12:45:43.902281 IP ServiceBroker.cisco.com.ssh > 10.77.140.97.4314: P 8752:8896(144) ack
81 win 15232
12:45:43.902414 IP ServiceBroker.cisco.com.ssh > 10.77.140.97.4314: P 8896:9024(128) ack
81 win 15232
12:45:43.902547 IP ServiceBroker.cisco.com.ssh > 10.77.140.97.4314: P 9024:9152(128) ack
81 win 15232
12:45:43.902687 IP ServiceBroker.cisco.com.ssh > 10.77.140.97.4314: P 9152:9296(144) ack
81 win 15232
12:45:43.902826 IP ServiceBroker.cisco.com.ssh > 10.77.140.97.4314: P 9296:9440(144) ack
81 win 15232
12:45:43.902965 IP ServiceBroker.cisco.com.ssh > 10.77.140.97.4314: P 9440:9584(144) ack
81 win 15232
12:45:43.903104 IP ServiceBroker.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 > ServiceBroker.cisco.com.ssh: . ack 7632 win 64271
12:45:43.922459 IP ServiceBroker.cisco.com.ssh > 10.77.140.97.4314: P 9728:10304(576) ack
81 win 15232
12:45:43.922622 IP ServiceBroker.cisco.com.ssh > 10.77.140.97.4314: P 10304:10432(128) ack
81 win 15232
12:45:43.922764 IP ServiceBroker.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 > ServiceBroker.cisco.com.ssh: . ack 8192 win 65535
12:45:44.053972 IP ServiceBroker.cisco.com.ssh > 10.77.140.97.4314: P 10576:10864(288) ack
81 win 15232
12:45:44.054308 IP ServiceBroker.cisco.com.ssh > 10.77.140.97.4314: P 10864:11104(240) ack
81 win 15232
12:45:44.054453 IP ServiceBroker.cisco.com.ssh > 10.77.140.97.4314: P 11104:11248(144) ack
81 win 15232
12:45:44.054596 IP ServiceBroker.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 > ServiceBroker.cisco.com.ssh: . ack 8752 win 64975
12:45:44.114712 IP ServiceBroker.cisco.com.ssh > 10.77.140.97.4314: P 11392:11712(320) ack
81 win 15232
12:45:44.115219 IP ServiceBroker.cisco.com.ssh > 10.77.140.97.4314: P 11712:11952(240) ack
81 win 15232
12:45:44.115381 IP ServiceBroker.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 > ServiceBroker.cisco.com.ssh: . ack 9152 win 64575
12:45:44.115617 IP ServiceBroker.cisco.com.ssh > 10.77.140.97.4314: P 12096:12336(240) ack
81 win 15232
12:45:44.115760 IP ServiceBroker.cisco.com.ssh > 10.77.140.97.4314: P 12336:12480(144) ack
81 win 15232
12:45:44.115904 IP ServiceBroker.cisco.com.ssh > 10.77.140.97.4314: P 12480:12624(144) ack
81 win 15232
12:45:44.116045 IP ServiceBroker.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 > ServiceBroker.cisco.com.ssh: . ack 9440 win 64287
12:45:44.116114 IP 10.77.140.97.4314 > ServiceBroker.cisco.com.ssh: . ack 9728 win 65535
12:45:44.116332 IP ServiceBroker.cisco.com.ssh > 10.77.140.97.4314: P 12768:13088(320) ack
81 win 15232

```

```
12:45:44.116473 IP ServiceBroker.cisco.com.ssh > 10.77.140.97.4314: P 13088:13232(144) ack
81 win 15232
12:45:44.116614 IP ServiceBroker.cisco.com.ssh > 10.77.140.97.4314: P 13232:13376(144) ack
81 win 15232
12:45:44.116755 IP ServiceBroker.cisco.com.ssh > 10.77.140.97.4314: P 13376:13520(144) ack
81 win 15232
12:45:44.116895 IP ServiceBroker.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 > ServiceBroker.cisco.com.ssh: . ack 10432 win 64831
12:45:44.135996 IP ServiceBroker.cisco.com.ssh > 10.77.140.97.4314: P 13664:13808(144) ack
81 win 15232
12:45:44.136223 IP ServiceBroker.cisco.com.ssh > 10.77.140.97.4314: P 13808:14048(240) ack
81 win 15232
12:45:44.136366 IP ServiceBroker.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 > ServiceBroker.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:

```
ServiceBroker# 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
```

# tcpdumpx

To dump the network traffic with the tcpdump extension for a multi-interface capture, use the **tcpdumpx** command in EXEC configuration mode.

**tcpdumpx** [*LINE*]

---

## Syntax Description

*LINE* (Optional) Dump options, -h to get help.

---



---

## Defaults

None

---

## Command Modes

EXEC configuration mode.

---

## Usage Guidelines

The **tcpdumpx** command enables tcpdump to capture multiple interfaces in separate files. Each member interface of a PortChannel can be captured in a separate file. For example, if eth2, eth3, eth4 and eth5 are members of PortChannel 1 (bond0), they can be captured in different files.

Current: issue “tcpdump -i” for each PortChannel member in a different shell at the same time.

Implemented: New flag (-j), not used by tcpdump, under tcpdumpx handles this:

```
tcpdumpx -j PortChannel 1 -w filename.cap
```

This command internally expands to capture each physical interface’s dump in an individual file:

```
tcpdump -i eth2 -w filename.eth2.cap
tcpdump -i eth3 -w filename.eth3.cap
tcpdump -i eth4 -w filename.eth4.cap
tcpdump -i eth5 -w filename.eth5.cap
```

If eth2 and eth3 need to be captured, use “--” as a command separator to separate the two tcpdump instances:

```
tcpdumpx -i eth2 -w filename.cap -k -m -- -i eth3 -w filename2.cap -c -k -- ... --
```

This command internally expands to:

```
tcpdump -i eth2 -w filename.cap
tcpdump -i eth3 -w filename.cap
```

Other examples:

```
tcpdumpx -j PortChannel 1 -w filename.cap -- -j PortChannel 2 -w filename2.cap
tcpdumpx -i eth2 -w filename.cap -- -i eth3 -w filename2.cap -- j PortChannel 1 -w filename3.cap
```

This is documented in tcpdumpx help “tcpdumpx -h”:

```
tcpdump          Dump traffic on a network
tcpdumpx        tcpdump extension for multi-interface capture
tcpdumpx -h
tcpdumpx - tcpdump extension for multiple interface capture
[WARNING] This program consumes HIGH CPU & memory and impacts system performance
```

```
Usage: tcpdumpx [-w filename] [-j PortChannel X] [--] [all tcpdump options]
```

```

[-w filename]      Required. Write tcpdump output to filename
[-j PortChannel X] Capture each PortChannel slave to file:
                  "filename" --> "filenameslavename"
                  "filename.xxx" --> "filename.slavename.xxx"
[--]              Interface seperator. Capture Multiple Interfaces by:
                  tcpdumpx -i eth0 -w eth0 -- -i eth2 -w eth2 -- ... -- ..
                  tcpdumpx -i eth0 -w eth0 -- -j PortChannel 1 -w pc
                  tcpdumpx -j PortChannel 1 -w pc1 -- -j PortChannel 2
                  -w pc2
[all tcpdump options] Specify any tcpdump options
                  Please use "tcpdump -h" to get tcpdump help options
[-h(elp)]         Print this help

```

### Examples

The following example shows how to dump the TCP network traffic with a tcpdump extension for multi-interface capture:

```
ServiceBroker# tcpdumpx
```

# tcpmon

To search all TCP connections, use the **tcpmon** command in EXEC configuration mode.

**tcpmon** *line*

<b>Syntax Description</b>	<i>line</i>	Shows TCP connection information, -h to get help.
---------------------------	-------------	---

<b>Command Defaults</b>	None
-------------------------	------

<b>Command Modes</b>	EXEC configuration.
----------------------	---------------------

<b>Usage Guidelines</b>	The <b>tcpmon</b> utility is a script that constantly calls the ss utility at specified intervals. The <b>tcpmon</b> 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 <b>tcpmon -h</b> .
-------------------------	--

[Table 4-16](#) describes the tcpmon output fields.

**Table 4-16** *tcpmon Output Fields*

Field	Description
State	One of the following TCP connection states: ESTAB, SYN-SENT, SYN-RCV, 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:

```
ServiceBroker# tcpmon -R 100 30
```

The following command sets the polling cycle to 30 seconds and displays only the sockets with window scaling disabled:

```
ServiceBroker# tcpmon -N 30
```

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

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>gulp</b>	Captures lossless gigabit packets and writes them to disk.
<b>netmon</b>	Displays the transmit and receive activity on an interface.
<b>netstatr</b>	Displays the rate of change of netstat statistics.
<b>ss</b>	Dumps socket statistics.

# tcp

To configure TCP-related parameters, 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**

---

<b>Syntax Description</b>	<b>timestamp</b> Enables TCP timestamps.
---------------------------	--

---



---

<b>Defaults</b>	TCP timestamp is enabled by default.
-----------------	--------------------------------------

---

<b>Command Modes</b>	Global configuration (config) mode.
----------------------	-------------------------------------

---

<b>Examples</b>	The following example shows how to disable the TCP timestamp:
-----------------	---

```
ServiceBroker# no tcp timestamp
ServiceBroker#
```

## telnet (EXEC Configuration)

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.

**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 SB CLI.

**Examples** The following example shows how to open a Telnet session to a network device using the hostname:

```
ServiceBroker# telnet cisco-ce
```

The following example shows how to open a Telnet session to a network device using the IP address:

```
ServiceBroker# 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:

```
ServiceBroker# telnet cisco-ce 8443
```

The following example shows how to open a Telnet session to a network device on port 80 using the hostname:

```
ServiceBroker# telnet www.yahoo.com 80
```

## telnet (Global Configuration)

To enable Telnet service, use the **telnet enable** command in Global configuration mode. To disable Telnet, use the **no** form of this command.

**telnet**

**no telnet**

Syntax Description	enable	Enables Telnet service.
--------------------	--------	-------------------------

Defaults	Telnet is enabled by default.
----------	-------------------------------

Command Modes	Global configuration (config) mode.
---------------	-------------------------------------

Usage Guidelines	Use this Terminal Emulation protocol for a remote terminal connection. The <b>telnet enable</b> command allows users to log in to other devices using a Telnet session.
------------------	---

Examples	The following example shows how to enable Telnet on the SB:
----------	---

```
ServiceBroker(config)# telnet enable
```

Related Commands	Command	Description
	<b>show telnet</b>	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	monitor [disable]
	<i>length</i>	
		<b>disable</b>

Sets the length of the display on the terminal.
Length of the display on the terminal (the range is 0 to 512). Setting the length to 0 means that there is no pausing.
Copies the debug output to the current terminal.
(Optional) Disables monitoring at this specified terminal.

**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:

```
ServiceBroker# terminal length 20
```

The following example shows how to configure the terminal for no pausing:

```
ServiceBroker# 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		
<b>ftp</b>		Specifies the FTP URL to be tested.
<i>url</i>		FTP URL to be tested. Use one of the following formats to specify the FTP URL: <ul style="list-style-type: none"> <li>ftp://domainname/path</li> <li>ftp://user:password@domainname/path</li> </ul>
<b>use-ftp-proxy</b>		(Optional) Specifies the FTP proxy that is used to test the URL.
<i>proxy_url</i>		FTP proxy URL. Use one of the following formats to specify the proxy URL: <ul style="list-style-type: none"> <li>proxy IP Address:proxy Port</li> <li>proxy Username:proxy Password@proxy IP Address:proxy Port</li> </ul>
<b>http</b>		Specifies the HTTP URL to be tested.
<i>url</i>		HTTP URL to be tested. Use one of the following formats to specify the HTTP URL: <ul style="list-style-type: none"> <li>http://domainname/path</li> <li>http://user:password@domainname/path</li> </ul>
<b>custom-header</b>		(Optional) Specifies the custom header information to be sent to the server.
<i>header</i>		Custom header information to be sent to the server. Use the format <i>header:line</i> to specify the custom header.
<b>head-only</b>		(Optional) Specifies that only the HTTP header information must be retrieved.
<b>use-http-proxy</b>		(Optional) Specifies the HTTP proxy that is used to test the URL.
<i>proxy_url</i>		HTTP proxy URL. Use one of the following formats to specify the HTTP proxy URL: <pre>http://proxyIp:proxyPort http://proxyUser:proxypasswd@proxyIp:proxyPort</pre>
<b>head-only</b>		(Optional) Specifies that only the HTTPS header information must be retrieved.

**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 SB 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:

```
ServiceBroker# test-url http http://cel.server.com
--02:27:20-- http://cel.server.com/
=> `/dev/null'
Len - 22 , Restval - 0 , contlen - 0 , Res - 134728056Resolving cel.server.com..

done.
Connecting to cel.server.com [ 192.168.171.22 ] :80... connected.
HTTP request sent, awaiting response...
 1 HTTP/1.1 200 OK
 2 Date: Mon, 26 Jul 2004 08:41:34 GMT
 3 Server: Apache/1.2b8
 4 Last-Modified: Fri, 25 Apr 2003 12:23:04 GMT
 5 ETag: "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`:

```
ServiceBroker# 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...
```

test-url

```

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:

```

ServiceBroker# test-url ftp ftp://ssivakum:ssivakum@10.77.157.148/antinat-0.90.tar
Mar 30 14:33:44 nramaraj-ce admin-shell: %SB-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 ]  
  
ServiceBroker#
```

**Related Commands**

Command	Description
<b>acquirer (EXEC)</b>	Starts or stops content acquisition on a specified acquirer delivery service.

# top

To see a dynamic real-time view of a running VDS-SB, use the **top** command in EXEC configuration mode.

**top** {*line*}

<b>Syntax Description</b>	<i>line</i> Specifies top options, enter <b>-h</b> to get Help. Press <b>q</b> to quit from the output.
---------------------------	---

<b>Defaults</b>	No default behavior values
-----------------	----------------------------

<b>Command Modes</b>	EXEC configuration mode.
----------------------	--------------------------

<b>Examples</b>	The following example shows sample output from the <b>top</b> command on an SB:
-----------------	---

```
ServiceBroker# 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.

```
traceroute {hostname | ip_address}
```

Syntax Description	hostname	Name of the remote host.
	ip_address	IP address of the remote host.

**Defaults** None

**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 SB:

```
ServiceBroker# 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 **tracert** command fails to trace the route to a remote host from the SB:

```

ServiceBroker# tracert 10.0.0.1
tracert to 10.0.0.1 (10.0.0.1), 30 hops max, 38 byte packets
 1  10.1.1.50 (10.1.1.50)  2.022 ms  1.970 ms  2.156 ms
 2  sblab2-rtr.cisco.com (192.168.10.1)  3.955 ms  172.19.231.249 (172.19.231.249)  0.654
ms  0.607 ms
 3  sjc22-00lab-gw1.cisco.com (172.24.115.65)  0.704 ms  0.625 ms  0.596 ms
 4  sjc20-lab-gw1.cisco.com (172.24.115.105)  0.736 ms  0.686 ms  0.615 ms
 5  sjc20-sbb5-gw1.cisco.com (128.107.180.85)  0.703 ms  0.696 ms  0.646 ms
 6  sjc20-rbb-gw5.cisco.com (128.107.180.22)  0.736 ms  0.782 ms  0.750 ms
 7  sjce-rbb-gw1.cisco.com (171.69.7.249)  1.291 ms  1.314 ms  1.218 ms
 8  sjce-corp-gw1.cisco.com (171.69.7.170)  1.477 ms  1.257 ms  1.221 ms
 9  * * *
10  * * *
.
.
.
29  * * *
30  * * *

```

Table 4-17 describes the fields in the **traceroute** command output.

**Table 4-17** *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
<b>ping</b>	Sends echo packets for diagnosing basic network connectivity on networks.

# transaction-log force

Command	Description
<b>ipv6</b>	Specifies the IPv6 address of the default gateway.

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

<b>archive</b>	Forces the archive of the <i>working.log</i> file.
<b>export</b>	Forces the archived files to be exported to the server.

## 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 SB 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 SB hard disk:

```
ServiceBroker# transaction-log force archive
```

The following example shows that the SB is configured to export its transaction logs to two FTP servers:

```
ServiceBroker(config)# transaction-logs export ftp-server 10.1.1.1 mylogin mypasswd
/ftpdirectory
ServiceBroker(config)# transaction-logs export ftp-server myhostname mylogin mypasswd
/ftpdirectory
```

The following example shows how to export the transaction log file from the SB hard disk to an FTP server designated by the **transaction-logs export ftp-server** command:

```
ServiceBroker# transaction-log force export
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>clear transaction logs</b>	Clears the working transaction log settings.
	<b>show statistics transaction-logs</b>	Displays the SB transaction log export statistics.
	<b>show transaction-logging</b>	Displays the transaction log configuration settings and a list of archived transaction log files.
	<b>transaction-logs</b>	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

<b>archive</b>	Configures archive parameters.
<b>interval</b>	Determines how frequently the archive file is to be saved.
<i>seconds</i>	Frequency of archiving, in seconds. The range is from 120 to 604800.
<b>every-day</b>	Archives using intervals of 1 day or less.
<b>at</b>	Specifies the local time at which to archive each day.
<i>hour:minute</i>	Time of day at which to archive in local time (hh:mm).
<b>every</b>	Specifies the interval in hours. Interval aligns with midnight.
<i>hours</i>	Number of hours for daily file archive. 1—Hourly 12—Every 12 hours 2—Every 2 hours 24—Every 24 hours 3—Every 3 hours 4—Every 4 hours 6—Every 6 hours 8—Every 8 hours
<b>every-hour</b>	Specifies the archives using intervals of 1 hour or less.
<b>at</b>	Sets the time to archive at each hour.
<i>minute</i>	Minute alignment for the hourly archive. The range is from 0 to 59.
<b>every</b>	Specifies the interval in minutes for hourly archive that aligns with the top of the hour.

<i>minutes</i>	Number of minutes for hourly archive. 10—Every 10 minutes 15—Every 15 minutes 2—Every 2 minutes 20—Every 20 minutes 30—Every 30 minutes 5—Every 5 minutes
<b>every-week</b>	Archives using intervals of 1 or more times a week.
<b>on</b>	(Optional) Sets the day of the week on which to archive.
<i>weekdays</i>	Weekdays on which to archive. One or more weekdays can be specified. Fri—Every Friday Mon—Every Monday Sat—Every Saturday Sun—Every Sunday Thu—Every Thursday Tue—Every Tuesday Wed—Every Wednesday
<b>at</b>	(Optional) Sets the local time at which to archive each day.
<i>hour:minute</i>	Time of day at which to archive in local time (hh:mm).
<b>max-file-number</b>	Sets the maximum number of the archived log file.
<i>file_number</i>	Maximum number of the archived log file. The range is from 1 to 10000.
<b>max-file-size</b>	Sets the maximum archive file size.
<i>filesize</i>	Maximum archive file size in kilobytes. The range is from 1000 to 2000000.
<b>ds-snapshot-counter enable</b>	Enables the per delivery service snapshot counter.
<b>enable</b>	Enables the transaction log.
<b>export</b>	Configures file export parameters.
<b>compress enable</b>	Compresses the archived files in the gzip format before exporting. Enables the exporting of log files at the specified interval.
<b>ftp-server</b>	Sets the FTP server to receive exported archived files.
<i>hostname</i>	Hostname of the target FTP server.
<i>serv_ip_addrs</i>	IP address of the target FTP server.
<i>login</i>	User login to target FTP server.
<i>passw</i>	User password to target FTP server.
<i>directory</i>	Target directory path for exported files on FTP server.
<b>interval</b>	Determines how frequently the file is to be exported.
<i>minutes</i>	Number of minutes in the interval at which to export a file. The range is from 1 to 10080.
<b>every-day</b>	Specifies the exports using intervals of 1 day or less.
<b>at</b>	Specifies the local time at which to export each day.
<i>hour:minute</i>	Time of day at which to export in local time (hh:mm).
<b>every</b>	Specifies the interval in hours for the daily export.

<i>hours</i>	Number of hours for the daily export. 1—Hourly 12—Every 12 hours 2— Every 2 hours 24—Every 24 hours 3— Every 3 hours 4—Every 4 hours 6—Every 6 hours 8—Every 8 hours
<b>every-hour</b>	Specifies the exports using intervals of 1 hour or less.
<b>at</b>	Specifies the time at which to export each hour.
<i>minute</i>	Minute alignment for the hourly export. The range is from 0 to 59.
<b>every</b>	Specifies the interval in minutes that align with the top of the hour.
<i>minutes</i>	Number of minutes for the hourly export. 10—Every 10 minutes 15—Every 15 minutes 2—Every 2 minutes 20—Every 20 minutes 30—Every 30 minutes 5—Every 5 minutes
<b>every-week</b>	Specifies the exports using intervals of 1 or more times a week.
<b>on</b>	(Optional) Specifies the days of the week for the export.
<i>weekdays</i>	Weekdays on which to export. One or more weekdays can be specified. Fri—Every Friday Mon—Every Monday Sat—Every Saturday Sun—Every Sunday Thu—Every Thursday Tue—Every Tuesday Wed—Every Wednesday
<b>at</b>	(Optional) Specifies the time of day at which to perform the weekly export.
<i>hour:minute</i>	Time of day at which to export in the local time (hh:mm).
<b>sftp-server</b>	Sets the SFTP <sup>1</sup> server to receive exported archived files.
<i>hostname</i>	Hostname of the target SFTP server.
<i>serv_ip_addr</i>	IP address of the target SFTP server.
<i>login</i>	User login to the target SFTP server (less than 40 characters).
<i>passw</i>	User password to the target SFTP server (less than 40 characters).
<i>directory</i>	Target directory path for exported files on the SFTP server.
<b>format</b>	Sets the format to use for the HTTP transaction log entries in the working.log file.
<b>apache</b>	Configures the HTTP transaction logs output to the Apache CLF <sup>2</sup> .
<b>custom</b>	Configures the HTTP transaction logs output to the custom log format.
<i>string</i>	Quoted log format string containing the custom log format.
<b>extended-squid</b>	Configures the HTTP transaction logs output to the Extended Squid log format.

<b>log-windows-domain</b>	Logs the Windows domain with an authenticated username if available in HTTP transaction log entries.
<b>enable</b>	Enables the remote transaction logging.
<b>entry-type</b>	Specifies the type of transaction log entry.
<b>all</b>	Sets the SB to send all transaction log messages to the remote syslog server.
<b>request-auth-failures</b>	Sets the SB to log to the remote syslog server only those transactions that the SB failed to authenticate with the Authentication Server.  <b>Note</b> 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.
<b>facility</b>	Configures a unique facility to create a separate log on the remote syslog host for real-time transaction log entries.
<i>parameter</i>	Specifies one of the following facilities:  auth—Authorization system daemon—System daemons kern—Kernel local0—Local use local1—Local use local2—Local use local3—Local use local4—Local use local5—Local use local6—Local use local7—Local use mail—Mail system news—USENET news syslog—Syslog itself user—User process uucp—UUCP system
<b>host</b>	Configures the remote syslog server.
<i>hostname</i>	Hostname of the remote syslog server.
<i>ip-address</i>	IP address of the remote syslog server.
<b>port</b>	Configures the port to use when sending transaction log messages to the syslog server.
<i>port-num</i>	Port number to use when sending transaction log messages to the syslog server. The default is 514.
<b>rate-limit</b>	Configures the rate at which the transaction logger is allowed to send messages to the remote syslog server.
<i>rate</i>	Rate (number of messages per second) at which the transaction logger is allowed to send messages to the remote syslog server.

1. SFTP = Secure File Transfer Protocol
2. CLF = common log format

---

**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**

SBs can record all errors and access activities. Each content service module on the SB 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 SB 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 SB (Windows Media server) can be parsed and saved to the normal WMT transaction logs that are stored on the SB.

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 4-18](#). The SB 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 SB. 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 SB.

Use the **transaction-logs ds-snapshot-counter enable** command to enable or disable snapshot counter transaction logs. This command is available for SB. On SB, the snapshot counter transaction log records per delivery service Storage Usage. On the SB, 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 4-18](#) 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 4-18](#) 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 4-18](#) 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 VDS Service Broker 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 4-18** Custom Format Log Format String Values

Format Token	Value
%a	IP address of the requesting client.
%A	IP address of the SB.
%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 4-18 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. <b>Note</b> All client request headers are only logged on the edge SB.

### 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 4-19 describes the name elements.

**Table 4-19** 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	VDS-SB 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 SB 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 4-20 lists the directory names and the corresponding examples of the archive filenames.

**Table 4-20** 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 4-20 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 SB 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 SB 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 SB 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 SB, 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 SB 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 SB 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:

```
ServiceBroker(config)# transaction-logs export ftp-server 10.1.1.1 mylogin mypasswd
/ftpdirectory
```

```
ServiceBroker(config)# transaction-logs export ftp-server myhostname mylogin mypasswd
/ftpdirectory
```

The following example shows how to delete an FTP server:

```
ServiceBroker(config)# no transaction-logs export ftp-server 10.1.1.1
ServiceBroker(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:

```
ServiceBroker(config)# no transaction-logs export enable
```

The following example shows how to change a username, password, or directory:

```
ServiceBroker(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:

```
ServiceBroker(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:

```
ServiceBroker(config)# no transaction-logs export sftp-server sftphostname
```

The following examples show how to configure the archiving intervals:

```
ServiceBroker(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
```

```
ServiceBroker(config)# transaction-logs archive interval every-day at
<0-23>: Time of day at which to archive (hh:mm)
```

```
ServiceBroker(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 SB has failed to export archive files:

```
ServiceBroker# 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:

```

ServiceBroker(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:

```

ServiceBroker(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):

```

ServiceBroker(config)# transaction-logs archive interval every-day every 4

```

The following example shows how to export once a day at midnight local time:

```

ServiceBroker(config)# transaction-logs export interval every-day every 24

```

The following example shows how to configure export intervals:

```

ServiceBroker(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

ServiceBroker(config)# transaction-logs archive interval every-hour at ?
<0-59>     Specify the minute alignment for the hourly archive
ServiceBroker(config)# transaction-logs archive interval every-hour every ?
<2-30>     Interval in minutes: { 2, 5, 10, 15, 20, 30 }

```

## Related Commands

Command	Description
<b>clear transaction-log</b>	Clears the working transaction log settings.
<b>show statistics transaction-logs</b>	Displays the SB transaction log export statistics.
<b>show transaction-logging</b>	Displays the transaction log configuration settings and a list of archived transaction log files.
<b>transaction-log force</b>	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*

<b>Syntax Description</b>	<i>filename</i> Name of file.
<b>Defaults</b>	None
<b>Command Modes</b>	EXEC configuration mode.
<b>Usage Guidelines</b>	Use this command to display the contents of a file within any SB 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 SB:

```
ServiceBroker# type /local1/syslog.txt

Jan 10 22:02:46 (none) populate_ds: %SB-CLI-5-170050: Cisco VDS Service Broker Software
starts booting
Jan 10 22:02:47 (none) create_etc_hosts.sh: %SB-CLI-5-170051: HOSTPLUSDOMAIN: NO-HOSTNAME
Jan 10 22:02:47 NO-HOSTNAME : %SB-CLI-5-170053: Recreated etc_hosts (1, 0)
Jan 10 22:02:48 NO-HOSTNAME Nodemgr: %SB-NODEMGR-5-330082: [ CLI_VER_NTP ] requests stop
service ntpd
Jan 10 22:02:49 NO-HOSTNAME Nodemgr: %SB-NODEMGR-5-330082: [ ver_tvout ] requests stop
service tvoutsvr
Jan 10 22:02:50 NO-HOSTNAME Nodemgr: %SB-NODEMGR-5-330084: [ ver_rtspg ] requests restart
service rtspg
Jan 10 22:02:50 NO-HOSTNAME Nodemgr: %SB-NODEMGR-5-330082: [ ver_ip_tv ] requests stop
service sbss
Jan 10 22:02:51 NO-HOSTNAME Nodemgr: %SB-NODEMGR-5-330080: [ ver_telnetd ] requests start
service telnetd
Jan 10 22:02:52 NO-HOSTNAME Nodemgr: %SB-NODEMGR-5-330082: [ ver_wmt ] requests stop
service wmt_mms
Jan 10 22:02:53 NO-HOSTNAME Nodemgr: %SB-NODEMGR-5-330082: [ ver_wmt ] requests stop
service wmt_logd
Jan 10 22:02:55 NO-HOSTNAME Nodemgr: %SB-NODEMGR-5-330082: [ Unknown ] requests stop
service mcast_sender
Jan 10 22:02:55 NO-HOSTNAME Nodemgr: %SB-NODEMGR-5-330082: [ Unknown ] requests stop
service mcast_receiver
Jan 10 22:02:56 NO-HOSTNAME Nodemgr: %SB-NODEMGR-5-330024: Service 'populate_ds' exited
normally with code 0
Jan 10 22:02:56 NO-HOSTNAME Nodemgr: %SB-NODEMGR-5-330040: Start service 'parser_server'
using: '/ruby/bin/parser_server' with pid: 1753
Jan 10 22:02:56 NO-HOSTNAME Nodemgr: %SB-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: %SB-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: %SB-SYS-5-900001: <6>setup.c: handling
flash window at [ 15MB..16MB)
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SB-SYS-5-900001: <6>BIOS-provided
physical RAM map:
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SB-SYS-5-900001: <4> BIOS-e820:
0000000000000000 - 0000000000009ec00 (usable)
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SB-SYS-5-900001: <4> BIOS-e820:
0000000000009ec00 - 000000000000a0000 (reserved)
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SB-SYS-5-900001: <4> BIOS-e820:
000000000000e0800 - 0000000000100000 (reserved)
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SB-SYS-5-900001: <4> BIOS-e820:
0000000000100000 - 0000000000f00000 (usable)
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SB-SYS-5-900001: <4> BIOS-e820:
0000000000f00000 - 0000000001000000 (reserved)
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SB-SYS-5-900001: <4> BIOS-e820:
0000000001000000 - 0000000010000000 (usable)
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SB-SYS-5-900001: <4> BIOS-e820:
00000000ffff00000 - 00000000100000000 (reserved)
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SB-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: %SB-SYS-5-900001: <4>On node 0 totalpages:
65536
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SB-SYS-5-900001: <4>zone(0): 4096 pages.
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SB-SYS-5-900001: <4>zone(1): 61440 pages.
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SB-SYS-5-900001: <4>zone(2): 0 pages.
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SB-SYS-5-900001: <4>Local APIC disabled
by BIOS -- reenabling.
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SB-SYS-5-900001: <4>Found and enabled
local APIC!
Jan 10 22:02:56 NO-HOSTNAME syslog_bootup_msgs: %SB-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: %SB-SYS-5-900001: <6>Initializing CPU# 0
<output truncated>

```

**Related Commands**

Command	Description
<b>cpfile</b>	Copies a file.
<b>dir</b>	Displays the files in a directory in a long-list format.
<b>lls</b>	Displays a long list of directory names.
<b>ls</b>	Lists the files and subdirectories in a directory.
<b>mkfile</b>	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	
<i>filename</i>	File to be examined.
<i>line</i>	(Optional) The number of lines from the end of the file to be displayed (the range is 1 to 65535).
<b>follow</b>	(Optional) Displays the end of the file continuously as new lines are added to the file.

**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-ServiceBroker# 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-ServiceBroker# 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.txt file:

```

stream-ServiceBroker# 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-ServiceBroker# type-tail /local1/syslog.txt ?
<1-65535> The numbers of lines from end
follow Follow the file as it grows
<cr>
stream-ServiceBroker# type-tail /local1/syslog.txt follow
Oct 8 21:49:39 stream-ce syslog:(26832)TRCE:in_mms.c:1747-> tv = NULL
Oct 8 21:49:41 stream-ce syslog:(26830)TRCE:input_serv.c:83-> select_with
return 0, ready = 0
Oct 8 21:49:41 stream-ce syslog:(26832)TRCE:al_master.c:246-> select_with
return 0, ready = 0
Oct 8 21:49:41 stream-ce syslog:(26832)TRCE:in_mms.c:1747-> tv = NULL
Oct 8 21:49:43 stream-ce syslog:(26830)TRCE:input_serv.c:83-> select_with
return 0, ready = 0
Oct 8 21:49:43 stream-ce syslog:(26832)TRCE:al_master.c:246-> select_with
return 0, ready = 0
Oct 8 21:49:43 stream-ce syslog:(26832)TRCE:in_mms.c:1747-> tv = NULL
Oct 8 21:49:45 stream-ce syslog:(26830)TRCE:input_serv.c:83-> select_with
return 0, ready = 0
Oct 8 21:49:45 stream-ce syslog:(26832)TRCE:al_master.c:246-> select_with
return 0, ready = 0
Oct 8 21:49:45 stream-ce syslog:(26832)TRCE:in_mms.c:1747-> tv = NULL
Oct 8 21:49:47 stream-ce syslog:(26830)TRCE:input_serv.c:83-> select_with
return 0, ready = 0
Oct 8 21:49:47 stream-ce syslog:(26832)TRCE:al_master.c:246-> select_with
return 0, ready = 0
Oct 8 21:49:47 stream-ce syslog:(26832)TRCE:in_mms.c:1747-> tv = NULL
Oct 8 21:49:49 stream-ce syslog:(26830)TRCE:input_serv.c:83-> select_with
return 0, ready = 0
Oct 8 21:49:49 stream-ce syslog:(26832)TRCE:al_master.c:246-> select_with
return 0, ready = 0
Oct 8 21:49:49 stream-ce syslog:(26832)TRCE:in_mms.c:1747-> tv = NULL

```

# undebug

To disable debugging functions, use the **undebug** EXEC command.

**undebug** *option*

**Syntax Description** This command has no arguments or keywords.

**Defaults** 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 2-47 for more information about debug functions.

Valid values for *command* are as follows:

Command	Description	Device Mode
<b>access-lists</b>	Access Control List debug commands.	SB
<b>all</b>	Disables all debugging.	All
<b>authentication</b>	Authentication debug commands.	All
<b>cli</b>	CLI debug commands.	SB
<b>cms</b>	Debugs the CMS <sup>1</sup> .	All
<b>dataserver</b>	Dataserver debug commands.	All
<b>dfs</b>	DFS <sup>2</sup> debug commands.	SB
<b>dhcp</b>	DHCP <sup>3</sup> debug commands.	All
<b>emdb</b>	Embedded database debug commands.	All
<b>logging</b>	LOG debug commands.	All
<b>malloc</b>	Memory allocation debug commands.	All
<b>ntp</b>	NTP <sup>4</sup> debug commands.	All
<b>rpc</b>	Interbox RPC <sup>5</sup> debug commands.	All
<b>service-broker</b>	Service Broker debug commands.	SB
<b>service-monitor</b>	Service Monitor debug commands.	All
<b>snmp</b>	SNMP debug commands.	All
<b>standby</b>	Standby debug commands.	SB
<b>stats</b>	Statistics debug commands.	VDSM
<b>translog</b>	Transaction Log debug commands.	SB

1. CMS = centralized management system
2. DFS = distributed filesystem
3. DHCP = Dynamic Host Configuration Protocol

■ **undebug**

4. NTP = network time protocol
5. RPC = remote procedure call

#### Related Commands

Command	Description
<b>debug</b>	Configures the debugging options.
<b>show debugging</b>	Displays the state of each debugging option.

# url-signature

The VDS-SB 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		
<b>key-id-owner</b>		Configures the owner ID for this key.
<i>num</i>		Specifies the ID for the owner of this key. The range is from 1 to 8.
<b>key-id-number</b>		Configures the number ID for this key.
<i>id_num</i>		Specifies the ID for the number of this key. The range is from 1 to 8.
<b>key</b>		Configures the encryption key for signing a URL.
<i>keyword</i>		Text of encryption key (maximum of 64 characters, no spaces).
	<b>Note</b>	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: {}!#\$%&()*+,-./:;<=>@\~^[]_.
<b>public-key</b>		Configures the Public Key file location (PEM).
<i>url</i>		The URL from where the Public Key file can be downloaded (maximum of 54 characters).
<b>symmetric-key</b>		(Optional) Configure the Symmetric Key.
<i>word</i>		The Symmetric Key (Must be 16 characters, no spaces).
<b>private-Key</b>		(Optional) Configures the Private Key file location (PEM).
<i>url</i>		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 SB. 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 SB 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 SB 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 SB 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 SBs 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 SB may redirect a client request to any SB 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 (VDS-SB).

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 vos-ims-urlsign.py http://www.cisco.com/index.html 8.1.0.4 200000 1 2 cisco
```

An example of the resulting signed URL follows:

```
http://www.cisco.com/index.html?IS=0&ET=1241194518&CIP=8.1.0.4&KO=1&KN=2&US=deebacde45bf716071c8b2fecaa755b9
```

If you specify Version 1 for the script, SHA-1 is used and the SIGV=1 string is added.

Following is an example of the URL signing script using the SHA-1 security hash algorithm:

```
python vos-ims-urlsign.py http://www.cisco.com/index.html 8.1.0.4 200000 1 2 cisco 1
```

An example of the resulting signed URL follows:

```
http://www.cisco.com/index.html?SIGV=1&IS=0&ET=1241194679&CIP=8.1.0.4&KO=1&KN=2&US=8349348ffac7987d11203122a98e7e64e410fa18
```

If you specify Version 2 for the script, SHA-1 is used. The protocol from the beginning of the URL is also removed before the signature is generated, and the SIGV=2 string is added. The protocol is RTSP, HTTP, or RTMP. The URL is signed without the protocol, but the final signed URL is printed with the protocol.

Following is an example of the URL signing script using the SHA-1 security hash algorithm with Version 2 specified:

```
python vos-ims-urlsign.py http://www.cisco.com/index.html 8.1.0.4 200000 1 2 cisco 2
```

An example of the resulting signed URL follows:

```
http://www.cisco.com/index.html?SIGV=2&IS=0&ET=1241194783&CIP=8.1.0.4&KO=1&KN=2&US=68b5f5ed97d1255a0ec42a42a4f779e794df679c
```



#### 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:

```
{ } ! # $ % & ( ) * + , - . / : ; < = > @ \ ~ ^ [ ] _
```

**Examples**

Following is an example of generating and encrypting the public key and private key using the **url-signature** command:

```
ServiceBroker(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 vos-ims-urldsign.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 vos-ims-urldsign.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 vos-ims-urldsign.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

<i>name</i>	Username.
<b>cifs-password</b>	Sets the Windows user password.
<b>samba-password</b>	Deprecated, same as <b>cifs-password</b> .
<b>0</b>	Specifies a clear-text password. This is the default password setting.
<i>plain_word</i>	Clear-text user password.
<b>1</b>	Specifies a type 1 encrypted password.
<i>lan_crypto</i>	Encrypted password for LAN Manager networks.
<i>nt_crypto</i>	Encrypted password for Windows NT networks.
<i>clear_text</i>	Unencrypted (clear-text) password for Windows NT networks.
<b>password</b>	Sets the user password.
<i>crypto_word</i>	Encrypted user password.
<b>uid</b>	Sets the user ID for a clear-text password or an encrypted password.
<i>u_id</i>	Encrypted password user ID (the range is 2001 to 65535).
<b>privilege</b>	Sets the user privilege level.
<b>0</b>	Sets the user privilege level for a normal user.
<b>15</b>	Sets the user privilege level for a superuser.

## 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 VDS-SB 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 VDS-SB network device should have an administrative password that can override the default password.

### User Authorization

Domains and roles are applied by the VDSM 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 VDSM 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 VDS-SB device to an VDS-SB 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:

```
ServiceBroker(config)# username admin password yoursecret
```

The following example shows how passwords and privilege levels are reconfigured:

```
ServiceBroker# show user username abeddoe
Uid          : 2003
Username     : abeddoe
Password     : ghQ.GyGhP96K6
Privilege    : normal user
ServiceBroker# show user username bwhidney
Uid          : 2002
Username     : bwhidney
Password     : bhlohIbIwAMOk
Privilege    : normal user
ServiceBroker(config)# username bwhidney password 1 victoria
ServiceBroker(config)# username abeddoe privilege 15
User's privilege changed to super user (=15)
ServiceBroker# show user username abeddoe
Uid          : 2003
Username     : abeddoe
Password     : ghQ.GyGhP96K6
Privilege    : super user

ServiceBroker# show user username bwhidney
Uid          : 2002
Username     : bwhidney
Password     : mhYWYw.7P1Ld6
Privilege    : normal user
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show user</b>	Displays the user identification number and username information for a particular user.
	<b>show users</b>	Displays the specified users.

# vds

To configure the VDS-SB IP address to be used for the SBs, or to configure the role and GUI parameters on a VDSM device, use the **VDSM** command in Global configuration mode. To negate these actions, use the **no** form of this command.

```
vds {ip {hostname | ip-address | role {primary | standby} | ui port port-num}}
```

```
no vds {ip | role {primary | standby} | ui port}
```

## Syntax Description

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

## Defaults

None

## Command Modes

Global configuration (config) mode.

## Usage Guidelines

You can use the **VDSM ui port** command to change the VDSM GUI port from the standard number 8443 as follows:

```
VDSM(config)# vds ui port 35535
```



### Note

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

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

After the device is configured with the VDSM 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 VDSM.

### Configuring Devices Inside a NAT

In an VDS-SB network, there are two methods for a device registered with the VDSM (SBs, or standby VDSM) to obtain configuration information from the primary VDSM. The primary method is for the device to periodically poll the primary VDSM on port 443 to request a configuration update. You cannot configure this port number. The backup method is when the VDSM 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. VDS-SB networks do not work reliably if devices registered with the VDSM are unable to poll the VDSM for configuration updates. Similarly, when a receiver SB requests content and content metadata from a forwarder SB, it contacts the forwarder SB on port 443.

All the above methods become complex in the presence of Network Address Translation (NAT) firewalls. When a device (SBs at the edge of the network, SBs, and primary or standby VDSMs) 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 VDSM. 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 VDSM 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 VDSM's inside local IP address on its NAT, and using this address, rather than the VDSM's inside local IP address, in the **VDSM ip ip-address** command when you register the device to the VDSM. If the SB is inside a NAT and the VDSM is outside the NAT, you can allow the SB to poll for `getUpdate` requests by configuring a static translation (inside global IP address) for the SB 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 VDSMs

The Cisco VDS Service Broker software implements a standby VDSM. This process allows you to maintain a copy of the VDS-SB network configuration. If the primary VDSM fails, the standby can be used to replace the primary.

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



#### Note

---

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

---

### Switching a VDSM from Warm Standby to Primary

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

```
ServiceBroker# configure
ServiceBroker(config)# VDSM 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 VDSM. 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 VDSM has fully replicated the primary VDSM configuration. If the update time is not current, check whether there is a connectivity problem or if the primary VDSM 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 VDSMs have the same Coordinated Universal Time (UTC) configured.

---

If you switch a warm standby VDSM to primary while your primary VDSM is still online and active, both VDSMs detect each other, automatically shut themselves down, and disable management services. The VDSMs 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 VDSM:

```
VDSM(config)# VDSM ip 10.1.1.1
VDSM(config)# VDSM role primary
```

The following example shows how to configure a new GUI port to access the VDSM GUI:

```
VDSM(config)# VDSM ui port 8550
```

The following example shows how to configure the VDSM as the standby VDSM:

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

The following example shows how to configure the standby VDSM with the IP address of the primary VDSM by using the **VDSM ip ip-address** command. This command associates the device with the primary VDSM so that it can be approved as a part of the network.

```
VDSM# VDSM ip 10.1.1.1
```

# 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.

---

**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 SB:

```
ServiceBroker# whoami  
admin
```

---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>pwd</b>	Displays the present working directory.

---

# write

To save startup configurations, use the **write** command in EXEC configuration mode.

**write [erase | memory | terminal]**

Syntax Description	
<b>erase</b>	(Optional) Erases the startup configuration from NVRAM.
<b>memory</b>	(Optional) Writes the configuration to NVRAM. This setting is the default.
<b>terminal</b>	(Optional) Writes the configuration to a terminal session.

**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 SB.

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 VDS-SB 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 VDS-SB 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 SB is erased.

**Examples**

The following command saves the running configuration to NVRAM:

```
ServiceBroker# write memory
```

**Related Commands**

Command	Description
<b>copy</b>	Copies the configuration or image files to and from the CD-ROM, flash memory, disk, or remote hosts.
<b>show running-config</b>	Displays the current operating configuration.

■ write



# A

## Acronyms

---

[Table A-1](#) defines the acronyms and abbreviations that are used in this publication.

*Table A-1 List of Acronyms*

<b>Acronym</b>	<b>Expansion</b>
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
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

**Table A-1**      *List of Acronyms (continued)*

<b>Acronym</b>	<b>Expansion</b>
CSS	Content Services Switch
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

Table A-1 List of Acronyms (continued)

<b>Acronym</b>	<b>Expansion</b>
LRU	least-recently-used
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
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)

<b>Acronym</b>	<b>Expansion</b>
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
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
SB	Service Broker
SCSI	Small Computer Systems Interface
SDP	Session Description Protocol
SE-NM	Service Broker 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
SRAM	static random-access memory
SRHP	service routing host packet
SRM	Send Routing Message
SSH	Secure Shell
SSL	Secure Sockets Layer
SSN	Send Sequence Number
swfs	software file system
sysfs	system file system
syslog	system logging
TAC	Technical Assistance Center
TACACS+	Terminal Access Controller Access Control System Plus

*Table A-1 List of Acronyms (continued)*

<b>Acronym</b>	<b>Expansion</b>
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
VDS	Videoscape Distribution Suite
VDS-SB	Videoscape Distribution Suite Service Broker
VOD	video on demand
VSF	Virtual Service Broker
VDSM	Virtual Distribution Suite Manager
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





## 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)*

<b>Time Zone</b>	<b>Offset from UTC</b>
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)*

<b>Time Zone</b>	<b>Offset from UTC</b>
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/Fakaofu	-10
Pacific/Fiji	+12
Pacific/Funafuti	+12
Pacific/Galapagos	-6
Pacific/Guadalcanal	+11
Pacific/Guam	+10
Pacific/Johnston	-10
Pacific/Kiritimati	+14
Pacific/Kosrae	+11
Pacific/Kwajalein	+12
Pacific/Majuro	+12
Pacific/Marquesas	-9.30
Pacific/Midway	-11
Pacific/Nauru	+12
Pacific/Niue	-11
Pacific/Norfolk	+11.30
Pacific/Noumea	+11
Pacific/Palau	+9
Pacific/Ponape	+11
Pacific/Port_Moresby	+10
Pacific/Rarotonga	-10

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)*

<b>Time Zone</b>	<b>Offset from UTC</b>
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) [4-325, 4-333](#)
- ? (question mark) [2-81](#)
- ... (ellipsis) [4-333](#)
- .bin files
  - installing [2-84](#)
- .pax files
  - installing [2-84](#)
- (hyphen) [2-82, 4-333](#)
- / (slash) [2-22](#)

---

### A

#### access lists

- configuration, displaying [3-151](#)
- configuring [2-13](#)
- enabling [2-13](#)
- group names [2-14](#)
- interfaces and applications
  - applying to [2-99](#)
- statistics
  - displaying [3-221, 3-223](#)

#### ACLs

- See IP ACLs

#### ACPI

- models supporting [4-272](#)

#### admission control

- statistics
  - displaying [3-224](#)

#### address translation tables [3-155](#)

#### administrative login authentication and authorization

- RADIUS

- enabling and disabling [3-136](#)

#### TACACS+

- enabling and disabling [4-301](#)

#### administrative privileges

- users, clearing [2-28](#)

#### alarm information

- for all alarms [3-152](#)
- for critical alarms [3-153](#)
- for major alarms [3-153](#)
- for minor alarms [3-153](#)

#### alarms

- displaying status and history [3-152](#)

#### alarm traps

- configuring [4-282](#)
- generating [4-282](#)

#### Apache CLF transaction log format [4-333](#)

#### applications

- applying access lists to [2-99](#)

#### archive log file

- compressing [4-338](#)
- marking beginning and end [4-333](#)
- maximum size [4-333](#)
- naming convention [4-336](#)

#### ARP table, displaying [3-155](#)

#### authentication

- access lists, enabling [2-13](#)
- configuration, displaying [3-156](#)
- users
  - creating [4-353](#)

---

### B

#### banners

- configuration of [2-19](#)
  - displaying [3-157](#)
  - enabling [2-20](#)
  - types of
    - EXEC [2-20](#)
    - login [2-20](#)
    - motd [2-20](#)
  - basic configuration settings
    - setting up [3-147](#)
  - BGP (Border Gateway Protocol)
    - routing table
      - content, displaying [3-191](#)
  - bit rate
    - displaying [3-158](#)
- 
- ## C
- caching services
    - setting up [3-147](#)
  - calendar
    - setting [2-29](#)
  - CAR
    - IP precedence
      - ToS [2-94](#)
  - Centralized Management System
    - See CMS
  - CISCO-ENTITY-ASSET-MIB
    - configuring [2-18](#)
  - Cisco script
    - executing [3-145](#)
  - Cisco Technical Assistance Center (TAC) [4-257](#)
  - classification
    - IP precedence
      - ToS field [2-94](#)
  - clock
    - clearing and setting [2-29](#)
    - daylight saving and local time, setting [2-31](#)
    - displaying standard timezones [3-159](#)
    - Service Engine, synchronizing [3-126](#)
    - software time and date, setting [3-128](#)
    - system clock settings, displaying [3-159](#)
    - UTC current time of day, setting [2-32](#)
    - UTC offset, setting [2-32](#)
  - CMS
    - database, configuring [2-35](#)
    - enabling [2-38](#)
    - maintenance routines, scheduling [2-38](#)
    - process information, displaying [3-162](#)
  - cold restart [3-139](#)
  - command-line processing [1-2](#)
  - command modes
    - EXEC [1-3](#)
    - global configuration [1-4](#)
    - interface configuration [1-4](#)
  - command syntax [1-5](#)
  - configuration modes
    - extended ACL [2-100](#)
    - standard ACL [2-100](#)
  - configuring
    - alarm traps [4-282](#)
    - disk space allocation [2-56](#)
  - console
    - setting length of display [4-317](#)
  - copying
    - configuration data [2-42](#)
    - files [2-44, 2-46](#)
    - image data [2-42](#)
  - custom transaction log format [4-333](#)
    - log format string values [4-334](#)
- 
- ## D
- date and time
    - setting [3-128](#)
  - daylight saving time
    - setting [2-31](#)
  - debug
    - disabling [4-347](#)

- information, displaying [3-164](#)
    - software functions [2-47](#)
  - debugshell
    - configuring [2-71](#)
  - default gateway
    - defining [2-90](#)
    - removing [2-90](#)
  - default status
    - restoring [3-141](#)
  - deleting
    - directories [2-51, 3-144](#)
    - directory trees [2-51](#)
    - files [2-50](#)
  - device mode
    - and linked CLI commands [1-1](#)
    - configuring [2-52](#)
    - displaying [3-165](#)
  - devices
    - shutting down [4-272](#)
  - differentiated service model
    - classification [2-94](#)
  - directories
    - changing [2-22](#)
    - creating [3-115](#)
    - deleting [2-51, 3-144](#)
    - files, viewing [2-54, 3-109](#)
  - disk drives
    - error handling thresholds
      - description of [2-63](#)
      - specifying [2-63](#)
  - disks
    - configuring [2-56](#)
      - space allocation [2-56](#)
    - details, viewing [3-167](#)
    - partitions, removing [3-141](#)
    - space allocation [2-56](#)
  - disk space allocated to system use [2-56](#)
  - DNS lookup [2-65](#)
  - domain name
    - resolving to IP address [2-65](#)
  - dumping network traffic [4-305, 4-310](#)
  - DWRED
    - IP precedence
      - ToS [2-94](#)
- 
- E
  - echo packets
    - sending [3-129](#)
  - ellipsis (...) [4-333](#)
  - embedded database parameters
    - configuring [2-34](#)
  - enabling
    - RADIUS authentication and authorization [3-137](#)
    - TACACS+ authentication and authorization [4-301](#)
  - exclamation point (!) [4-325, 4-333](#)
  - EXEC command mode
    - described [1-3](#)
    - returning to [2-70](#)
  - exiting
    - from configuration modes [2-70](#)
    - from privileged EXEC mode [2-55](#)
  - exporting transaction logs
    - forced [4-326](#)
    - to FTP server [4-338](#)
    - to SFTP server [4-338](#)
  - extended access lists [2-100](#)
  - extended IP ACLs
    - configuration examples [2-106](#)
    - configuring [2-101](#)
    - ICMP message types [2-104](#)
    - supported keywords [2-103](#)
    - TCP keywords [2-104](#)
  - Extended Squid transaction log format [4-333](#)
  - external FTP server
    - exporting transaction logs to [4-338](#)
    - permanent error from [4-339](#)

---

**F**

## field descriptor limit

## statistics

displaying [3-226](#)

## file

copying [2-46](#)creating [3-116, 4-326](#)deleting [2-50](#)displaying name [3-109, 4-342](#)management [2-22](#)renaming [3-140](#)

## flash memory

configuring upon reload [3-139](#)data, removing [3-141](#)version and usage, displaying [3-172](#)**FTP**access lists [2-101](#)caching configuration, displaying [3-174](#)enable [2-76](#)

## FTP servers

exporting transaction logs to [4-338](#)


---

**G**

## Gigabit Ethernet

configuring [2-85](#)

## global configuration command mode

enable password [2-67](#)entering [2-41](#)exiting [2-68](#)negating command [3-122](#)setting [2-41](#)

## global configuration mode

description [1-4](#)**GMT**UTC and [2-32](#)

## Greenwich Mean Time

See GMT

## group names

access lists [2-14](#)gulp [2-78](#)


---

**H**

## hardware interface

displaying information [3-184](#)shutting down [4-271](#)hardware status, displaying [3-177](#)help system [1-7, 2-81](#)

## history

statistics, clearing [2-25](#)

## hostname

of Service Engine [2-82](#)resolving to IP address [2-65](#)

## hosts

name servers and IP addresses, displaying [3-183](#)**HTTP**status codes [4-333](#)transaction logging [4-332](#)users, managing [4-354](#)hyphen (-) [2-82, 4-333](#)


---

**I**

## I/O statistics

showing [2-89](#)**ICMP**access lists [2-101](#)keywords for message type and code [2-104](#)

## statistics

clearing [2-25](#)displaying [4-227](#)

## image data

copying [2-42](#)

## initial network device settings

changing [2-90](#)

installing system image [2-83, 2-84](#)

interface

- configuring [2-85](#)
- displaying hardware status [3-184](#)
- standby [3-217](#)

interface configuration command mode [1-4](#)

interface IP

- configuring [2-96](#)

Internet socket connection statistics

- displaying [4-237](#)

inventory information

- displaying [3-189](#)

IP ACLs

- activating on an interface [2-106](#)
- clearing IP ACL counter [2-23](#)
- creating and modifying [2-99](#)
- description of [2-102](#)
- extended configuration mode
  - accessing [2-101](#)
- extended IP ACLs [2-103](#)
- standard configuration mode
  - accessing [2-100](#)
- standard IP ACLs [2-103](#)
- typical uses of [2-102](#)

IP address

- starting autodiscovery utility [2-91](#)
- statistics, clearing [2-25](#)
- Virtual Origin Server Manager, configuring [4-356](#)

IP default domain name

- defining [2-91](#)
- removing [2-91](#)

IP default gateway

- defining [2-90](#)
- removing [2-90](#)

IP precedence

- edge function [2-94](#)
- ToS field
  - classification [2-94](#)

IP statistics, display [4-233](#)

---

## K

kernel debugger [2-107](#)

keystroke combinations, CLI [1-2](#)

---

## L

launching

- Setup utility [3-147](#)

lists

- directory names [3-109](#)
- file [3-114](#)

load balancing

- for port channel [3-130](#)

log file

- number of lines to view [4-344](#)

log files

- exporting [4-336](#)
- restarting the export of [4-340](#)

logging

- configuring [3-110](#)
- file rotation of logs [3-112](#)
- RealProxy errors [3-113](#)

logging in

- to Service Engine
  - using SSH [4-297, 4-298](#)
  - using Telnet [4-316](#)

---

## M

mapping syslog priority levels to RealProxy error codes [3-113](#)

MIB view

- defining [4-293](#)

modes

- command
  - EXEC [1-3](#)
  - global configuration [1-4](#)
  - interface configuration [1-4](#)

configuration

- extended ACL [1-4](#)
- HTTP server [1-4](#)
- standard ACL [1-4](#)

mount option

- configuring [3-118](#)

mpstat

- displaying statistics [3-119](#)

multicast

- disabling backup senders [2-39](#)

---

N

NAT

- configuring [2-72](#)

negating interface configurations [3-124](#)

netmon [3-120](#)

netstat [3-121](#)

Network Address Translation

- See NAT

network connectivity

- testing [3-129](#)

network host name

- Service Engine [2-82](#)

network interfaces

- EtherChannel [2-87](#)

Network Time Protocol

- See NTP

network traffic

- dumping [4-305, 4-310](#)

node

- activating [2-35](#)
- communication over secure channels [2-34](#)

NTP

- configuring and enabling [3-126](#)
- setting software time and date [3-128](#)
- status, displaying [3-197, 3-198](#)
- system clock, synchronizing [3-126](#)

number of lines displayed [4-317](#)

NVRAM

- configuration stored, displaying [3-218](#)
- startup configuration, writing or erasing [4-360](#)

---

## O

offset from UTC [B-1](#)

online help [2-81](#)

---

## P

patterns

- searching in files [2-74](#)

permanent errors

- FTP server [4-339](#)

ping [3-129](#)

port channel

- configuring [2-85](#)
- load balancing options [3-130](#)

powering off [4-272](#)

present working directory

- information, displaying [3-109, 3-134](#)

preserving configurations on device restore [3-141](#)

preserving data on device restore [3-141](#)

primary interface

- changing to a different interface [3-132](#)
- configuring for Ethernet [3-132](#)

privileged level EXEC commands

- accessing [2-66](#)
- disabling [2-55](#)

processes

- CPU or memory, displaying [3-200](#)

---

## Q

question mark (?) [2-81](#)

- 
- R**
- RADIUS server
    - authentication [3-135](#)
    - excluding domains [3-136](#)
    - information, displaying [3-202](#)
    - parameters, configuring [3-135](#)
    - statistics
      - clearing [2-25](#)
      - displaying [4-238](#)
  - RealProxy
    - error logging [3-113](#)
  - rebooting Service Engine [3-139](#)
  - regular pattern expression
    - searching [2-74](#)
  - reload [3-139](#)
  - reloading Service Engine
    - automatic reload option [2-63](#)
  - remote host route trace [4-323](#)
  - removing
    - nodes from the VDS-OS network [2-35](#)
  - renaming a file [3-140](#)
  - resetting
    - device to default condition [3-141](#)
  - restart, cold [3-139](#)
  - restoring
    - device to default condition [3-141](#)
  - rotated log files [3-112](#)
  - routes
    - tracing [4-323](#)
  - running configuration
    - current profile, displaying [3-204](#)
    - saving [4-360](#)
  - running statistics, clearing [2-25](#)
- 
- S**
- saving
    - configuration changes [1-7](#)
  - file system contents [3-139](#)
  - script
    - executing [3-145](#)
  - secret keys
    - RADIUS [3-136](#)
    - TACACS+ [4-302](#)
  - Secure Shell
    - See SSH
  - send echo packets (ping) [3-129](#)
  - service [3-146](#)
  - Service Engine
    - automatic reload [2-63](#)
  - Service Router
    - configuration [3-208](#)
  - services
    - access lists [2-99](#)
    - information [3-210](#)
    - statistics [4-239](#)
  - setup
    - configuring [3-147](#)
  - shutting down
    - Content Delivery System Managers [4-272](#)
    - hardware interfaces [4-271](#)
    - Program Managers [4-272](#)
    - Service Engines [4-272](#)
    - Service Routers [4-272](#)
  - slash (/) [2-22](#)
  - SNMP
    - communications status, displaying [3-212](#)
    - community string, configuring [4-280](#)
    - host trap recipient, setting [4-286](#)
    - security model group, defining [4-284](#)
    - server user, defining [4-291](#)
    - statistics, clearing [2-25](#)
    - statistics, displaying [4-240](#)
    - system location string, setting [4-288](#)
    - system notify inform string, configuring [4-289](#)
    - system server contact string, setting [4-281](#)
    - traps, configuring [4-282](#)

- traps, disabling [4-282](#)
  - traps, enabling [4-282](#)
  - Version 2 MIB view, defining [4-293](#)
  - socket connection
    - statistics, displaying [4-237](#)
  - software clock
    - setting [3-128](#)
  - source IP routing
    - configuring [2-91](#)
  - Squid transaction log format [4-333](#)
  - ss [4-295](#)
  - SSH
    - configuration and status, displaying [3-216](#)
    - enabling daemon [4-298](#)
    - generating host key [4-297](#)
    - session timeout [2-69](#)
  - standard access lists
    - creating [2-100](#)
  - standard time zones
    - and offsets from UTC [B-1](#)
    - list of [B-1](#)
  - standard timezones, displaying [3-159](#)
  - standby interface
    - displaying information [3-217](#)
  - starting service [3-146](#)
  - startup configuration
    - displaying [3-218](#)
  - static IP routing
    - configuring [2-91](#)
  - statistics
    - clearing [2-25](#)
  - subdirectories
    - viewing names [3-109](#)
  - summer daylight saving time
    - setting [2-31](#)
  - synchronizing
    - system clock [3-126](#)
  - syslog
    - configuration, displaying [3-195](#)
    - configuring [3-110](#)
    - hosts, configuring [3-112](#)
    - RealProxy priority level error mapping [3-113](#)
    - sysfs location [3-112](#)
  - system clock
    - synchronized by time server [3-126](#)
  - system disk space usage [2-56](#)
  - system hardware
    - displaying status [3-177](#)
  - system help [1-7](#)
  - system image
    - installing [2-84](#)
  - system inventory
    - displaying [3-189](#)
  - system logging
    - configuring [3-112](#)
    - to console [3-110](#)
    - to disk [3-110](#)
    - to remote hosts [3-112](#)
- 
- T
  - TAC
    - viewing technical support information [4-257](#)
  - TACACS+
    - authentication information, displaying [4-255](#)
    - configuring server parameters [4-301](#)
    - statistics
      - clearing [2-25](#)
      - displaying [4-242](#)
  - TCP
    - access lists [2-101](#)
    - keywords and port numbers [2-104](#)
    - statistics
      - clearing [2-25](#)
      - displaying [4-243](#)
    - timestamp [4-314](#)
  - tcpmon [4-312](#)
  - technical support information

- viewing [4-257](#)
  - Telnet services
    - configuration, displaying [4-261](#)
    - enabling [4-316](#)
    - session timeout [2-3, 2-69](#)
  - terminal
    - setting number of lines to be displayed [4-317](#)
  - testing
    - connectivity of URLs
      - for FTP-over-HTTP [4-319](#)
      - for HTTP [4-319](#)
  - test-url command
    - troubleshooting
      - with the HTTP CLI client [4-319](#)
  - TFTP
    - access lists [2-101](#)
  - thresholds
    - disk error handling [2-63](#)
  - time and date
    - setting [3-128](#)
  - timeout of a nonresponsive host [3-129](#)
  - timestamp
    - TCP [4-314](#)
  - time zone
    - list of [B-1](#)
    - offset setting [2-32](#)
    - setting [2-31](#)
  - token strings [4-333](#)
  - ToS
    - classification [2-94](#)
  - trace the route of remote host [4-323](#)
  - transaction logging
    - archive file naming convention [4-336](#)
    - archiving working log files [2-27](#)
    - compressing archive files [4-338](#)
    - configuration and archived files, displaying [4-262](#)
    - configuring and enabling [4-328](#)
    - exporting [4-338](#)
    - forcing archive or export [4-326](#)
    - formats [4-333](#)
    - log export statistics, displaying [4-252](#)
    - permanent errors from external server [4-339](#)
  - transaction logs
    - archiving of [4-336](#)
    - clearing [2-27](#)
    - displaying configuration of [4-262](#)
    - exporting [4-336](#)
    - sanitizing [4-335](#)
  - traps
    - enabling [4-282](#)
  - troubleshooting
    - with ping [3-129](#)
    - with Telnet client [4-315](#)
    - with the HTTP CLI client [4-319](#)
    - with traceroute [4-323](#)
  - troubleshooting utilities
    - gulp [2-78](#)
    - netmon [3-120](#)
    - netstatr [3-121](#)
    - ss [4-295](#)
    - tcpmon [4-312](#)
- 
- U
  - UDI compliance [3-189](#)
  - UDP
    - access lists [2-101](#)
    - keywords and port numbers [2-103](#)
    - statistics
      - clearing [2-25](#)
      - displaying [4-254](#)
  - undoing global configuration commands [3-122](#)
  - Universal Coordinated Time
    - See UTC [B-1](#)
  - updating the calendar [2-29](#)
  - URL signature [4-349](#)
    - information, displaying [4-266](#)
    - shared key [4-351](#)

user-level EXEC command mode [1-3](#)

username

displaying [4-359](#)

users

administrative and authenticated, displaying [4-268](#)

authenticated users, clearing [2-28](#)

authentication [4-353](#)

defining for SNMP server [4-291](#)

removing data from disk [3-141](#)

user identification number and name,  
displaying [4-267](#)

UTC

and standard time zones [B-1](#)

clock EXEC command [2-32](#)

offsets from [B-1](#)

---

## V

VDS-OS

installing [2-83, 2-84](#)

version

displaying information about [4-269](#)

Virtual Origin Server Manager

configuring IP address [4-356](#)

primary role [2-34](#)

SSL [2-35](#)

---

## W

WFQ

IP precedence

ToS [2-94](#)

working.log file [4-332](#)