



Cisco Wide Area Application Services Command Reference

Software Release 4.0.19
June 11, 2008

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-16377-01

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

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

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

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

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

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0805R)

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 Wide Area Application Services Command Reference
© 2006-2008 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface **xiii**

- Audience **xiii**
- Document Organization **xiv**
- Document Conventions **xv**
- Related Documentation **xv**
- Obtaining Documentation and Submitting a Service Request **xvi**

CHAPTER 1

Using the WAAS Command-Line Interface **1-1**

- Using Command Modes **1-1**
 - Organization of the WAAS CLI **1-2**
 - Using EXEC Mode **1-2**
 - Using Global Configuration Mode **1-3**
 - Using the Interface Configuration Mode **1-4**
 - Using ACL Configuration Modes **1-4**
 - Command Modes Summary **1-5**
 - Device Mode **1-5**
- Using Command-Line Processing **1-6**
- Checking Command Syntax **1-7**
- Using the no Form of Commands **1-8**
- Using System Help **1-9**
- Saving Configuration Changes **1-9**
- Navigating the WAAS Directories on a WAE **1-9**
 - Directory Descriptions **1-11**
- Managing WAAS Files Per Device **1-12**

CHAPTER 2

Cisco WAAS Software Command Summary **2-1**

CHAPTER 3

CLI Commands **3-1**

EXEC Mode Commands **3-2**

- cd **3-3**
- cifs **3-4**
- clear **3-5**

clear users 3-8

clock 3-10

cms 3-11

cms secure-store 3-14

configure 3-16

copy cdrom 3-17

copy compactflash 3-18

copy disk 3-19

copy ftp 3-20

copy http 3-25

copy running-config 3-29

copy startup-config 3-30

copy sysreport 3-31

copy system-status 3-33

copy tech-support 3-34

copy tftp 3-35

cpfile 3-37

debug 3-38

delfile 3-44

deltree 3-45

dir 3-46

disable 3-48

disk 3-49

dnslookup 3-53

enable 3-54

exit 3-55

find-pattern 3-56

help 3-58

install 3-59

less 3-61

lls 3-62

ls 3-64

mkdir 3-66

mkfile 3-67

ntpdate 3-68

ping	3-69
pwd	3-70
reload	3-71
rename	3-72
restore	3-73
rmdir	3-77
scp	3-78
script	3-80
setup	3-81
show aaa accounting	3-82
show adapter	3-84
show alarms	3-85
show arp	3-88
show authentication	3-89
show auto-register	3-91
show banner	3-92
show bypass	3-93
show cdp	3-94
show cifs	3-100
show clock	3-102
show cms	3-104
show cms secure-store	3-107
show debugging	3-108
show device-mode	3-109
show disks	3-111
show egress-methods	3-118
show flash	3-119
show hardware	3-120
show hosts	3-123
show inetd	3-124
show interface	3-125
show inventory	3-130
show ip access-list	3-131
show ip routes	3-133
show kerberos	3-134

show key-manager 3-135

show logging 3-136

show memory 3-137

show ntp 3-138

show policy-engine application 3-140

show policy-engine status 3-144

show print-services 3-146

show processes 3-148

show radius-server 3-150

show running-config 3-152

show services 3-154

show smb-conf 3-155

show snmp 3-157

show ssh 3-163

show standby 3-164

show startup-config 3-166

show statistics authentication 3-168

show statistics cifs 3-169

show statistics content-distribution-network 3-171

show statistics dre 3-172

show statistics dre connection 3-174

show statistics dre peer 3-176

show statistics epm 3-179

show statistics flow 3-180

show statistics icmp 3-183

show statistics ip 3-185

show statistics key-manager 3-188

show statistics netstat 3-189

show statistics radius 3-190

show statistics services 3-192

show statistics snmp 3-193

show statistics tacacs 3-195

show statistics tcp 3-197

show statistics tfo 3-203

show statistics udp 3-205

[show statistics wccp](#) 3-206
[show statistics windows-domain](#) 3-211
[show sysfs volumes](#) 3-213
[show tacacs](#) 3-214
[show tcp](#) 3-216
[show tech-support](#) 3-218
[show telnet](#) 3-221
[show tfo accelerators](#) 3-222
[show tfo auto-discovery](#) 3-223
[show tfo bufpool](#) 3-225
[show tfo connection](#) 3-227
[show tfo egress-methods connection](#) 3-229
[show tfo filtering](#) 3-233
[show tfo status](#) 3-235
[show tfo synq](#) 3-236
[show transaction-logging](#) 3-237
[show user](#) 3-238
[show users administrative](#) 3-239
[show version](#) 3-241
[show wccp](#) 3-242
[show windows-domain](#) 3-248
[shutdown](#) 3-250
[snmp trigger](#) 3-253
[ssh](#) 3-256
[tcpdump](#) 3-257
[telnet](#) 3-259
[terminal](#) 3-260
[tethered](#) 3-261
[traceroute](#) 3-263
[transaction-log](#) 3-264
[type](#) 3-265
[type-tail](#) 3-266
[undebug](#) 3-268
[wafs](#) 3-273
[whoami](#) 3-275

windows-domain 3-276

write 3-279

Configuration Mode Commands 3-280

(config) aaa accounting 3-281

(config) adapter 3-285

(config) alarm overload-detect 3-286

(config) asset 3-288

(config) authentication 3-289

(config) authentication strict-password-policy 3-294

(config) auto-register 3-296

(config) banner 3-299

(config) bypass 3-302

(config) cdp 3-304

(config) central-manager 3-306

(config) clock 3-310

(config) cms 3-314

(config) device mode 3-316

(config) disk disk-name 3-318

(config) disk encrypt enable 3-320

(config) disk error-handling 3-322

(config) disk logical shutdown 3-324

(config) egress-method 3-325

(config) end 3-327

(config) exec-timeout 3-328

(config) exit 3-329

(config) external-ip 3-330

(config) flow monitor 3-332

(config) help 3-333

(config) hostname 3-335

(config) inetd enable 3-337

(config) interface 3-338

(config) ip 3-344

(config) ip access-list 3-347

(config) kerberos 3-350

(config) kernel kdb 3-352

(config) line	3-353
(config) logging	3-354
(config) no	3-358
(config) ntp	3-360
(config) policy-engine application classifier	3-362
(config) policy-engine application map adaptor EPM	3-364
(config) policy-engine application map adaptor WAFS transport	3-366
(config) policy-engine application map basic delete	3-368
(config) policy-engine application map basic disable	3-369
(config) policy-engine application map basic insert	3-370
(config) policy-engine application map basic list	3-371
(config) policy-engine application map basic move	3-372
(config) policy-engine application map basic name	3-374
(config) policy-engine application map other optimize DRE	3-376
(config) policy-engine application map other optimize full	3-378
(config) policy-engine application map other pass-through	3-379
(config) policy-engine application name	3-380
(config) policy-engine config	3-382
(config) port-channel	3-383
(config) primary-interface	3-384
(config) print-services	3-386
(config) radius-server	3-389
(config) smb-conf	3-391
(config) snmp-server access-list	3-395
(config) snmp-server community	3-396
(config) snmp-server contact	3-398
(config) snmp-server enable traps	3-399
(config) snmp-server group	3-402
(config) snmp-server host	3-404
(config) snmp-server location	3-406
(config) snmp-server mib persist event	3-407
(config) snmp-server notify inform	3-409
(config) snmp-server trap-source	3-410
(config) snmp-server user	3-412
(config) snmp-server view	3-414

(config) sshd 3-415

(config) ssh-key-generate 3-418

(config) tacacs 3-419

(config) tcp 3-422

(config) telnet enable 3-425

(config) tfo auto-discovery 3-426

(config) tfo optimize 3-427

(config) tfo tcp keepalive 3-428

(config) tfo tcp optimized-mss 3-429

(config) tfo tcp optimized-receive-buffer 3-430

(config) tfo tcp optimized-send-buffer 3-431

(config) tfo tcp original-mss 3-432

(config) tfo tcp original-receive-buffer 3-433

(config) tfo tcp original-send-buffer 3-434

(config) transaction-logs 3-435

(config) username 3-442

(config) wccp access-list 3-445

(config) wccp flow-redirect enable 3-448

(config) wccp router-list 3-449

(config) wccp shutdown 3-450

(config) wccp tcp-promiscuous 3-452

(config) wccp version 3-454

(config) windows-domain 3-456

Interface Configuration Mode Commands 3-458

(config-if) autosense 3-459

(config-if) bandwidth 3-460

(config-if) cdp 3-462

(config-if) exit 3-463

(config-if) failover timeout 3-464

(config-if) full-duplex 3-465

(config-if) half-duplex 3-467

(config-if) inline 3-469

(config-if) ip 3-471

(config-if) ip access-group 3-473

(config-if) mtu 3-475

(config-if) no 3-476
(config-if) shutdown 3-478
(config-if) standby 3-479

Standard ACL Configuration Mode Commands 3-484

(config) ip access-list standard 3-485
(config-std-nacl) delete 3-488
(config-std-nacl) deny 3-489
(config-std-nacl) exit 3-491
(config-std-nacl) list 3-492
(config-std-nacl) move 3-493
(config-std-nacl) permit 3-494

Extended ACL Configuration Mode Commands 3-496

(config-ext-nacl) delete 3-499
(config-ext-nacl) deny 3-500
(config-ext-nacl) exit 3-505
(config-ext-nacl) list 3-506
(config-ext-nacl) move 3-507
(config-ext-nacl) permit 3-508

APPENDIX A

Acronyms and Abbreviations A-1

**CLI COMMAND
SUMMARY BY
MODE**



Preface

This preface describes who should read the *Cisco Wide Area Application Services Command Reference*, how it is organized, and its document conventions. It contains the following sections:

- [Audience, page xiii](#)
- [Document Organization, page xiv](#)
- [Document Conventions, page xv](#)
- [Related Documentation, page xv](#)
- [Obtaining Documentation and Submitting a Service Request, page xvi](#)

Audience

This command reference is intended for administrators who want to use the command-line interface (CLI) of the Wide Area Application Services (WAAS) software to configure, manage, and monitor WAAS devices on a per-device basis. This guide assumes that the WAAS device is running the WAAS software. The guide provides descriptions and syntax of the WAAS CLI command.

The WAAS CLI allows you to configure, manage, and monitor WAAS devices on a per-device basis through a console connection or a terminal emulation program. The WAAS CLI also allows you to configure certain features that are only supported through the WAAS CLI (for example, configuring LDAP signing on a WAE).

The instructions and examples in this guide describe only those features that can be configured on an individual WAAS device using the WAAS CLI.

In addition to the WAAS CLI, there are three WAAS graphical user interfaces (GUIs) that you access from your browser:

- The WAAS Central Manager GUI allows you to centrally configure, manage, and monitor a WAE or group of WAEs that are registered with the WAAS Central Manager. You also use this GUI to configure, manage, and monitor the WAAS Central Manager, which is the dedicated appliance on which the WAAS Central Manager GUI is running.



Note

When you use the WAAS Central Manager GUI, you have the added capability of centrally configuring settings and policies for groups of WAEs (device groups). When you use the WAAS CLI, you can only configure settings and policies on a per-device basis.

- The WAE Device Manager GUI allows you to remotely configure, manage, and monitor an individual WAE through your browser. In many cases, the same device settings can be found in both the WAE Device Manager GUI and the WAAS Central Manager GUI. For this reason, we strongly recommend that you always configure a WAE from the WAAS Central Manager GUI whenever possible.
- The WAAS Print Services Administration GUI allows you to remotely configure an individual WAAS print server and view a list of active and completed print jobs. You can access the WAAS Print Services Administration GUI from either the WAAS Central Manager GUI or the WAE Device Manager GUI.

The WAAS GUIs are the primary resources for configuration and monitoring WAEs. We strongly recommend that you use the WAAS Central Manager GUI instead of the WAAS CLI, whenever possible. For more information about how to use the WAAS GUIs to configure, manage, and monitor your WAAS devices, see the *Cisco Wide Area Application Services Configuration Guide*.

We recommend that you be familiar with the basic concepts and terminology used in internetworking, in your network topology, and in the protocols that the devices in your network can use. We also recommend that you have a working knowledge of the operating systems on which you are running your WAAS network, such as Microsoft Windows, Linux, or Solaris. This guide is not a tutorial.

Document Organization

This command reference includes the following chapters:

Chapter	Description
Chapter 1, “Using the WAAS Command-Line Interface”	Describes how to use the command-line interface.
Chapter 2, “Cisco WAAS Software Command Summary”	Lists WAAS software commands, providing a brief description of each.
Chapter 3, “CLI Commands”	Provides detailed information for the following types of CLI commands for the WAAS software: <ul style="list-style-type: none"> • Commands you can enter after you log in to the WAAS device (EXEC mode). • Configuration mode commands that you can enter after you log in to the WAAS device, and then access configuration mode and its subset of modes. The description of each command includes: <ul style="list-style-type: none"> • The syntax of the command • Any related commands, when appropriate
Appendix A, “Acronyms and Abbreviations”	Defines the acronyms used in this publication.
“CLI Command Summary by Mode”	Lists each command by command mode.

Document Conventions

This command reference uses these basic conventions to represent text and table information:

Convention	Description
boldface font	Commands, keywords, and button names are in boldface .
<i>italic font</i>	Variables for which you supply values are in <i>italics</i> . Directory names and filenames are also in italics.
screen font	Terminal sessions and information the system displays are printed in <code>screen font</code> .
boldface screen font	Information you must enter is in boldface screen font .
<i>italic screen font</i>	Variables you enter are printed in <i>italic screen font</i> .
plain font	Enter one of a range of options as listed in the syntax description.
^D or Ctrl-D	Hold the Ctrl key while you press the D key.
string	Defined as a nonquoted set of characters. For example, when setting a community string for SNMP to “public,” do not use quotation marks around the string, or the string will include the quotation marks.
Vertical bars ()	Vertical bars separate alternative, mutually exclusive, elements.
{ }	Elements in braces are required elements.
[]	Elements in square brackets are optional.
{x y z}	Required keywords are grouped in braces and separated by vertical bars.
[x y z]	Optional keywords are grouped in brackets and separated by vertical bars.
[{ }]	Braces within square brackets indicate a required choice within an optional element.



Note

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

For additional information on the Cisco WAAS software, see the following documentation:

- *Release Note for Cisco Wide Area Application Services*
- *Cisco Wide Area Application Services Configuration Guide*
- *Cisco Wide Area Application Services Quick Configuration Guide*

- *Cisco Wide Area Application Services Command Reference* (this manual)
- *Regulatory Compliance and Safety Information for the Cisco Content Networking Product Series*
- *Cisco Wide Area Application Engine 511 and 611 Hardware Installation Guide*
- *Cisco Wide Area Application Engine 512 and 612 Hardware Installation Guide*
- *Cisco Wide Area Application Engine 7326 Hardware Installation Guide*
- *Cisco Wide Area Application Engine 7341, 7371, and 674 Hardware Installation Guide*
- *Cisco Network Modules Hardware Installation Guide*
- *Using the Print Utilities to Troubleshoot and Fix Samba Driver Installation Problems*

The following sections provide sources for obtaining documentation from Cisco Systems.

Obtaining Documentation and Submitting a Service Request

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

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

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



CHAPTER 1

Using the WAAS Command-Line Interface

The Cisco WAAS software command-line interface (CLI) is used in combination with the WAAS Manager GUI to configure, monitor, and maintain a WAAS device. The CLI on a WAAS device can be accessed directly through the console port of an attached PC or remotely through a Telnet session on a PC running terminal emulation software.



Note

The WAAS software runs on the WAE-511, WAE-512, WAE-611, WAE-612, WAE-7326, WAE-7341, and WAE-7371. You must deploy the WAAS Central Manager on a dedicated appliance.

Throughout this book, the term WAE is used to refer collectively to the supported WAE platforms unless otherwise noted. For simplification, the term WAAS device is used to refer collectively to WAAS Central Managers and WAEs that are running the WAAS software.

This chapter provides an overview of how to use the WAAS CLI, including an explanation of CLI command modes, navigation and editing features, and help features.

This chapter includes the following sections:

- [Using Command Modes, page 1-1](#)
- [Using Command-Line Processing, page 1-6](#)
- [Checking Command Syntax, page 1-7](#)
- [Using the no Form of Commands, page 1-8](#)
- [Using System Help, page 1-9](#)
- [Saving Configuration Changes, page 1-9](#)
- [Navigating the WAAS Directories on a WAE, page 1-9](#)
- [Managing WAAS Files Per Device, page 1-12](#)

Using Command Modes

The CLI for WAAS software is similar to the CLI for Cisco IOS software. Like Cisco IOS software, the WAAS CLI is organized into different command and configuration modes. Each mode provides access to a specific set of commands. This section describes the command modes provided by the WAAS software CLI and includes the following topics:

- [Organization of the WAAS CLI, page 1-2](#)
- [Using EXEC Mode, page 1-2](#)

- [Using Global Configuration Mode, page 1-3](#)
- [Using the Interface Configuration Mode, page 1-4](#)
- [Using ACL Configuration Modes, page 1-4](#)
- [Command Modes Summary, page 1-5](#)
- [Device Mode, page 1-5](#)

Organization of the WAAS CLI

The WAAS software CLI is organized into multiple command modes. Each command mode has its own set of commands to use for the configuration, maintenance, and monitoring of a WAAS WAE. The commands available to you at any given time depend on the mode you are in. Entering a question mark (?) at the system prompt allows you to obtain a list of commands available for each command mode.

The WAAS command modes include the following:

- EXEC mode—For setting, viewing, and testing system operations. This mode is divided into two access levels: user and privileged. To use the privileged access level, enter the **enable** command at the user access level prompt, and then enter the privileged EXEC password when you see the password prompt.
- Global configuration mode—For setting, viewing, and testing configuration of WAAS software features for the entire device. To use this mode, enter the **configure** command from privileged EXEC mode.
- Interface configuration mode—For setting, viewing, and testing the configuration of a specific interface. To use this mode, enter the **interface** command from global configuration mode.
- Standard ACL configuration mode—For creating and modifying standard access lists on a WAAS device for controlling access to interfaces or applications. To use this mode, enter the **ip access-list standard** command from global configuration mode.
- Extended ACL configuration mode—For creating and modifying extended access lists on a WAAS device for controlling access to interfaces or applications. To use this mode, enter the **ip access-list extended** command.

Use specific commands to navigate from one command mode to another. Use this standard order to access the modes: user EXEC mode, privileged EXEC mode, global configuration mode, interface configuration mode, standard ACL configuration mode, or extended ACL configuration mode.

Using EXEC Mode

Use the EXEC mode for setting, viewing, and testing system operations. In general, the user EXEC commands allow you to connect to remote devices, change terminal line settings on a temporary basis, perform basic tests, and list system information.

The EXEC mode is divided into two access levels: user and privileged. The user EXEC mode is used by local and general system administrators, while the privileged EXEC mode is used by the root administrator. 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 hostname followed by a right angle bracket (>). You can change the hostname using the **hostname** global configuration

command. 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:

```
WAE> enable
WAE#
```

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

Most EXEC mode commands are one-time commands, such as **show** or **more** commands, which show the current configuration status, and **clear** commands, which clear counters or interfaces. EXEC mode commands are not saved across reboots of the WAE.

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

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

```
--More--
```

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

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

```
WAE# exit
WAE>
```

The EXEC commands are entered in EXEC mode.

Using Global Configuration Mode

Use global configuration mode for setting, viewing, and testing configuration of WAAS software features for the entire device. To enter this mode, enter the **configure** command from privileged EXEC mode. The prompt for global configuration mode consists of the hostname of the WAE followed by (config) and the pound sign (#). You must be in global configuration mode to enter global configuration commands.

```
WAE# configure
WAE(config)#
```

Commands entered in global configuration mode update the running configuration file as soon as they are entered. These changes are not saved into the startup configuration file until you enter the **copy running-config startup-config** EXEC mode command. See the [“Saving Configuration Changes” section on page 1-9](#). Once the configuration is saved, it is maintained across WAE reboots.

You also can use global configuration mode to enter specific configuration modes. From global configuration mode you can enter the interface configuration mode, standard ACL configuration mode, or the extended ACL configuration mode.

From configuration modes, you can enter configuration submodes. Configuration submodes are used for the configuration of specific features within the scope of a given configuration mode. As an example, this chapter describes the subinterface configuration mode, a submode of the interface configuration mode.

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

```
WAE(config)# end
WAE#
```

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.

Configuration changes that you make in global configuration mode on a WAE are propagated to the Centralized Management System (CMS) database on the WAAS Central Manager. CLI changes are sent to the Central Manager after you exit out of configuration mode, or if all configuration mode sessions have been inactive for 10 minutes.

Using the Interface Configuration Mode

Use the interface configuration mode for setting, viewing, and testing the configuration of WAAS 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:

```
WAE# configure
WAE(config)# interface ?
  GigabitEthernet  Select a gigabit ethernet interface to configure
  InlineGroup      Select an inline group interface to configure
  InlinePort       Select an inline port interface to configure
  PortChannel      Ethernet Channel of interfaces
  Standby          Standby groups
WAE(config)# interface gigabitethernet ?
  <1-2>/ GigabitEthernet slot/port
WAE(config)# interface gigabitethernet 1/0
WAE(config-if)#
```

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

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

The interface configuration commands are entered in interface configuration mode.

Using ACL Configuration Modes

From global configuration mode, you can enter the standard and extended ACL configuration modes.

- 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 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 exit an ACL configuration mode, enter **exit** to return to global configuration mode:

```
WAE(config-std-nacl)# exit
WAE(config)#
```

To return to global configuration mode, enter the **exit** command.

Command Modes Summary

Table 1-1 shows a summary of the WAAS command modes.

Table 1-1 WAAS Command Modes Summary

Command Mode	Access Method	Prompt	Exit Method
User EXEC	Log in to WAE.	WAE>	Use the end command.
Privileged EXEC	From user EXEC mode, use the enable EXEC command.	WAE#	To return to user EXEC mode, use the disable command. To enter global configuration mode, use the configure command.
Global configuration	From privileged EXEC mode, use the configure command.	WAE(config)#	To return to privileged EXEC mode, use the exit command or press Ctrl-Z . To enter interface configuration mode, use the interface command.
Interface configuration	From global configuration mode, use the interface command.	WAE(config-if)#	To return to global configuration mode, use the exit command. To return to privileged EXEC mode, use the end command or press Ctrl-Z .
Standard ACL configuration	From global configuration mode, use the ip access-list standard command.	WAE(config-std-nacl)#	To return to global configuration mode, use the exit command. To return to privileged EXEC mode, use the end command or press Ctrl-Z .
Extended ACL configuration	From global configuration mode, use the ip access-list extended command.	WAE(config-ext-nacl)#	To return to global configuration mode, use the exit command. To return to privileged EXEC mode, use the end command or press Ctrl-Z .

Device Mode

The WAAS software provides the ability to specify the device mode of a WAAS device. In a WAAS network, you must deploy a WAAS device in one of the following device modes:

- Central Manager mode—Mode that the WAAS Central Manager device needs to use.
- Application accelerator mode—Mode for a WAAS Accelerator (that is a Core WAE or Edge WAE) that is running the WAAS software. WAEs are used to optimize TCP traffic over your network. When client and server applications attempt to communicate with each other, the network intercepts and redirects this traffic to the WAEs so that they can act on behalf of the client application and the destination server. The WAEs examine the traffic and use built-in application policies to determine whether to optimize the traffic or allow it to pass through your network unoptimized.
- Replication accelerator mode—Mode for a WAAS Accelerator specifically optimized for replication applications running between data centers. This mode is similar to application accelerator mode, but the WAE's optimization policies are tuned for data-center-to-data-center operations.

The default device mode for a WAAS device is application accelerator mode. The **device mode** global configuration command allows you to change the device mode of a WAAS device.

```

waas-cm(config)# device mode ?
  application-accelerator  Configure device to function as a WAAS Engine.
  replication-accelerator  Configure device to function as a WAAS Engine in replication
                           environment.
  central-manager          Configure device to function as a WAAS Central Manager.

```

For example, after you use the WAAS CLI to specify the basic network parameters for the designated WAAS Central Manager (the WAAS device named `waas-cm`) and assign it as a primary interface, you can use the **device mode** configuration command to specify its device mode as `central-manager`.

```

waas-cm# configure
waas-cm(config)#
waas-cm(config)# primary-interface gigabitEthernet 1/0
waas-cm(config)# device mode central-manager
waas-cm(config)# exit
waas-cm# copy run start
waas-cm# reload
Proceed with reload?[confirm] y
Shutting down all services, will Reload requested by CLI@ttyS0.
Restarting system.

```

To display the current mode that the WAAS device is operating in, enter the **show device-mode current EXEC** command:

```

WAE# show device-mode current
Current device mode: application-accelerator

```

To display the configured device mode that has not taken effect, enter the **show device-mode configured EXEC** command. For example, if you had entered the **device mode central-manager** global configuration command on a WAAS device to change its device mode to central manager but have not entered the **copy run start EXEC** command to save the running configuration on the device, then if you were to enter the **show device-mode configured** command on the WAAS device, the command output would indicate that the configured device mode is `central-manager`:

```

WAE# show device-mode configured
Configured device mode: central-manager

```

A WAAS device can operate only in one device mode. The set of WAAS CLI commands that are available vary based on the device mode of the WAAS device.

Using Command-Line Processing

Cisco WAAS 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 also scroll through the last 20 commands stored in the history buffer and enter or edit the command at the prompt. [Table 1-2](#) lists and describes the function performed by the available WAAS command-line processing options.

Table 1-2 Command-Line Processing Keystroke Combinations

Keystroke Combinations	Function
Ctrl-A	Jumps to the first character of the command line.
Ctrl-B or the Left Arrow key	Moves the cursor back one character.
Ctrl-C	Escapes and terminates prompts and tasks.
Ctrl-D	Deletes the character at the cursor.
Ctrl-E	Jumps to the end of the current command line.
Ctrl-F or the Right Arrow key ¹	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 ¹	Enters the next command line in the history buffer.
Ctrl-P or the Up Arrow key ¹	Enters the previous command line in the history buffer.
Ctrl-T	Transposes the character at the cursor with the character to the left of the cursor.
Ctrl-U; Ctrl-X	Deletes from the cursor to the beginning of the command line.
Ctrl-W	Deletes the last word typed.
Esc-B	Moves the cursor back one word.
Esc-D	Deletes from the cursor to the end of the word.
Esc-F	Moves the cursor forward one word.
Delete key or Backspace key	Erases a mistake when entering a command; re-enter the command after using this key.

1. The arrow keys function only on ANSI-compatible terminals such as VT100s.

Checking Command Syntax

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

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

```
WAE# clock 1222
      ^
%Invalid input detected at '^' marker.
WAE# 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.

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

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

```
WAE# 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, and then add a space and question mark (?) to display the additional arguments.

```
WAE# clock set 13:32:00 ?
<1-31> Day of the month
april
august
december
february
january   Month of the Year
july
june
march
may
november
october
september
```

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

```
WAE# clock set 13:32:00 23 December ?
<1993-2035> Year
```

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

```
WAE# clock set 13:32:00 23 December 05 ^
%Invalid input detected at '^' marker.
WAE#
```

The caret symbol (^) and help response indicate an error with the 05 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**.

```
WAE# clock set 13:32:00 23 December ?
<1993-2035> Year
WAE# clock set 13:32:00 23 December
```

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

```
WAE# clock set 13:32:00 23 December 2005
WARNING: Setting the clock may cause a temporary service interruption.
Do you want to proceed? [no] yes
Sat Dec 23 13:32:00 EST 2005
WAE#
```

Using the no Form of Commands

Almost every configuration command has a no form. The **no** form of a command is generally used to disable a feature or function, but it can also be used to set the feature or function to its default values. Use the command without the **no** keyword to reenable a disabled feature or to enable a feature that is disabled by default.

Using 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 (?).

```
WAE# c1?
clear clock
```

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

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

Saving Configuration Changes

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

```
WAE# copy running-config startup-config
```

or

```
WAE# write
```

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

Navigating the WAAS Directories on a WAE

The WAAS CLI provides several commands for navigating among directories and viewing their contents. These commands are entered from privileged EXEC mode. [Table 1-3](#) lists and describes these commands.

Table 1-3 WAAS Navigation Commands

Command	Description
cd [<i>directory-name</i>]	Change Directory—Moves you from the current directory to the specified directory in the WAAS tree. If no directory is specified, cd takes you up one directory.
deltree <i>directory-name</i>	Remove Directory Tree—Deletes the specified directory and all subdirectories and files without displaying a warning message to you.
dir [<i>directory-name</i>]	Show Directory—Lists the size, date of last changes, and the name of the specified directory (or all directories if one is not specified) within the current directory path. The output from this command is the same as the lls command.

Table 1-3 WAAS Navigation Commands (continued)

Command	Description
ls [<i>directory-name</i>]	Show Directory Names—Lists the names of directories in the current directory path.
lls [<i>directory-name</i>]	Show Directory—Lists the size, the date of the last changes, and the name of the specified directory (or all directories if one is not specified) within the current directory path. The output from this command is the same as the dir command.
mkdir <i>directory-name</i>	Create Directory—Creates a directory of the specified name in the current directory path.
pwd	Present Working Directory—Lists the complete path from where this command is entered.
rmdir <i>directory-name</i>	Delete Directory—Removes the specified directory from the current directory path. All files in the directory must first be deleted before the directory can be deleted.

The following example displays a detailed list of all the files for the WAE's current directory:

```

WAE# dir
size          time of last change          name
-----
4096  Fri Feb 24 14:40:00 2006  <DIR>  actona
4096  Tue Mar 28 14:42:44 2006  <DIR>  core_dir
4096  Wed Apr 12 20:23:10 2006  <DIR>  crash
4506  Tue Apr 11 13:52:45 2006  dbupgrade.log
4096  Tue Apr 4 22:50:11 2006  <DIR>  downgrade
4096  Sun Apr 16 09:01:56 2006  <DIR>  errorlog
4096  Wed Apr 12 20:23:41 2006  <DIR>  logs
16384  Thu Feb 16 12:25:29 2006  <DIR>  lost+found
4096  Wed Apr 12 03:26:02 2006  <DIR>  sa
24576  Sun Apr 16 23:38:21 2006  <DIR>  service_logs
4096  Thu Feb 16 12:26:09 2006  <DIR>  spool
9945390  Sun Apr 16 23:38:20 2006  syslog.txt
10026298  Thu Apr 6 12:25:00 2006  syslog.txt.1
10013564  Thu Apr 6 12:25:00 2006  syslog.txt.2
10055850  Thu Apr 6 12:25:00 2006  syslog.txt.3
10049181  Thu Apr 6 12:25:00 2006  syslog.txt.4
4096  Thu Feb 16 12:29:30 2006  <DIR>  var
508  Sat Feb 25 13:18:35 2006  wdd.sh.signed

```

The following example displays only the detailed information for the logs directory:

```

WAE# dir logs
size          time of last change          name
-----
4096  Thu Apr 6 12:13:50 2006  <DIR>  actona
4096  Mon Mar 6 14:14:41 2006  <DIR>  apache
4096  Sun Apr 16 23:36:40 2006  <DIR>  emdb
4096  Thu Feb 16 11:51:51 2006  <DIR>  export
92  Wed Apr 12 20:23:20 2006  ftp_export.status
4096  Wed Apr 12 20:23:43 2006  <DIR>  rpc_httpd
0  Wed Apr 12 20:23:41 2006  snmpd.log
4096  Sun Mar 19 18:47:29 2006  <DIR>  tfo

```

Directory Descriptions

Several top-level directories of the WAAS software contain information used internally by the software and are not useful to you. These directories include the `core_dir`, `crash`, `downgrade`, `errorlog`, `lost+found`, `sa`, `service_logs`, `spool`, and `var` directories.

Table 1-4 describes the directories that contain information that is useful for troubleshooting or monitoring.

Table 1-4 WAAS Directory Descriptions

Directory/File Name	Contents
<code>actona</code>	This directory contains the current software image installed on the WAAS device and any previous images that were installed.
<code>logs</code>	This directory contains application-specific logs used in troubleshooting. The <code>actona</code> subdirectory contains the commonly used <code>Manager.log</code> , <code>Utilities.log</code> , and <code>Watchdog.log</code> log files. See the <i>Cisco Wide Area Application Services Configuration Guide</i> for more details about how these log files are used.
<code>syslog.txt</code>	This file is the central repository for log messages. Important messages about the operation of WAAS or its components are sometimes logged in this file. They are often intermingled with routine messages that require no action. You may be requested to provide this file, the output of the show tech-support EXEC command, and perhaps other output to Cisco TAC personnel if a problem arises.



Note

The WAAS software uses the CONTENT file system for both the Wide Area File Services (WAFS) file system and the data redundancy elimination (DRE) cache.

Managing WAAS Files Per Device

The WAAS CLI provides several commands for managing files and viewing their contents per device. These commands are entered from privileged EXEC mode. [Table 1-5](#) describes the WAAS file management commands.

Table 1-5 WAAS File Management Commands

Command	Description
copy { <i>source</i> <i>image</i> }	Copy—Copies the selected source file, image, or configuration information: <ul style="list-style-type: none"> • <i>cdrom</i>—Copies the file from the CDROM. • <i>compactflash</i>—Copies the file from the CompactFlash card. • <i>disk</i>—Copies the configuration or file from the disk. • <i>ftp</i>—Copies the file from the FTP server. • <i>http</i>—Copies the file from the HTTP server. • <i>running-config</i>—Copies information from the current system configuration. • <i>startup-config</i>—Copies information from the startup configuration. • <i>sysreport</i>—Copies system information. • <i>system-status</i>—Copies the system status for debugging reference. • <i>tech-support</i>—Copies system information for technical support. • <i>tftp</i>—Copies the software image from the TFTP server.
cpfile <i>source-filename</i> <i>destination-filename</i>	Copy File—Makes a copy of a source file, and puts it in the current directory.
delfile <i>filename</i>	Remove File—Deletes the specified file from the current directory path.
less <i>filename</i>	Display File Using LESS—Displays the specified file on the screen using the LESS program. The filename is case sensitive. Enter q to stop viewing the file and return to the directory.
mkfile <i>filename</i>	Create File—Creates a file of the specified name in the current directory path.
rename <i>old-filename</i> <i>new-filename</i>	Rename File—Renames the specified file with a new filename.
type <i>filename</i>	Display File—Displays the content of the specified file on the screen.
type-tail <i>filename</i> [<i>line</i> follow {begin <i>LINE</i> exclude <i>LINE</i> include <i>LINE</i> }]	Display End of File—Displays the last few lines of the specified file. Can also be used to view the last lines of a file continuously as new lines are added to the file, to start at a particular line in the file, or to include or exclude specific lines in the file.
find-pattern <i>pattern</i>	Find in a File—Searches a file for the specified pattern.

The following example shows how to save the currently running configuration to the startup configuration using the **copy** EXEC command:

```
WAE# copy running-config startup-config
```



Note To back up, restore, or create a system report about the WAFS-specific configuration on a WAE, use the **wafs EXEC** command. To save the WAFS-system specific configuration information, use the **wafs backup-config EXEC** command. See the *Cisco Wide Area Application Services Configuration Guide* for more information on backing up.

The following example shows how to remove a file named *sample* from the directory named *test* using the **delfile** command:

```
WAE# cd test
WAE# ls
sample
sample2
WAE# delfile sample
WAE# ls
sample2
```

The following example shows how to view the last lines of the *Watchdog.log* file:

```
WAE# cd logs
WAE# cd actona
WAE# ls
Watchdog.log
WAE# type-tail Watchdog.log
[2006-01-30 15:13:44,769][FATAL] - System got fatal error going to restart.
[2006-03-19 18:43:08,611][FATAL] - System got fatal error going to restart.
[2006-03-19 19:05:11,216][FATAL] - System got fatal error going to restart.
WAE#
```




CHAPTER 2

Cisco WAAS Software Command Summary

This chapter summarizes the Cisco WAAS 4.0.19 software commands.

[Table 2-1](#) lists the WAAS commands (alphabetically) and indicates the command mode for each command. The commands used to access configuration modes are marked with an asterisk. Commands that do not indicate a particular mode are EXEC mode commands. The same command may have different effects when entered in a different command mode, so they are listed and documented separately. (See [Chapter 1, “Using the WAAS Command-Line Interface”](#) for a discussion about using CLI command modes.)

In [Table 2-1](#), in the Device Mode column “All” indicates that the particular CLI command is supported in both central manager mode and application accelerator mode.



Note

When viewing this reference 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.

Throughout this book, the term WAAS device refers collectively to a WAAS Central Manager and a WAE. The term WAE refers collectively to the supported WAE platforms that are running the WAAS software.

Table 2-1 Command Summary

Command	Description	CLI Mode	Device Mode
(config) aaa accounting	Configures AAA accounting.	global configuration	All
(config) adapter	Enables the EndPoint Mapper (EPM) service.	global configuration	application accelerator
(config) alarm overload-detect	Configures the detection of alarm overload.	global configuration	All
(config) asset	Configures the tag name for the asset tag string.	global configuration	All
(config) authentication	Configures administrative login authentication and authorization parameters.	global configuration	All
(config) auto-register	Enables the discovery of a primary interface on a WAE and its automatic registration with the WAAS Central Manager through DHCP.	global configuration	application accelerator
(config-if) autosense	Sets the current interface to autosense.	interface configuration	All

Table 2-1 Command Summary (continued)

Command	Description	CLI Mode	Device Mode
(config-if) bandwidth	Sets the specified interface bandwidth to 10, 100, or 1000 Mbps.	interface configuration	All
(config) banner	Configures message-of-the-day, login, login and EXEC banners.	global configuration	All
(config) bypass	Configures the bypass functions on a WAE.	global configuration	application accelerator
cd	Changes the directory.	user-level EXEC and privileged-level EXEC	All
(config) cdp	Enables the Cisco Discovery Protocol (CDP) for the WAAS device.	global configuration	All
(config-if) cdp	Enables CDP on an interface.	interface configuration	All
(config) central-manager	In application accelerator mode, used to specify the IP address of the WAAS Central Manager with which the WAE needs to register. In central manager mode, used to specify the WAAS Central Manager's role and GUI port number.	global configuration	All
cifs	Controls CIFS adapter operations and run-time configurations.	user-level EXEC and privileged-level EXEC	application accelerator
clear	Resets the counters and other specified functions.	privileged-level EXEC	All
clock	Manages the system clock.	privileged-level EXEC	All
(config) clock	Sets the summer daylight saving time of day and time zone.	global configuration	All
cms	Configures the parameters for the Centralized Management System (CMS) embedded database.	privileged-level EXEC	All
(config) cms	Schedules the maintenance and enables the Centralized Management System on a specific WAAS device.	global configuration	All
cms secure-store	Configures the data encryption strength used when disk encryption is enabled.	privileged-level EXEC	All
configure*	Enters configuration mode from privileged EXEC mode.	privileged-level EXEC	All
copy cdrom	Copies files from a CD-ROM.	privileged-level EXEC	All
copy compactflash	Copies files from the Compact Flash card.	privileged-level EXEC	All
copy disk	Copies configuration information or files from a disk.	privileged-level EXEC	All
copy ftp	Copies files from an FTP server.	privileged-level EXEC	All
copy http	Copies files from an HTTP server.	privileged-level EXEC	All
copy running-config	Copies information from the current system configuration.	privileged-level EXEC	All

Table 2-1 Command Summary (continued)

Command	Description	CLI Mode	Device Mode
copy startup-config	Copies information from the startup configuration.	privileged-level EXEC	All
copy sysreport	Copies system troubleshooting information.	privileged-level EXEC	All
copy system-status	Copies the system status for debugging reference.	privileged-level EXEC	All
copy tech-support	Copies system information for technical support.	privileged-level EXEC	All
copy tftp	Copies the software image from the TFTP server.	privileged-level EXEC	All
cpfile	Copies a file to the current directory.	user-level EXEC and privileged-level EXEC	All
debug	Configures the debugging options. Note The following debug options are supported only in the application accelerator device mode: dre , epm , print-spooler , tfo , wafs , and wccp .	privileged-level EXEC	All
(config-std-nacl) delete	Deletes a line from the standard ACL	standard ACL configuration	All
(config-ext-nacl) delete	Deletes a line from the extended ACL	extended ACL configuration	All
delfile	Deletes a file.	user-level EXEC and privileged-level EXEC	All
deltree	Deletes a directory and its subdirectories.	user-level EXEC and privileged-level EXEC	All
(config-std-nacl) deny	Adds a line to a standard access-list that specifies the type of packets that you want the WAAS device to drop.	standard ACL configuration	All
(config-ext-nacl) deny	Adds a line to an extended access-list that specifies the type of packets that you want the WAAS device to drop.	extended ACL configuration	All
(config) device mode	Specifies the device mode of the WAAS device.	global configuration	All
dir	Displays the files in long list format.	user-level EXEC and privileged-level EXEC	All
disable	Turns off the privileged EXEC commands.	privileged-level EXEC	All
disk	Configures the disks on the WAAS device.	privileged-level EXEC	All
(config) disk disk-name	Disables a RAID-1 disk for online removal.	global configuration	All
(config) disk encrypt enable	Enables disk encryption.	global configuration	application accelerator
(config) disk error-handling	Configures how the disk errors should be handled.	global configuration	All

Table 2-1 Command Summary (continued)

Command	Description	CLI Mode	Device Mode
dnslookup	Resolves a DNS hostname.	user-level EXEC and privileged-level EXEC	All
(config) egress-method	Configures the egress method for intercepted connections.	global configuration	application accelerator
enable*	Accesses the privileged EXEC commands.	user-level EXEC	All
(config) end	Exits configuration and privileged EXEC modes.	global configuration	All
(config) exec-timeout	Configures the length of time that an inactive Telnet or SSH session remains open.	global configuration	All
exit	Exits from privileged EXEC mode.	privileged-level EXEC	All
(config) exit	Exits from global configuration mode.	global configuration	All
(config-if) exit	Exits from interface configuration mode.	interface configuration	All
(config-std-nacl) exit	Exits from standard ACL configuration mode.	standard ACL configuration	All
(config-ext-nacl) exit	Exits from extended ACL configuration mode.	extended ACL configuration	All
(config) external-ip	Configures up to a maximum of eight external IP addresses on a WAE.	global configuration	application accelerator
find-pattern	Searches for a particular pattern in a file.	privileged-level EXEC	All
(config) flow monitor	Configures network traffic flow monitoring.	global configuration	application accelerator
(config-if) full-duplex	Sets the current interface to the full-duplex mode.	interface configuration	All
(config-if) half-duplex	Sets the current interface to half-duplex mode.	interface configuration	All
(config-if) inline	Configures inline interception for an inlineGroup interface.	interface configuration	All
help	Provides assistance for the WAAS command-line interface in EXEC mode.	user-level EXEC and privileged-level EXEC	All
(config) help	Provides assistance for the WAAS command-line interface.	global configuration	All
(config) hostname	Configures the hostname of the WAAS device in global configuration mode.	global configuration	All
(config) inetd enable	Enables FTP, RCP, and TFTP services.	global configuration	All
install	Installs a new image into Flash memory.	privileged-level EXEC	All
(config) interface*	Configures a Gigabit Ethernet, Port Channel, or Standby interface. Provides access to interface configuration mode.	global configuration	All

Table 2-1 Command Summary (continued)

Command	Description	CLI Mode	Device Mode
(config) ip	Configures the initial network device configuration settings (for example, the IP address of the default gateway) on a WAAS device.	global configuration	All
(config-if) ip	Configures the IP address, subnet mask, or DHCP IP address negotiation on the interface of the WAAS device.	interface configuration	All
(config-if) ip access-group	Controls the connections on a specific interface by applying a predefined access list.	interface configuration	All
(config) ip access-list*	Creates and modifies the access lists for controlling access to interfaces or applications. Provides access to ACL configuration mode.	global configuration	All
(config) kerberos	Configures user authentication against a Kerberos database.	global configuration	All
(config) kernel kdb	Enables the kernel debugger configuration mode.	global configuration	All
less	Displays the contents of a file using the LESS application.	user-level EXEC and privileged-level EXEC	All
(config) line	Specifies the terminal line settings.	global configuration	All
(config-std-nacl) list	Displays a list of specified entries within the standard ACL	standard ACL configuration	All
(config-ext-nacl) list	Displays a list of specified entries within the extended ACL	extended ACL configuration	All
lls	Displays the files in a long list format.	user-level EXEC and privileged-level EXEC	All
(config) logging	Configures system logging (syslog).	global configuration	All
ls	Lists the files and subdirectories in a directory.	user-level EXEC and privileged-level EXEC	All
mkdir	Makes a directory.	user-level EXEC and privileged-level EXEC	All
mkfile	Makes a file (for testing).	user-level EXEC and privileged-level EXEC	All
(config-std-nacl) move	Moves a line to a new position within the standard ACL	standard ACL configuration	All
(config-ext-nacl) move	Moves a line to a new position within the extended ACL	extended ACL configuration	All
(config-if) mtu	Sets the interface Maximum Transmission Unit (MTU) packet size.	interface configuration	All
(config) no	Negates a global configuration command or sets its defaults.	global configuration	All

Table 2-1 Command Summary (continued)

Command	Description	CLI Mode	Device Mode
(config-if) no	Negates an interface command or restores it to its default values.	interface configuration	All
(config) ntp	Configures the NTP server.	global configuration	All
ntpdate	Sets the NTP server name.	privileged-level EXEC	All
(config-std-nacl) permit	Adds a line to a standard access-list that specifies the type of packets that you want the WAAS device to permit for further processing.	standard ACL configuration	All
(config-ext-nacl) permit	Adds a line to an extended access-list that specifies the type of packets that you want the WAAS device to permit for further processing.	extended ACL configuration	All
ping	Sends the echo packets.	user-level EXEC and privileged-level EXEC	All
(config) policy-engine application classifier	Defines a WAE's application policy and assigns the policy a name, a classifier, and a policy map.	global configuration	application accelerator
(config) policy-engine application map adaptor EPM	Configures a WAE's application policy with advanced policy map lists of the EndPoint Mapper (EPM) service.	global configuration	application accelerator
(config) policy-engine application map adaptor WAFS transport	Configures a WAE's application policies with the WAFS transport option.	global configuration	application accelerator
(config) policy-engine application map basic delete	Deletes a specific basic (static) application policy map from the WAE's list of application policy maps.	global configuration	application accelerator
(config) policy-engine application map basic disable	Disables a specific basic (static) application policy map from the WAE's list of application policy maps.	global configuration	application accelerator
(config) policy-engine application map basic insert	Inserts new basic (static) application policy map to the list of application policy maps on a WAE.	global configuration	application accelerator
(config) policy-engine application map basic list	Displays a list of basic (static) application policy maps for a WAE.	global configuration	application accelerator
(config) policy-engine application map basic move	Moves the application policy with the basic policy map list based on L3 or L4 parameters only.	global configuration	application accelerator
(config) policy-engine application map basic name	Configures the WAE's application policy with the basic policy map name.	global configuration	application accelerator
(config) policy-engine application map other optimize DRE	Configures the WAE's optimize DRE command action for non-classified traffic.	global configuration	application accelerator

Table 2-1 Command Summary (continued)

Command	Description	CLI Mode	Device Mode
(config) policy-engine application map other optimize full	Configures the application policy for non-classified traffic with the optimize full command action.	global configuration	application accelerator
(config) policy-engine application map other pass-through	Configures the application policy for non-classified traffic with the pass-through command action.	global configuration	application accelerator
(config) policy-engine application name	Creates a new application definition that specifies general information about an application.	global configuration	application accelerator
(config) policy-engine config	Removes all of the application policy configuration or restores the application policy factory defaults on a WAE.	global configuration	application accelerator
(config) port-channel	Configures the Port Channel load-balancing options.	global configuration	All
(config) primary-interface	Configures a primary interface for the WAAS device.	global configuration	All
(config) print-services	Enables and disables WAAS print services and configures an administrative group.	global configuration	All
pwd	Displays the present working directory.	user-level EXEC and privileged-level EXEC	All
(config) radius-server	Configures the RADIUS parameters on a WAAS device.	global configuration	All
reload	Halts a device and performs a cold restart.	privileged-level EXEC	All
rename	Renames a file.	user-level EXEC and privileged-level EXEC	All
restore	Restores a device to its manufactured default status.	privileged-level EXEC	All
rmdir	Removes a directory.	user-level EXEC and privileged-level EXEC	All
scp	Specifies the SCP client.	privileged-level EXEC	All
script	Checks the errors in a script or executes a script.	privileged-level EXEC	All
setup	Configures the basic configuration settings. Invokes the interactive setup utility.	privileged-level EXEC	All
show aaa accounting	Displays the AAA accounting configuration.	privileged-level EXEC	All
show adapter	Displays the status and configuration of the EndPoint Mapper (EPM) adapter.		application accelerator
show alarms	Displays information on various types of alarms, their status, and history.	privileged-level EXEC	All
show arp	Displays the ARP entries.	user-level EXEC and privileged-level EXEC	All

Table 2-1 Command Summary (continued)

Command	Description	CLI Mode	Device Mode
show authentication	Displays the authentication configuration.	user-level EXEC and privileged-level EXEC	All
show auto-register	Displays the status of auto registration feature for a WAE.	privileged-level EXEC	application accelerator
show bypass	Displays the bypass configuration of a WAE.	user-level EXEC and privileged-level EXEC	application accelerator
show cdp	Displays the CDP configuration.	user-level EXEC and privileged-level EXEC	All
show cifs	Displays CIFS run-time information.	user-level EXEC and privileged-level EXEC	application accelerator
show clock	Displays the system clock.	user-level EXEC and privileged-level EXEC	All
show cms	Displays the management service information.	user-level EXEC and privileged-level EXEC	All
show debugging	Displays the state of each debugging option.	user-level EXEC and privileged-level EXEC	All
show device-mode	Displays the device mode.	user-level EXEC and privileged-level EXEC	All
show disks	Displays the disk configurations.	user-level EXEC and privileged-level EXEC	All
show egress-methods	Displays the egress method that is configured and that is being used on a particular WAE.	user-level EXEC and privileged-level EXEC	application accelerator
show flash	Displays the flash memory information.	user-level EXEC and privileged-level EXEC	All
show hardware	Displays the system hardware information.	user-level EXEC and privileged-level EXEC	All
show hosts	Displays the IP domain name, name servers, IP addresses, and host table.	user-level EXEC and privileged-level EXEC	All
show inetd	Displays the status of TCP/IP services.	user-level EXEC and privileged-level EXEC	All
show interface	Displays the hardware interface information.	user-level EXEC and privileged-level EXEC	All
show inventory	Displays the system inventory information.	user-level EXEC and privileged-level EXEC	All
show ip access-list	Displays the information about access lists that are defined and applied to specific interfaces or applications.	user-level EXEC and privileged-level EXEC	All
show ip routes	Displays the IP routing table.	user-level EXEC and privileged-level EXEC	All
show kerberos	Displays the Kerberos authentication configuration.	user-level EXEC and privileged-level EXEC	All

Table 2-1 Command Summary (continued)

Command	Description	CLI Mode	Device Mode
show key-manager	Displays the key manager information for each WAAS device.	user-level EXEC and privileged-level EXEC	central manager
show logging	Displays the system logging configuration.	user-level EXEC and privileged-level EXEC	All
show memory	Displays the memory blocks and statistics.	user-level EXEC and privileged-level EXEC	All
show ntp	Displays the NTP configuration status.	user-level EXEC and privileged-level EXEC	All
show policy-engine application	Displays the display application policy information.	user-level EXEC and privileged-level EXEC	application accelerator
show policy-engine status	Displays the policy-engine high-level information. This information includes the usage of the available resources, which include application names, classifiers, and conditions.	user-level EXEC and privileged-level EXEC	application accelerator
show print-services	Displays the print services administrator and process information.	user-level EXEC and privileged-level EXEC	All
show processes	Displays the process status.	user-level EXEC and privileged-level EXEC	All
show radius-server	Displays the RADIUS server information.	user-level EXEC and privileged-level EXEC	All
show running-config	Displays the current operating configuration.	user-level EXEC and privileged-level EXEC	All
show services	Displays information related to services.	user-level EXEC and privileged-level EXEC	All
show smb-conf	Displays the smb-conf configurations.	user-level EXEC and privileged-level EXEC	All
show snmp	Displays the SNMP statistics.	user-level EXEC and privileged-level EXEC	All
show ssh	Displays the status and configuration of the Secure Shell (SSH) service.	user-level EXEC and privileged-level EXEC	All
show standby	Displays the information related to the standby interface.	user-level EXEC and privileged-level EXEC	All
show startup-config	Displays the startup configuration.	user-level EXEC and privileged-level EXEC	All
show statistics authentication	Displays the authentication statistics.	user-level EXEC and privileged-level EXEC	All
show statistics cifs	Displays the CIFS statistics information.	user-level EXEC and privileged-level EXEC	application accelerator
show statistics content-distribution-network	Displays the status of a WAE or group of WAEs that are registered with the WAAS Central Manager.	user-level EXEC and privileged-level EXEC	central manager

Table 2-1 Command Summary (continued)

Command	Description	CLI Mode	Device Mode
<code>show statistics dre</code>	Displays the Data Redundancy Elimination (DRE) statistics for a WAE.	user-level EXEC and privileged-level EXEC	application accelerator
<code>show statistics dre connection</code>	Displays the DRE connection statistics for a WAE.	user-level EXEC and privileged-level EXEC	application accelerator
<code>show statistics dre peer</code>	Displays the DRE peer statistics for a WAE.	user-level EXEC and privileged-level EXEC	application accelerator
<code>show statistics epm</code>	Displays the DCE-RPC EPM statistics.	user-level EXEC and privileged-level EXEC	application accelerator
<code>show statistics icmp</code>	Displays the ICMP statistics.	user-level EXEC and privileged-level EXEC	All
<code>show statistics ip</code>	Displays the IP statistics.	user-level EXEC and privileged-level EXEC	All
<code>show statistics key-manager</code>	Displays the key manager information for each WAAS device.	user-level EXEC and privileged-level EXEC	central manager
<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 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 tfo</code>	Displays the Transport Flow Optimization (TFO) statistics for a WAE.	user-level EXEC and privileged-level EXEC	application accelerator
<code>show statistics udp</code>	Displays the User Datagram Protocol (UDP) statistics.	user-level EXEC and privileged-level EXEC	All
<code>show statistics wccp</code>	Displays the WCCP statistics for a WAE.	user-level EXEC and privileged-level EXEC	application accelerator
<code>show statistics windows-domain</code>	Displays the Windows domain configuration.	user-level EXEC and privileged-level EXEC	All
<code>show sysfs volumes</code>	Displays the system file system (SYSFS) information.	user-level EXEC and privileged-level EXEC	All
<code>show tacacs</code>	Displays the TACACS+ configuration.	user-level EXEC and privileged-level EXEC	All
<code>show tcp</code>	Displays the TCP configuration.	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

Table 2-1 Command Summary (continued)

Command	Description	CLI Mode	Device Mode
show telnet	Displays the Telnet services configuration.	user-level EXEC and privileged-level EXEC	All
show tfo accelerators	Displays the Transport Flow Optimization (TFO) information including the accelerators, auto-discovery, buffer manager information, connection and status for a WAE.	user-level EXEC and privileged-level EXEC	application accelerator
show tfo auto-discovery	Displays TFO auto-discovery statistics for a WAE.	user-level EXEC and privileged-level EXEC	application accelerator
show tfo bufpool	Displays TFO buffer pool information for a WAE.	user-level EXEC and privileged-level EXEC	application accelerator
show tfo connection	Displays TFO connection information for a WAE.	user-level EXEC and privileged-level EXEC	application accelerator
show tfo egress-methods connection	Displays detailed information about the egress methods for a WAE.	user-level EXEC and privileged-level EXEC	application accelerator
show tfo filtering	Displays TFO flow information for a WAE.	user-level EXEC and privileged-level EXEC	application accelerator
show tfo status	Displays TFO status information for a WAE.	user-level EXEC and privileged-level EXEC	application accelerator
show tfo synq	Displays TFO statistics for the SynQ module.	user-level EXEC and privileged-level EXEC	application accelerator
show transaction-logging	Displays the transaction logging information for a WAE.	user-level EXEC and privileged-level EXEC	application accelerator
show user	Displays information about a particular user.	user-level EXEC and privileged-level EXEC	All
show users administrative	Displays the administrative users.	user-level EXEC and privileged-level EXEC	All
show version	Displays the software version.	user-level EXEC and privileged-level EXEC	All
show wccp	Displays the WCCP information for a WAE.	user-level EXEC and privileged-level EXEC	application accelerator
show windows-domain	Displays the Windows domain configuration.	user-level EXEC and privileged-level EXEC	All
(config-if) shutdown	Shuts down the specified interface.	interface configuration	All
shutdown	Shuts down the device (stops all applications and operating system).	privileged-level EXEC	All
(config) smb-conf	Manually configures parameters in the Samba configuration file, <i>smb-conf</i> .	global configuration	All
(config) snmp-server access-list	Configures an access control list to allow access through an SNMP agent.	global configuration	All
(config) snmp-server community	Enables SNMP; sets the community string, optionally names the group, and enables the read-write access with the community string.	global configuration	All

Table 2-1 Command Summary (continued)

Command	Description	CLI Mode	Device Mode
(config) snmp-server contact	Specifies the text for the system contact MIB object.	global configuration	All
(config) snmp-server enable traps	Enables the SNMP traps.	global configuration	All
(config) snmp-server group	Defines a user security model group.	global configuration	All
(config) snmp-server host	Specifies the hosts to receive SNMP traps.	global configuration	All
(config) snmp-server location	Specifies the path for MIB object sysLocation.	global configuration	All
(config) snmp-server mib persist event	Configures the persistence for the SNMP Event MIB.	global configuration	All
(config) snmp-server notify inform	Configures the SNMP inform request.	global configuration	All
(config) snmp-server user	Defines a user who can access the SNMP engine.	global configuration	All
(config) snmp-server view	Defines an SNMPv2 MIB view.	global configuration	All
snmp trigger	Creates or deletes SNMP triggers on a MIB variable.	privileged-level EXEC	All
ssh	Allows secure encrypted communications between an untrusted client machine and a WAAS device over an insecure network.	user-level EXEC and privileged-level EXEC	All
(config) sshd	Configures the parameters for the Secure Shell (SSH) service.	global configuration	All
(config) ssh-key-generate	Generates a SSH host key.	global configuration	All
(config-if) standby	Configures an interface to be a backup for another interface.	interface configuration	All
(config) tacacs	Configures the TACACS+ parameters on a WAAS device.	global configuration	All
(config) tcp	Configures the TCP parameters.	global configuration	All
tcpdump	Dumps the TCP traffic on the network.	privileged-level EXEC	All
telnet	Starts the Telnet client.	user-level EXEC and privileged-level EXEC	All
(config) telnet enable	Enables the Telnet services.	global configuration	All
terminal	Sets the terminal output commands.	user-level EXEC and privileged-level EXEC	All
tethereal	Analyzes network traffic from the command line.	privileged-level EXEC	All
(config) tfo auto-discovery	Discovers origin servers that cannot receive TCP packets with options and adds the IP addresses to a blacklist for a specified number of minutes.	global configuration	application accelerator

Table 2-1 Command Summary (continued)

Command	Description	CLI Mode	Device Mode
(config) tfo optimize	Configures TFO optimization for DRE or full generic optimization on the WAE.	global configuration	application accelerator
(config) tfo tcp keepalive	Configures TFO optimization with TCP keepalive on a WAE.	global configuration	application accelerator
(config) tfo tcp optimized-mss	Configures TFO optimization with optimized-side TCP maximum segment size on a WAE.	global configuration	application accelerator
(config) tfo tcp optimized-receive-buffer	Configures TFO optimization with an optimized-side receive buffer on a WAE.	global configuration	application accelerator
(config) tfo tcp optimized-send-buffer	Configures TFO optimization with an optimized-side send buffer on a WAE.	global configuration	application accelerator
(config) tfo tcp original-mss	Configures TFO optimization with an unoptimized-side TCP maximum segment size on the WAE.	global configuration	application accelerator
(config) tfo tcp original-receive-buffer	Configures TFO optimization with unoptimized-side receive buffer on a WAE.	global configuration	application accelerator
(config) tfo tcp original-send-buffer	Configures TFO optimization with unoptimized-side send buffer on a WAE.	global configuration	application accelerator
traceroute	Traces the route to a remote host.	user-level EXEC and privileged-level EXEC	All
transaction-log	Forces the transaction logging for TFO and export on a WAE.	privileged-level EXEC	application accelerator
(config) transaction-logs	Configures the transaction logging on a WAE.	global configuration	application accelerator
type	Displays a file.	user-level EXEC and privileged-level EXEC	All
type-tail	Displays the last several lines of a file.	user-level EXEC and privileged-level EXEC	All
undebug	Disables the debugging functions. (See debug .)	privileged-level EXEC	All
(config) username	Establishes the username authentication.	global configuration	All
wafs	Performs backup or restores system configuration, and creates a system report on a WAE.	privileged-level EXEC	application accelerator
(config) wccp access-list	Configures the IP access list for inbound Web Cache Coordination Protocol (WCCP) GRE-encapsulated traffic on a WAE.	global configuration	application accelerator
(config) wccp flow-redirect enable	Enables the WCCP flow redirection on a WAE.	global configuration	application accelerator
(config) wccp router-list	Creates a router list on a WAE for use in the WCCP Version 2 services.	global configuration	application accelerator

Table 2-1 Command Summary (continued)

Command	Description	CLI Mode	Device Mode
<code>(config) wccp shutdown</code>	Sets the maximum time interval after which the WAE will perform a clean shutdown.	global configuration	application accelerator
<code>(config) wccp tcp-promiscuous</code>	Configures the TCP promiscuous mode service (WCCP Version 2 services 61 and 62) on a WAE.	global configuration	application accelerator
<code>(config) wccp version</code>	Specifies the WCCP version number.	global configuration	application accelerator
<code>whoami</code>	Displays the name of the current user.	user-level EXEC and privileged-level EXEC	All
<code>windows-domain</code>	Accesses Windows domain utilities.	privileged-level EXEC	All
<code>(config) windows-domain</code>	Configures Windows domain server options.	global configuration	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



CHAPTER 3

CLI Commands

This chapter provides detailed information for the following types of CLI commands for the WAAS software:

- EXEC mode commands you can enter after you log in to the WAAS device. See the [“EXEC Mode Commands”](#) section for a complete listing of commands.
- Global configuration mode commands that you can enter after you log in to the WAAS device and access global configuration mode. See the [“Configuration Mode Commands”](#) section for a complete listing of commands.
- Interface configuration mode commands that you can enter after you access global configuration mode (see the [“Interface Configuration Mode Commands”](#) section for a complete listing of commands.
- Standard or extended ACL configuration mode commands that you can enter after you access global configuration mode (see the [“Standard ACL Configuration Mode Commands”](#) and [“Extended ACL Configuration Mode Commands”](#) sections for a complete listing of commands.

The description of each command includes the following:

- The syntax of the command, default values, command modes, usage guidelines, and examples.
- Any related commands, when appropriate

See [Chapter 1, “Using the WAAS Command-Line Interface”](#) for a discussion about using the CLI and about the CLI command modes.

EXEC Mode Commands

Use the EXEC mode for setting, viewing, and testing system operations. In general, the user EXEC commands allow you to connect to remote devices, change terminal line settings on a temporary basis, perform basic tests, and list system information.

The EXEC mode is divided into two access levels: user and privileged.

The user EXEC mode is used by local and general system administrators, while the privileged EXEC mode is used by the root administrator. 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 hostname 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.

**Note**

You can change the hostname using the **hostname** global configuration command.

In the following example, a user accesses the privileged-level EXEC command line from the user level:

```
WAE> enable
WAE#
```

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

```
WAE# exit
WAE>
```

cd

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

cd *directoryname*

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

Defaults	No default behavior or values
-----------------	-------------------------------

Command Modes	EXEC
----------------------	------

Device Modes	application-accelerator replication-accelerator central-manager
---------------------	-----------------------------------------------------------------------

Usage Guidelines	Use this command to navigate between directories and for file management. The directory name becomes the default prefix for all relative paths. Relative paths do not begin with a slash (/). Absolute paths begin with a slash (/).
-------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Examples	The following example shows how to change to a directory using a relative path:
-----------------	---------------------------------------------------------------------------------

```
WAE(config)# cd local1
```

The following example shows how to change to a directory using an absolute path:

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

Related Commands	deltree dir lls ls mkdir pwd
-------------------------	---------------------------------------------------------------------------------------------------------------------------------------------

cifs

To control CIFS adapter operations and run-time configurations, use the **cifs** EXEC command.

```
cifs { auto-discovery { disable | enable | reset-log } | mss value | restart [core | edge] | reverse-dns
{ active | disable | enable } | session disconnect [client-ip ipaddress | server-ip ipaddress] }
```

Syntax Description

auto-discovery	Controls CIFS auto-discovery configuration and debug.
disable	Disables CIFS server auto-discovery.
enable	Enables CIFS server auto-discovery.
reset-log	Resets the log memory.
mss	Sets the TCP maximum segment size (MSS) for the CIFS adapter.
<i>value</i>	Maximum segment size. This value must be an integer in the range of 512–1460.
restart	Restarts the CIFS application.
core	Restarts the CIFS application on the Core WAE.
edge	Restarts the CIFS application on the Edge WAE.
reverse-dns	Uses reverse DNS to resolve server names on the Core WAE.
active	Checks whether reverse DNS is active.
disable	Deactivates reverse DNS on the Core WAE.
enable	Activates reverse DNS on the Core WAE.
session	Configures operations on active CIFS sessions.
disconnect	Disconnects the CIFS sessions.
client-ip	Sets the client IP address or address set.
<i>ipaddress</i>	IP address.
server-ip	Sets the server IP address or address set.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

Use the **cifs restart** command to restart the WAFS services for a configuration change without having to reboot the WAE.

Related Commands

[show cifs](#)

[show statistics cifs](#)

clear

To clear the hardware interface, statistics, and other settings, use the **clear** EXEC command.

```
clear arp-cache [ipaddress | interface { GigabitEthernet 1-2/port | PortChannel 1-2 | Standby 1-4}]
```

```
clear cache dre
```

```
clear cdp { counters | table }
```

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

```
clear logging
```

```
clear statistics { all | authentication | epm | flow monitor tepstat-v1 | history | iemp | inline | ip | radius | running | tacacs | tcp | udp | windows-domain }
```

```
clear statistics dre [connection | global | nack | peer]
```

```
clear statistics tfo { all | auto-discovery | blacklist | filtering | peer | policy-engine | synq }
```

```
clear windows-domain-log
```

Syntax Description

arp-cache	Clears the ARP cache.
<i>ipaddress</i>	Clears all ARP entries for the IP address.
interface	Clears all ARP entries on the interface.
GigabitEthernet	GigabitEthernet interface.
<i>1-2/port</i>	GigabitEthernet slot/port.
PortChannel	PortChannel interface.
<i>1-2</i>	PortChannel number. Values are 1 or 2.
Standby	Standby interface.
<i>1-4</i>	Stand by interface number 1, 2, 3, or 4.
cache	Clears cached objects.
dre	Clears the DRE cache.
cdp	Resets the Cisco Discovery Protocol (CDP) statistical data.
counters	Clears the CDP counters.
table	Clears the CDP tables.
ip access-list	Clears the IP access list statistical information.
counters	Clears the IP access list counters.
<i>acl-num</i>	(Optional) Clears the counters for the specified access list, identified using a numeric identifier (standard access list: 1–99; extended access list: 100–199).
<i>acl-name</i>	(Optional) Clears the counters for the specified access list, identified using an alphanumeric identifier of up to 30 characters, beginning with a letter.
logging	Clears the syslog messages saved in the disk file.

statistics	Clears the statistics as specified.
all	Clears all statistics.
authentication	Clears the authentication statistics.
dre	Clears the Data Redundancy Elimination (DRE) statistics.
connection	(Optional) Clears all DRE connection statistics.
global	(Optional) Clears the global DRE statistics.
nack	(Optional) Clears all DRE NACK statistics.
peer	(Optional) Clears all DRE peer statistics.
epm	Clears the DCE-RPC EPM statistics.
flow	Clears the network traffic flow statistics.
monitor	Clears the monitor flow performance statistics.
tcpstat-v1	Clears the tcpstat-v1 collector statistics.
history	Clears the statistics history.
icmp	Clears the ICMP statistics.
inline	Clears the inline interception statistics.
ip	Clears the IP statistics.
radius	Clears the RADIUS statistics.
running	Clears the running statistics.
tacaacs	Clears the TACACS+ statistics.
tcp	Clears the TCP statistics.
udp	Clears the UDP statistics.
windows-domain	Clears the Windows domain statistics.
tfo	Clears the TCP flow optimization (TFO) statistics.
all	Clears all of the TFO statistics.
auto-discovery	Clears the TFO auto-discovery statistics.
blacklist	Clears the TFO blacklist statistics.
filtering	Clears the TFO filter table statistics.
peer	Clears the TFO peer statistics.
policy-engine	Clears the TFO application and pass-through statistics.
synq	Clears the TFO SynQ module statistics.
windows-domain-log	Clears the Samba, Kerberos, and Winbind log files.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

replication-accelerator

central-manager

Usage Guidelines

After you use the **clear cache dre** command, the first 1 MB of data is not optimized. Cisco WAAS does not optimize the first 1 MB of data after a restart of the tcproxy service. Data transmitted after the first 1 MB of data will be optimized according to the configured policy.

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 WAE# exec_clear_logging:Syslog cleared
```

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

The **clear windows-domain-log** command removes all current entries from the Windows domain log file.

Examples

The following example clears all entries in the *syslog.txt* file on the WAAS device:

```
WAE# clear logging
```

The following example clears all authentication, RADIUS and TACACS+ information on the WAAS device:

```
WAE# clear statistics radius
WAE# clear statistics tacacs
WAE# clear statistics authentication
```

The following example clears all entries in the Windows domain log file on the WAAS device:

```
WAE# clear windows-domain-log
```

Related Commands

[show interface](#)

[show wccp](#)

clear users

To clear user connections or to unlock users that have been locked out, use the **clear users EXEC** command.

clear users [**administrative** | **locked-out** {**all** | **username** *username*}]

Syntax Description

users	Clears the connections (logins) of authenticated users.
administrative	Clears the connections (logins) of administrative users authenticated through a remote login service.
locked-out all	Unlocks all locked-out user accounts.
locked-out username	Unlocks the specified locked-out user account.
<i>username</i>	The account username to be unlocked.

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator
 replication-accelerator
 central-manager

Usage Guidelines

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

The **clear users locked-out** command unlocks user accounts that have been locked out. If strong password policy is enable (see [\(config\) authentication strict-password-policy](#)) a user account will be locked out if the user fails three consecutive login attempts. (This does not apply to the “admin” account.)

Examples

The following example clears the connections of all authenticated users:

```
WAE(config)# clear users
```

The following example clears the connections of all administrative users authenticated through a remote login service (it does not affect administrative users authenticated through the local database):

```
WAE(config)# clear users administrative
```

The following example unlocks all locked-out user accounts:

```
WAE(config)# clear users locked-out all
```

The following example unlocks the account for username darcy:

```
WAE(config)# clear users locked-out username darcy
```

Related Commands

[clear](#)

[\(config\) authentication strict-password-policy](#)

clock

To set clock functions or update the calendar, use the **clock** EXEC command. To clear clock functions and calendar, use the **no** form of this command.

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

Syntax Description

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

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator
 replication-accelerator
 central-manager

Usage Guidelines

If you have an outside source on your network that provides time services (such as a NTP server), you do not need to set the system clock manually. When setting the clock, enter the local time. The WAAS device calculates the UTC based on the time zone set by the **clock timezone** global configuration command.

Two clocks exist in the system: the software clock and the hardware clock. The software uses the software clock. The hardware clock is used only at startup to initialize the software clock.

The **set** keyword sets the software clock.

Examples

The following example sets the software clock on the WAAS device:

```
WAE# clock set 13:32:00 01 February 2005
```

Related Commands

[show clock](#)

cms

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

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

Syntax Description		
config-sync		Sets the node to synchronize configuration with the WAAS Central Manager.
database		Creates, backs up, deletes, restores, or validates the CMS-embedded database management tables or files.
backup		Backs up the database management tables.
create		Creates the embedded database management tables.
delete		Deletes the embedded database files.
downgrade		Downgrades the CMS database.
script		(Optional) Downgrades the CMS database by applying a downgrade script.
<i>filename</i>		Downgraded script filename.
lcm		Configures local/central management on a WAAS device that is registered with the WAAS Central Manager.
enable		Enables synchronization of the WAAS network configuration of the device with the local CLI configuration.
disable		Disables synchronization of the WAAS network configuration of the device with the local CLI configuration.
maintenance		Cleans and reindexes the embedded database tables.
full		Specifies a full maintenance routine for the embedded database tables.
regular		Specifies a regular maintenance routine for the embedded database tables.
restore		Restores the database management tables using the backup local filename.
<i>filename</i>		Database local backup filename.
validate		Validates the database files.
deregister		Removes the registration of the CMS proto device.
force		(Optional) Forces the removal of the node registration.
recover		Recovers the identity of a WAAS device.
identity		Specifies the identity of the recovered device.
<i>word</i>		Identity of the recovered device.

Defaults No default behavior or values

Command Modes EXEC

Device Modes

application-accelerator
replication-accelerator
central-manager

Usage Guidelines

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

Use the **cms config-sync** command to enable registered WAAS devices and standby WAAS Central Manager to contact the primary WAAS Central Manager 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 WAAS Central Manager and activated, it appears as Pending in the WAAS Central Manager 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 WAAS network, it must first be registered and then activated. The **cms enable** global configuration command automatically registers the node in the database management tables and enables the CMS. The node sends its attribute information to the WAAS Central Manager over the SSL protocol and then stores the new node information. The WAAS Central Manager 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 WAAS Central Manager GUI.

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

To back up the existing management database for the WAAS Central Manager, 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.

**Note**

For information on the procedure to back up and restore the CMS database on the WAAS Central Manager, see the *Cisco Wide Area Application Services Configuration Guide*.

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 having the same registration information, you must specify the device recovery key that you configured in the Modifying Config Property, System.device.recovery.key window of the WAAS Central Manager GUI.

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

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

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

If LCM is disabled, the settings configured through the WAAS Central Manager GUI will overwrite the settings configured from the WAEs; however, this rule applies only to those local device settings that have been overwritten by the WAAS Central Manager 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 WAAS Central Manager, the local device configuration will be applicable until the WAAS Central Manager requests a full device statistics update from the WAEs (clicking the **Force full database update** button from the Device Home window of the WAAS Central Manager GUI triggers a full update). When the WAAS Central Manager requests a full update from the device, the WAAS Central Manager settings will overwrite the local device settings.

Examples

The following example backs up the cms database management tables on the WAAS Central Manager named waas-cm:

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

The following example validates the cms database management tables on the WAAS Central Manager named waas-cm:

```
waas-cm# cms database validate
Management tables are valid
```

Related Commands

[\(config\) cms](#)

[show cms](#)

cms secure-store

To configure secure store encryption, use the **cms secure-store** commands.

cms secure-store {init | open | change | clear}

Syntax Description		
	init	Initializes secure store encryption on the WAAS device. Secure store encryption is not active until you subsequently execute the cms secure-store open command. On the Central Manager, this command prompts you to enter the secure store encryption pass phrase.
	open	Activates secure store encryption (the WAAS encrypts the stored data using secure store encryption). Secure store encryption must already be initialized using the cms secure-store init command. On the Central Manager, this command prompts you to enter the secure store encryption pass phrase.
	change	Changes the secure store encryption pass phrase and encryption key. On the Central Manager this command prompts you to enter and confirm the new pass phrase. The WAAS device uses the pass phrase to generate the encryption key for secure disk encryption.
	clear	Disables secure store encryption.

Defaults The standard encryption and key management is the default.

Command Modes EXEC

Device Modes
application-accelerator
replication-accelerator
central-manager

Usage Guidelines Secure storage encryption provides stronger encryption and key management for your WAAS system. The WAAS Central Manager and WAE devices use secure storage encryption for handling passwords, managing encryption keys, and for data encryption.

When you use the **cms secure-store EXEC** command to enable secure store on the Central Manager, or a WAE device, the WAAS system uses strong encryption algorithms and key management policies to protect certain data on the system. This data includes encryption keys used by applications in the WAAS system, CIFS passwords, and user login passwords.

When secure store is enabled on Central Manager, the data is encrypted using an key encryption key generated from the pass phrase you enter with SHA-1 hashing and an AES 256-bit algorithm. When secure store is enabled on a WAE device, the data is encrypted using a 256-bit key encryption key

generated by SecureRandom, a cryptographically strong pseudorandom number. You must enter a password to enable secure store. You must enter this password through the console terminal every time the Central Manager is rebooted.

When you enable secure store on a WAE, The WAE initializes and retrieves a new encryption key from the Central Manager. The WAE uses this key to encrypt WAFS password credentials stored on the WAE, and to encrypt the disk if disk encryption is also enabled. When you reboot the WAE after enabling secure store, the WAE retrieves the key from the Central Manager automatically, allowing normal access to the data that is stored in WAAS persistent storage.

Examples

The following example shows how to initialize and activate secure store encryption on the WAAS Central Manager:

```
waas-cm# cms secure-store init
enter pass-phrase(case-sensitive, no less than 8 characters)*****
re-enter pass-phrase*****
successfully initialized secure-store.
```

```
waas-cm#cms secure-store open
stopping cms..stopped
stopping keymgr..stopped.
enter pass-phrase: <pass phrase>
successfully updated cifs password in database.
successfully opened secure-store.
starting cms..started.
starting keymgr..started.
waas-cm#
```

The following example shows how to deactivates secure store encryption:

```
waas-cm#cms secure-store clear
stopping cms..stopped
stopping keymgr..stopped.
successfully updated cifs password in database.
secure-store clear
starting cms..started.
starting keymgr..started.
waas-cm#
```

Related Commands

[show cms secure-store](#)

configure

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

configure

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

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines Use this command to enter global configuration mode.

Examples The following example shows how to enable global configuration mode on a WAAS device:

```
WAE# configure  
WAE(config)#
```

Related Commands [\(config\) end](#)
[\(config\) exit](#)
[show running-config](#)
[show startup-config](#)

copy cdrom

To copy software release files from a CD-ROM, use the **copy cdrom** EXEC command.

copy cdrom install *filedir filename*

Syntax Description	cdrom	Copies a file from the CD-ROM.
	install	Installs the software release file.
	<i>filedir</i>	Directory location of the software release file.
	<i>filename</i>	Filename of the software release file.

Defaults No default behaviors or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Related Commands [install](#)
[reload](#)
[show running-config](#)
[show startup-config](#)
[wafs](#)
[write](#)

copy compactflash

To copy software release files from a CompactFlash card, use the **copy compactflash** EXEC command.

```
copy compactflash install filename
```

Syntax Description	compactflash	Copies a file from the CompactFlash card.
	install	Installs a software release file.
	filename	Image filename.

Defaults No default behaviors or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Related Commands [install](#)
[reload](#)
[show running-config](#)
[show startup-config](#)
[wafs](#)
[write](#)

copy disk

To copy the configuration or image data from a disk to a remote location using FTP or to the startup configuration, use the **copy disk** EXEC command.

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

Syntax Description		
disk		Copies a local disk file.
ftp		Copies to a file on an FTP server.
<i>hostname</i>		Hostname of the FTP server.
<i>ip-address</i>		IP address of the FTP server.
<i>remotefiledir</i>		Directory on the FTP server to which the local file is copied.
<i>remotefilename</i>		Name of the local file once it has been copied to the FTP server.
<i>localfilename</i>		Name of the local file to be copied.
startup-config		Copies the configuration file from the disk to startup configuration (NVRAM).
<i>filename</i>		Name of the existing configuration file.

Defaults No default behaviors or values

Command Modes EXEC

Device Modes application-accelerator
 replication-accelerator
 central-manager

Usage Guidelines Use the **copy disk ftp** EXEC command to copy files from a SYSFS partition to an FTP server. Use the **copy disk startup-config** EXEC command to copy a startup configuration file to NVRAM.

Related Commands [install](#)
[reload](#)
[show running-config](#)
[show startup-config](#)
[wafs](#)
[write](#)

copy ftp

To copy software configuration or image data from an FTP server, use the **copy ftp** EXEC command.

```
copy ftp { central { hostname | ip-address } remotefiledir remotefilename slotnumber [username username password] | proxy { hostname | ip-address } proxy_portnum [username username password] | port port-num | md5 md5sum] | disk { hostname | ip-address } remotefiledir remotefilename localfilename | install { hostname | ip-address } remotefiledir remotefilename }
```

Syntax Description

ftp	Copies a file from an FTP server.
central	Copies a file to the software upgrade image repository.
<i>hostname</i>	Hostname of the FTP server.
<i>ip-address</i>	IP address of the FTP server.
<i>remotefile</i> <i>dir</i>	Directory on the FTP server where the image file to be copied is located.
<i>remotefile</i> <i>name</i>	Name of the file to be copied to the image repository.
<i>slotnumber</i>	Slot location (1–5) into which the upgrade image is to be copied.
username	(Optional) Specifies FTP authentication.
<i>username</i>	(Optional) Clear text of the username.
<i>password</i>	(Optional) Password for FTP authentication.
proxy	(Optional) Specifies proxy address.
<i>hostname</i>	(Optional) Hostname of the proxy server.
<i>ip-address</i>	(Optional) IP address of the proxy server.
<i>proxy_portnum</i>	(Optional) Port number on the proxy server.
username	(Optional) Specifies the proxy server authentication username.
<i>username</i>	(Optional) Clear text of the username.
<i>password</i>	(Optional) Password for proxy server authentication.
port	(Optional) Specifies port at which to connect to the FTP server.
<i>port-num</i>	(Optional) Port number on the FTP server.
md5	(Optional) Specifies MD5 signature of the file being copied.
<i>md5sum</i>	(Optional) MD5 signature.
disk	Copies a file to a local disk.
<i>hostname</i>	Hostname of the FTP server.
<i>ip-address</i>	IP address of the FTP server.
<i>remotefile</i> <i>dir</i>	Directory on the FTP server where the file to be copied is located.
<i>remotefile</i> <i>name</i>	(Optional) Name of the file to be copied to the local disk.
<i>localfilename</i>	(Optional) Name of the copied file as it appears on the local disk.
install	(Optional) Copies the file from an FTP server and installs the software release file to the local device.
<i>hostname</i>	(Optional) Name of the FTP server.
<i>ip-address</i>	(Optional) IP address of the FTP server.
<i>remotefile</i> <i>dir</i>	Remote file directory.
<i>remotefile</i> <i>name</i>	Remote filename.

Defaults No default behaviors or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines Use the **copy ftp disk EXEC** command to copy a file from an FTP server to a SYSFS partition on the WAAS device.

Use the **copy ftp install EXEC** command to install an image file from an FTP server on a WAAS device. Part of the image goes to disk and part goes to flash memory. Use the **copy ftp central EXEC** command to download a software image into the repository from an FTP server.

You can also use the **copy ftp install EXEC** commands to redirect your transfer to a different location. A username and a password have to be authenticated with a primary domain controller (PDC) before the transfer of the software release file to the WAAS device is allowed.

Upgrading the BIOS

You can remotely upgrade the BIOS on the WAE-511, WAE-512, WAE-611, WAE-612, and the WAE-7326. All computer hardware has to work with software through an interface. The Basic Input Output System (BIOS) provides such an interface. It gives the computer a built-in starter kit to run the rest of the software from the hard disk drive. The BIOS is responsible for booting the computer by providing a basic set of instructions. It performs all the tasks that need to be done at start-up time, such as Power-On Self Test (POST) operations and booting the operating system from the hard disk drive. Furthermore, it provides an interface between the hardware and the operating system in the form of a library of interrupt handlers. For instance, each time a key is pressed, the CPU performs an interrupt to read that key, which is similar for other input/output devices, such as serial and parallel ports, video cards, sound cards, hard disk controllers, and so forth. Some older PCs cannot interoperate with all the modern hardware because their BIOS does not support that hardware; the operating system cannot call a BIOS routine to use it. This problem can be solved by replacing the BIOS with a newer one that does support your new hardware or by installing a device driver for the hardware.

All BIOS files needed for a particular hardware model BIOS update are available on Cisco.com as a single *.bin* package file. This file is a special *<WAAS-installable>.bin* file that you can install by using the normal software update procedure.

To update the BIOS version on a WAAS device that supports BIOS version updates, you need the following items:

- FTP server with the software files
- Network connectivity between the device to be updated and the server hosting the update files
- Appropriate *.bin* BIOS update file:
 - 511_bios.bin
 - 611_bios.bin
 - 7326_bios.bin

**Caution**

Be *extraordinarily* careful when upgrading a Flash BIOS. Make *absolutely* sure that the BIOS upgrade patch is the exact one required. If you apply the wrong patch, you can render the system unbootable, making it difficult or impossible to recover even by reapplying the proper patch.

**Caution**

Because a failed Flash BIOS update can have dire results, never update a Flash BIOS without first connecting the system to an uninterruptible power supply (UPS).

To remotely install a BIOS update file, use the **copy ftp install EXEC** command as follows:

```
WAE# copy ftp install ftp-server remote_file_dir 7326_bios.bin
```

After the BIOS update file is copied to your system, use the **reload EXEC** command to reboot as follows:

```
WAE# reload
```

The new BIOS takes effect after the system reboots.

Examples

The following example shows how to copy an image file from an FTP server and install the file on the local device:

```
WAE# copy ftp install 10.1.1.1 //ftp-sj.cisco.com/cisco/waas/4.0 WAAS-4.0.0-k9.bin
Enter username for remote ftp server:biff
Enter password for remote ftp server:*****
Initiating FTP download...
printing one # per 1MB downloaded
Sending:USER biff
10.1.1.1 FTP server (Version) Mon Feb 28 10:30:36 EST
2000) ready.
Password required for biff.
Sending:PASS *****
User biff logged in.
Sending:TYPE I
Type set to I.
Sending:PASV
Entering Passive Mode (128,107,193,244,55,156)
Sending:CWD //ftp-sj.cisco.com/cisco/waas/4.0
CWD command successful.
Sending PASV
Entering Passive Mode (128,107,193,244,55,156)
Sending:RETR WAAS-4.0.0-k9.bin
Opening BINARY mode data connection for ruby.bin (87376881 bytes).
#####
writing flash component:
.....
The new software will run after you reload.
```

The following example shows how to upgrade the BIOS. All output is written to a separate file (*/local1/bios_upgrade.txt*) for traceability. The hardware dependant files that are downloaded from Cisco.com for the BIOS upgrade are automatically deleted from the WAAS device after the BIOS upgrade procedure has been completed.

```
WAE-7326# copy ftp install upgradesever /bios/update53/derived/ 7326_bios.bin
Enter username for remote ftp server:myusername
Enter password for remote ftp server:*****
Initiating FTP download...
printing one # per 1MB downloaded
```

```
Sending:USER myusername
upgradeserver.cisco.com FTP server (Version wu-2.6.1-18) ready.
Password required for myusername.
Sending:PASS *****
Please read the file README_dotfiles
  it was last modified on Wed Feb 19 16:10:26 2005- 94 days ago
Please read the file README_first
  it was last modified on Wed Feb 19 16:05:29 2005- 94 days ago
User myusername logged in.
Sending:TYPE I
Type set to I.
Sending:PASV
Entering Passive Mode (128,107,193,240,57,37)
Sending:CWD /bios/update53/derived/
CWD command successful.
Sending PASV
Entering Passive Mode (128,107,193,240,146,117)
Sending:RETR 7326_bios.bin
Opening BINARY mode data connection for 7326_bios.bin (834689 bytes).
Fri Jan 7 15:29:07 UTC 2005
BIOS installer running!
Do not turnoff the system till BIOS installation is complete.
Flash chipset:Macronix 29LV320B
0055000.FLS:280000 [80000]
Erasing block 2f:280000 - 28ffff
Erasing block 30:290000 - 29ffff
Erasing block 31:2a0000 - 2affff
Erasing block 32:2b0000 - 2bffff
Erasing block 33:2c0000 - 2cffff
Erasing block 34:2d0000 - 2dffff
Erasing block 35:2e0000 - 2effff
Erasing block 36:2f0000 - 2fffff
Programming block 2f:280000 - 28ffff
Programming block 30:290000 - 29ffff
Programming block 31:2a0000 - 2affff
Programming block 32:2b0000 - 2bffff
Programming block 33:2c0000 - 2cffff
Programming block 34:2d0000 - 2dffff
Programming block 35:2e0000 - 2effff
Programming block 36:2f0000 - 2fffff
SCSIROM.BIN:260000 [20000]
Erasing block 2d:260000 - 26ffff
Erasing block 2e:270000 - 27ffff
Programming block 2d:260000 - 26ffff
Programming block 2e:270000 - 27ffff
PXEROM.BIN:250000 [10000]
Erasing block 2c:250000 - 25ffff
Programming block 2c:250000 - 25ffff
Primary BIOS flashed successfully
Cleanup BIOS related files that were downloaded....
The new software will run after you reload.
WAE-7326#
```

Related Commands[install](#)[reload](#)[show running-config](#)[show startup-config](#)[wafs](#)

write

copy http

To copy configuration or image files from an HTTP server to the WAAS device, use the **copy http** EXEC command.

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

Syntax	Description
http	Copies the file from an HTTP server.
install	Copies the file from an HTTP server and installs the software release file to the local device.
<i>hostname</i>	Name of the HTTP server.
<i>ip-address</i>	IP address of the HTTP server.
<i>remotefiledir</i>	Remote file directory.
<i>remotefilename</i>	Remote filename.
port	(Optional) Port to connect to the HTTP server (default is 80).
<i>portnum</i>	HTTP server port number (1–65535).
proxy	(Optional) Allows the request to be redirected to an HTTP proxy server.
<i>proxy_portnum</i>	HTTP proxy server port number (1–65535).
username	(Optional) Username to access the HTTP proxy server.
<i>username</i>	User login name.
<i>password</i>	Establishes password authentication.

Defaults HTTP server port: 80

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines Use the **copy http install** EXEC command to install an image file from an HTTP server and install it on a WAAS device. It transfers the image from an HTTP server to the WAAS device using HTTP as the transport protocol and installs the software on the device. Part of the image goes to disk and part goes to flash memory. Use the **copy http central** EXEC command to download a software image into the repository from an HTTP server.

You can also use the **copy http install** EXEC commands 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 a primary domain controller (PDC) before the transfer of the software release file to the WAAS device is allowed.

Upgrading the BIOS

You can remotely upgrade the BIOS on the WAE-511, WAE-512, WAE-611, WAE-612, and the WAE-7326. All computer hardware has to work with software through an interface. The Basic Input Output System (BIOS) provides such an interface. It gives the computer a built-in starter kit to run the rest of the software from the hard disk drive. The BIOS is responsible for booting the computer by providing a basic set of instructions. It performs all the tasks that need to be done at start-up time, such as Power-On Self Test (POST) operations and booting the operating system from the hard disk drive. Furthermore, it provides an interface between the hardware and the operating system in the form of a library of interrupt handlers. For instance, each time a key is pressed, the CPU performs an interrupt to read that key, which is similar for other input/output devices, such as serial and parallel ports, video cards, sound cards, hard disk controllers, and so forth. Some older PCs cannot interoperate with all the modern hardware because their BIOS does not support that hardware; the operating system cannot call a BIOS routine to use it. This problem can be solved by replacing the BIOS with a newer one that does support your new hardware or by installing a device driver for the hardware.

All BIOS files needed for a particular hardware model BIOS update are available on Cisco.com as a single *.bin* package file. This file is a special *<WAAS-installable>.bin* file that you can install by using the normal software update procedure.

To update the BIOS version on a WAAS device that supports BIOS version updates, you need the following items:

- HTTP server with the software files
- Network connectivity between the device to be updated and the server hosting the update files
- Appropriate *.bin* BIOS update file:
 - 511_bios.bin
 - 611_bios.bin
 - 7326_bios.bin



Caution

Be *extraordinarily* careful when upgrading a Flash BIOS. Make *absolutely* sure that the BIOS upgrade patch is the exact one required. If you apply the wrong patch, you can render the system unbootable, making it difficult or impossible to recover even by reapplying the proper patch.



Caution

Because a failed Flash BIOS update can have dire results, never update a Flash BIOS without first connecting the system to an uninterruptible power supply (UPS).

To install the BIOS update file on a WAAS device, use the **copy http install EXEC** command as follows:

```
WAE# copy http install http-server remote_file_dir 7326_bios.bin
[portnumber]
```

After the BIOS update file is copied to your system, use the **reload EXEC** command to reboot the WAAS device as follows:

```
WAE# reload
```

The new BIOS takes effect after the system reboots.

Examples

The following example shows how to copy an image file from an HTTP server and install the file on the WAAS device:

```
WAE# copy http install 10.1.1.1 //ftp-sj.cisco.com/cisco/waas/4.0 WAAS-4.0.0-k9.bin
Enter username for remote ftp server:biff
Enter password for remote ftp server:*****
Initiating FTP download...
printing one # per 1MB downloaded
Sending:USER biff
10.1.1.1 FTP server (Version) Mon Feb 28 10:30:36 EST
2000) ready.
Password required for biff.
Sending:PASS *****
User biff logged in.
Sending:TYPE I
Type set to I.
Sending:PASV
Entering Passive Mode (128,107,193,244,55,156)
Sending:CWD //ftp-sj.cisco.com/cisco/waas/4.0
CWD command successful.
Sending PASV
Entering Passive Mode (128,107,193,244,55,156)
Sending:RETR WAAS-4.0.0-k9.bin
Opening BINARY mode data connection for ruby.bin (87376881 bytes).
#####
writing flash component:
.....
The new software will run after you reload.
```

The following example shows how to upgrade the BIOS. All output is written to a separate file (*/local/bios_upgrade.txt*) for traceability. The hardware dependant files that are downloaded from Cisco.com for the BIOS upgrade are automatically deleted from the WAAS device after the BIOS upgrade procedure has been completed.

```
WAE-7326# copy ftp install upgradserver /bios/update53/derived/ 7326_bios.bin
Enter username for remote ftp server:myusername
Enter password for remote ftp server:*****
Initiating FTP download...
printing one # per 1MB downloaded
Sending:USER myusername
upgradserver.cisco.com FTP server (Version wu-2.6.1-18) ready.
Password required for myusername.
Sending:PASS *****
Please read the file README_dotfiles
  it was last modified on Wed Feb 19 16:10:26 2005- 94 days ago
Please read the file README_first
  it was last modified on Wed Feb 19 16:05:29 2005- 94 days ago
User myusername logged in.
Sending:TYPE I
Type set to I.
Sending:PASV
Entering Passive Mode (128,107,193,240,57,37)
Sending:CWD /bios/update53/derived/
CWD command successful.
Sending PASV
Entering Passive Mode (128,107,193,240,146,117)
Sending:RETR 7326_bios.bin
Opening BINARY mode data connection for 7326_bios.bin (834689 bytes).
Fri Jan 7 15:29:07 UTC 2005
BIOS installer running!
Do not turnoff the system till BIOS installation is complete.
Flash chipset:Macronix 29LV320B
0055000.FLS:280000 [80000]
```

```
Erasing block 2f:280000 - 28ffff
Erasing block 30:290000 - 29ffff
Erasing block 31:2a0000 - 2affff
Erasing block 32:2b0000 - 2bffff
Erasing block 33:2c0000 - 2cffff
Erasing block 34:2d0000 - 2dffff
Erasing block 35:2e0000 - 2effff
Erasing block 36:2f0000 - 2fffff
Programming block 2f:280000 - 28ffff
Programming block 30:290000 - 29ffff
Programming block 31:2a0000 - 2affff
Programming block 32:2b0000 - 2bffff
Programming block 33:2c0000 - 2cffff
Programming block 34:2d0000 - 2dffff
Programming block 35:2e0000 - 2effff
Programming block 36:2f0000 - 2fffff
SCSIROM.BIN:260000 [20000]
Erasing block 2d:260000 - 26ffff
Erasing block 2e:270000 - 27ffff
Programming block 2d:260000 - 26ffff
Programming block 2e:270000 - 27ffff
PXEROM.BIN:250000 [10000]
Erasing block 2c:250000 - 25ffff
Programming block 2c:250000 - 25ffff
Primary BIOS flashed successfully
Cleanup BIOS related files that were downloaded...
The new software will run after you reload.
```

Related Commands[install](#)[reload](#)[show running-config](#)[show startup-config](#)[wafs](#)[write](#)

copy running-config

To copy a configuration or image data from the current configuration, use the **copy running-config EXEC** command.

```
copy running-config {disk filename | startup-config | tftp {hostname | ip-address}
                    remotefilename}
```

Syntax Description		
running-config		Copies the current system configuration.
disk		Copies the current system configuration to a disk file.
<i>filename</i>		Name of the file to be created on disk.
startup-config		Copies the running configuration to startup configuration (NVRAM).
tftp		Copies the running configuration to a file on a TFTP server.
<i>hostname</i>		Hostname of the TFTP server.
<i>ip-address</i>		IP address of the TFTP server.
<i>remotefilename</i>		Remote filename of the configuration file to be created on the TFTP server. Use the complete pathname.

Defaults No default behaviors or values

Command Modes EXEC

Device Modes

- application-accelerator
- replication-accelerator
- central-manager

Usage Guidelines Use the **copy running-config EXEC** command to copy the WAAS device's running system configuration to a SYSFS partition, flash memory, or TFTP server. The **copy running-config startup-config EXEC** command is equivalent to the **write memory EXEC** command.

Related Commands

- [install](#)
- [reload](#)
- [show running-config](#)
- [show startup-config](#)
- [wafs](#)
- [write](#)

copy startup-config

To copy configuration or image data from the startup configuration, use the **copy startup-config** EXEC command.

```
copy startup-config { disk filename | running-config | tftp { hostname | ip-address }
                    remotefilename }
```

Syntax Description		
startup-config		Copies the startup configuration.
disk		Copies the startup configuration to a disk file.
<i>filename</i>		Name of the startup configuration file to be copied to the local disk.
running-config		Copies the startup configuration to running configuration.
tftp		Copies the startup configuration to a file on a TFTP server.
<i>hostname</i>		Hostname of the TFTP server.
<i>ip-address</i>		IP address of the TFTP server.
<i>remotefilename</i>		Remote filename of the startup configuration file to be created on the TFTP server. Use the complete pathname.

Defaults No default behaviors or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines Use the **copy startup-config** EXEC command to copy the startup configuration file to a TFTP server or to a SYSFS partition.

Related Commands [install](#)
[reload](#)
[show running-config](#)
[show startup-config](#)
[wafs](#)
[write](#)

copy sysreport

To copy system troubleshooting information from the device, use the **copy sysreport** EXEC command.

```
copy sysreport {disk filename | ftp {hostname | ip-address} remotedirectory remotefilename | tftp
  {hostname | ip-address} remotefilename} [start-date {day month | month day} year [end-date
  {day month | month day} year]]
```

Syntax	Description
sysreport	Generates and saves a report containing WAAS system information in a file.
disk	Copies system information to a disk file.
<i>filename</i>	Name of the file to be created on disk. Note that .tar.gz is appended to the filename that you specify.
ftp	Copies system information to a FTP server.
<i>hostname</i>	Hostname of the FTP server.
<i>ip-address</i>	IP address of the FTP server.
<i>remotedirectory</i>	Remote directory where the system information file is to be created on the FTP server.
<i>remotefilename</i>	Remote filename of the system information file to be created on the FTP server.
tftp	Copies system information to a TFTP server.
<i>hostname</i>	Hostname of the TFTP server.
<i>ip-address</i>	IP address of the TFTP server.
<i>remotefilename</i>	Remote filename of the system information file to be created on the TFTP server. Use the complete pathname.
start-date	(Optional) Start date of information in the generated system report.
<i>day month</i>	Start date day of the month (1–31) and month of the year (January, February, March, April, May, June, July, August, September, October, November, December). You can alternately specify the month first, followed by the day.
<i>year</i>	Start date year (1993–2035).
end-date	(Optional) End date of information in the generated system report. If omitted, this date defaults to today's date. The report includes files through the end of this day.
<i>day month</i>	End date day of the month (1–31) and month of the year (January, February, March, April, May, June, July, August, September, October, November, December). You can alternately specify the month first, followed by the day.
<i>year</i>	End date year (1993–2035).

Defaults If **end-date** is not specified, today's date is used.

Command Modes EXEC

Device Modes

application-accelerator
replication-accelerator
central-manager

Usage Guidelines

The **copy sysreport** command consumes significant CPU and disk resources and can adversely affect system performance while it is running.

Examples

The following example shows how to copy system information to the file `mysysinfo` on the local WAAS device:

```
WAE# copy sysreport disk mysysinfo start-date 1 April 2006 end-date April 30 2006
```

The following example shows how to copy system information by FTP to the file `foo` in the root directory of the FTP server named `myserver`:

```
WAE# copy sysreport ftp myserver / foo start-date 1 April 2006 end-date April 30 2006
```

Related Commands

[show running-config](#)
[show startup-config](#)
[wafs](#)

copy system-status

To copy status information from the system for debugging, use the **copy system-status EXEC** command.

copy system-status disk *filename*

Syntax Description	system-status disk	Copies the system status to a disk file.
	<i>filename</i>	Name of the file to be created on the disk.

Defaults No default behaviors or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines Use the **copy system-status EXEC** command to create a file on a SYSFS partition that contains hardware and software status information.

Related Commands [install](#)
[reload](#)
[show running-config](#)
[show startup-config](#)
[wafs](#)
[write](#)

copy tech-support

To copy the configuration or image data from the system to use when working with Cisco TAC, use the **copy tech-support** EXEC command.

```
copy tech-support {disk filename | tftp {hostname | ip-address} remotefilename}
```

Syntax Description		
tech-support		Copies system information for technical support.
disk		Copies system information for technical support to disk file.
<i>filename</i>		Name of the file to be created on disk.
tftp		Copies system information for technical support to a TFTP server.
<i>hostname</i>		Hostname of the TFTP server.
<i>ip-address</i>		IP address of the TFTP server.
<i>remotefilename</i>		Remote filename of the system information file to be created on the TFTP server. Use the complete pathname.

Defaults No default behaviors or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines Use the **copy tech-support tftp** EXEC command to copy technical support information to a TFTP server or to a SYSFS partition.

Related Commands [install](#)
[reload](#)
[show running-config](#)
[show startup-config](#)
[wafs](#)
[write](#)

copy tftp

To copy configuration or image data from a TFTP server, use the **copy tftp** EXEC command.

```
copy tftp { disk { hostname | ip-address } remotefilename localfilename | running-config
  { hostname | ip-address } remotefilename | startup-config { hostname | ip-address }
  remotefilename }
```

Syntax Description	
tftp	Copies an image from a TFTP server.
disk	Copies an image from a TFTP server to a disk file.
<i>hostname</i>	Hostname of the TFTP server.
<i>ip-address</i>	IP address of the TFTP server.
<i>remotefilename</i>	Name of the remote image file to be copied from the TFTP server. Use the complete pathname.
<i>localfilename</i>	Name of the image file to be created on the local disk.
running-config	Copies an image from a TFTP server to the running configuration.
<i>hostname</i>	Hostname of the TFTP server.
<i>ip-address</i>	IP address of the TFTP server.
<i>remotefilename</i>	Name of the remote image file to be copied from the TFTP server. Use the complete pathname.
startup-config	Copies an image from a TFTP server to the startup configuration.
<i>hostname</i>	Hostname of the TFTP server.
<i>ip-address</i>	IP address of the TFTP server.
<i>remotefilename</i>	Name of the remote image file to be copied from the TFTP server. Use the complete pathname.

Defaults No default behaviors or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines Use the **copy tftp disk** EXEC command to copy a file from a TFTP server to disk.

Related Commands [install](#)
[reload](#)

show running-config

show startup-config

wafs

write

cpfile

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

```
cpfile oldfilename newfilename
```

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

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines Use this EXEC 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.

```
WAE# cpfile fe511-194616.bin fd511-194618.bin
```

Related Commands [deltree](#)
[dir](#)
[lls](#)
[ls](#)
[mkdir](#)
[pwd](#)
[rename](#)

debug

To monitor and record the WAAS application acceleration and central manager functions, use the **debug EXEC** command. To disable debugging, use the **no** form of the command. (See also the [undebug](#) command.)

In the application-accelerator device mode, the **debug** commands are as follows:

```
debug authentication { content-request | user | windows-domain }
debug buf { all | dmbuf | dmsg }
debug cdp { adjacency | events | ip | packets }
debug cli { all | bin | parser }
debug cms
debug dataserver { all | clientlib | server }
debug dhcp
debug dre { aggregation | all | cache | connection { aggregation [acl] | cache [acl] | core [acl] |
    message [acl] | misc [acl] | acl } | core | lz | message | misc }
debug epm
debug flow monitor tcpstat-v1
debug logging all
debug ntp
debug print-spooler { all | brief | errors | warnings }
debug rbcp
debug snmp { all | cli | main | mib | traps }
debug stats { all | collections | computation | history }
debug tfo { buffer-mgr | connection [auto-discovery [acl] | comp-mgr [acl] | conn-mgr [acl] |
    egress-method [acl] | filtering [acl] | netio-engine [acl] | policy-engine [acl] | synq [acl] | acl }
    | stat-mgr | translog }
debug translog export
debug wafs { { all | core-fe | edge-fe | manager | utilities } { debug | error | info | warn } }
debug wccp { all | detail | error | events | keepalive | packets | slowstart }
```

**Note**

The **dre**, **epm**, **flow monitor**, **print-spooler**, **rbcp**, **tfo**, **translog**, **wafs**, and **wccp** command options are supported in the application-accelerator device mode only.

In the central manager device mode, the **debug** commands are as follows:

```

debug aaa accounting

debug all

debug authentication {content-request | user | windows-domain}

debug buf {all | dmbuf | dmsg}

debug cdp {adjacency | events | ip | packets}

debug cli {all | bin | parser}

debug cms

debug dataserver {all | clientlib | server}

debug dhcp

debug emdb [level [levelnum]]

debug key-manager

debug logging all

debug ntp

debug rpc {detail | trace}

debug snmp {all | cli | main | mib | traps}

debug stats {all | collections | computation | history}

```

**Note**

The **emdb** and **rpc** command options are supported in the central manager device mode only.

Syntax Description

aaa accounting	(Optional) Enables AAA accounting actions.
all	(Optional) Enables all debugging options.
authentication	(Optional) Enables authentication debugging.
content-request	Enables content request authentication debugging.
user	Enables debugging of the user login against the system authentication.
windows-domain	Enables Windows domain authentication debugging.
buf	(Optional) Enables buffer manager debugging.
all	Enables all buffer manager debugging.
dmbuf	Enables only dmbuf debugging.
dmsg	Enables only dmsg debugging.
cdp	(Optional) Enables CDP debugging.
adjacency	Enables CDP neighbor information debugging.

events	Enables CDP events debugging.
ip	Enables CDP IP debugging.
packets	Enables packet-related CDP debugging.
cli	(Optional) Enables CLI debugging.
all	Enables all CLI debugging.
bin	Enables CLI command binary program debugging.
parser	Enables CLI command parser debugging.
cms	(Optional) Enables CMS debugging.
dataserver	(Optional) Enables data server debugging.
all	Enables all data server debugging.
clientlib	Enables data server client library module debugging.
server	Enables data server module debugging.
dhcp	(Optional) Enables DHCP debugging.
dre	(Optional) Enables DRE debugging.
aggregation	Enables DRE chunk-aggregation debugging.
all	Enables the debugging of all DRE commands.
cache	Enables DRE cache debugging.
connection	Enables DRE connection debugging.
aggregation [<i>acl</i>]	Enables DRE chunk-aggregation debugging for a specified connection.
cache [<i>acl</i>]	Enables DRE cache debugging for a specified connection.
core [<i>acl</i>]	Enables DRE core debugging for a specified connection.
message [<i>acl</i>]	Enables DRE message debugging for a specified connection.
misc [<i>acl</i>]	Enables DRE other debugging for a specified connection.
<i>acl</i>	ACL to limit connections traced.
core	Enables DRE core debugging.
message	Enables DRE message debugging.
misc	Enables DRE other debugging.
epm	(Optional) Enables the DCE-RPC EPM debugging.
flow	(Optional) Enables network traffic flow debugging.
monitor	Enables monitor flow performance debugging commands.
tcpstat-v1	Enables tcpstat-v1 debugging.
logging	(Optional) Enables logging debugging.
all	Enables all logging debugging.
ntp	(Optional) Enables NTP debugging.
print-spooler	(Optional) Enables print spooler debugging.
all	Enables print spooler debugging using all debug features.
brief	Enables print spooler debugging using only brief debug messages.
errors	Enables print spooler debugging using only the error conditions.
warnings	Enables print spooler debugging using only the warning conditions.

rbcpl	(Optional) Enables RBCP debugging.
snmp	(Optional) Enables SNMP debug commands.
all	Enables all SNMP debug commands.
cli	Enables SNMP CLI debugging.
main	Enables SNMP main debugging.
mib	Enables SNMP MIB debugging.
traps	Enables SNMP trap debugging.
stats	(Optional) Enables statistics debugging.
all	Enables all statistics debug commands.
collection	Enables collection statistics debugging.
computation	Enables computation statistics debugging.
history	Enables history statistics debugging.
tfo	(Optional) Enables TFO debugging.
buffer-mgr	Enables TFO buffer manager debugging.
connection	Enables TFO connection debugging.
auto-discovery [<i>acl</i>]	Enables TFO connection debugging for the auto-discovery module.
comp-mgr [<i>acl</i>]	Enables TFO connection debugging for the compression module.
conn-mgr [<i>acl</i>]	Enables TFO connection debugging for the connection manager.
egress-method [<i>acl</i>]	Enables TFO connection debugging for the connection egress method.
filtering [<i>acl</i>]	Enables TFO connection debugging for filtering module.
netio-engine [<i>acl</i>]	Enables TFO connection debugging for network input/output module.
policy-engine [<i>acl</i>]	Enables TFO connection debugging of application policies.
synq [<i>acl</i>]	Enables TFO connection debugging for the SynQ module.
<i>acl</i>	ACL to limit TFO connections.
stat-mgr	Enables TFO statistics manager debugging.
translog	Enables TFO transaction log debugging.
translog	(Optional) Enables transaction logging debug commands.
export	Enables transaction log FTP export debugging.
wafs	(Optional) Unsets the notification level (debug, info, warn, error) at which messages from the WAAS software component and utilities are logged.
all	Unsets the logging level for all software components and utilities at once.
core-fe	Unsets the logging level for WAEs acting as a core File Engine.
edge-fe	Unsets the logging level for WAEs acting as an edge File Engine.
manager	Unsets the logging level for the Device Manager.
utilities	Unsets the logging level for WAAS utilities.
wccp	(Optional) Enables the WCCP information debugging.
all	Enables all WCCP debugging functions.
detail	Enables the WCCP detail debugging.

error	Enables the WCCP error debugging.
events	Enables the WCCP events debugging.
keepalive	Enables the debugging for WCCP keepalives that are sent to the applications.
packets	Enables the WCCP packet-related information debugging.
slowstart	Enables the WCCP slow-start debugging.

The following syntax table describes the options that are available in the central manager device mode:

emdb	(Optional) Enables embedded database debugging.
level	(Optional) Enables the specified debug level for EMDB service.
<i>levelnum</i>	(Optional) Debug level to disable. (Level 0 disables debugging.)
key-manager	(Optional) Enables the Central Manager key manager debugging.
rpc	(Optional) Enables the remote procedure calls (RPC) logs.
detail	Enables the RPC logs of priority “detail” level or higher.
trace	Enables the RPC logs of priority “trace” level or higher.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator
 replication-accelerator
 central-manager

Usage Guidelines

Because the performance of the WAAS device degrades when you use the **debug** command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the [“Obtaining Documentation and Submitting a Service Request”](#) section on page xvi.

If the watchdog utility is not running, the message “WAAS is not running” appears.

Use the **show debugging** command to display enabled **debug** options.

Examples

The following example shows how to enable debug monitoring of user authentication, verify it is enabled, and then disable debug monitoring:

```
WAE# debug authentication user
WAE# show debugging
Debug authentication (user) is ON
WAE# no debug authentication user
```

The following example shows how to set the logging level to debug for the Core WAEs in your system, then return the logging level to its default (info):

```
WAE# debug wafs ?
all          log level for all components
core-fe     log level for Core FE
edge-fe     log level for Edge FE
manager     log level for Manager
utilities   log level for Utilities
WAE# debug wafs core-fe ?
debug       set log level to DEBUG
error       set log level to ERROR
info        set log level to INFO (default)
warn        set log level to WARN
WAE# debug wafs core-fe debug
corefe log level set to DEBUG
```

Related Commands

- [show debugging](#)
- [undebug](#)

delfile

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

delfile *filename*

Syntax Description

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

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator
replication-accelerator
central-manager

Usage Guidelines

Use this EXEC command to remove a file from a SYSFS partition on the disk drive of the WAAS device.

Examples

The following example shows how to delete a temporary file from the */local1* directory using an absolute path:

```
WAE# delfile /local1/tempfile
```

Related Commands

[cpfile](#)
[dir](#)
[lls](#)
[ls](#)
[mkdir](#)
[pwd](#)
[rename](#)

deltree

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

deltree *directory*

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

Defaults	No default behavior or values
-----------------	-------------------------------

Command Modes	EXEC
----------------------	------

Device Modes	application-accelerator replication-accelerator central-manager
---------------------	-----------------------------------------------------------------------

Usage Guidelines	Use this EXEC command to remove a directory and all files within the directory from the WAAS SYSFS file system. No warning is given that you are removing the subdirectories and files.
-------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



Note

Be sure you do not remove files or directories required for the WAAS device to function properly.

Examples	The following example shows how to delete the <i>testdir</i> directory from the <i>/local1</i> directory:
-----------------	-----------------------------------------------------------------------------------------------------------

```
WAE# deltree /local1/testdir
```

Related Commands	cpfile dir lls ls mkdir pwd rename
-------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------

dir

To view details of one file or all files in a directory, use the **dir** EXEC command.

dir [*directory*]

Syntax Description

directory (Optional) Name of the directory to list.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator
 replication-accelerator
 central-manager

Usage Guidelines

Use this EXEC command to view a detailed list of files contained within the working directory, including names, sizes, and time created. The **lls** EXEC command produces the same output.

Examples

The following example shows a detailed list of all the files for the current directory:

```
WAE# dir
size          time of last change          name
-----
    4096  Fri Feb 24 14:40:00 2006 <DIR>  actona
    4096  Tue Mar 28 14:42:44 2006 <DIR>  core_dir
    4096  Wed Apr 12 20:23:10 2006 <DIR>  crash
    4506  Tue Apr 11 13:52:45 2006      dbupgrade.log
    4096  Tue Apr  4 22:50:11 2006 <DIR>  downgrade
    4096  Sun Apr 16 09:01:56 2006 <DIR>  errorlog
    4096  Wed Apr 12 20:23:41 2006 <DIR>  logs
   16384  Thu Feb 16 12:25:29 2006 <DIR>  lost+found
    4096  Wed Apr 12 03:26:02 2006 <DIR>  sa
   24576  Sun Apr 16 23:38:21 2006 <DIR>  service_logs
    4096  Thu Feb 16 12:26:09 2006 <DIR>  spool
  9945390  Sun Apr 16 23:38:20 2006      syslog.txt
  10026298  Thu Apr  6 12:25:00 2006      syslog.txt.1
  10013564  Thu Apr  6 12:25:00 2006      syslog.txt.2
  10055850  Thu Apr  6 12:25:00 2006      syslog.txt.3
  10049181  Thu Apr  6 12:25:00 2006      syslog.txt.4
    4096  Thu Feb 16 12:29:30 2006 <DIR>  var
    508   Sat Feb 25 13:18:35 2006      wdd.sh.signed
```

The following example shows only the detailed information for the *logs* directory:

```
WAE# dir logs
size          time of last change          name
-----
4096 Thu Apr 6 12:13:50 2006 <DIR> actona
4096 Mon Mar 6 14:14:41 2006 <DIR> apache
4096 Sun Apr 16 23:36:40 2006 <DIR> emdb
4096 Thu Feb 16 11:51:51 2006 <DIR> export
  92 Wed Apr 12 20:23:20 2006 ftp_export.status
4096 Wed Apr 12 20:23:43 2006 <DIR> rpc_httpd
  0 Wed Apr 12 20:23:41 2006 snmpd.log
4096 Sun Mar 19 18:47:29 2006 <DIR> tfo
```

Related Commands[lls](#)[ls](#)

disable

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

disable

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines Use the WAAS software CLI EXEC mode for setting, viewing, and testing system operations. This command mode is divided into two access levels, user and privileged. To access privileged-level EXEC mode, enter the **enable** EXEC command at the user access level prompt and specify a privileged EXEC password (superuser or admin-equivalent password) when prompted for a password.

```
WAE> enable
Password:
```

The **disable** command places you in the user-level EXEC shell (notice the prompt change).

Examples The following example enters the user-level EXEC mode from the privileged EXEC mode:

```
WAE# disable
WAE>
```

Related Commands [enable](#)

disk

To configure disks on a WAAS device, use the **disk EXEC** command.

disk delete-partitions *diskname*


disk disk-name diskxx replace

disk insert *diskname*

disk recreate-raid

disk reformat *diskname*

disk scan-errors *diskname*

delete-partitions	Deletes data on the specified logical disk drive. After using this command, the WAAS software treats the specified disk drive as blank. All previous data on the drive is inaccessible.
<i>diskname</i>	Name of the disk from which to delete partitions (disk00, disk01). For RAID-5 systems, this option is not available because only one logical drive is available.
disk-name diskxx replace	Shuts down the physical disk with the name diskxx (disk00, disk01, etc.) so that it can be replaced in the RAID-5 array. Note This option is available only on RAID-5 systems.
insert	Instructs the SCSI host to rescan the bus to detect and mount the newly inserted disk. Note This option is available only on WAE-612 and WAE-7326 models.
<i>diskname</i>	Name of the disk to be inserted (disk00, disk01).
recreate-raid	Recreates the RAID-5 array. Note This option is available only on RAID-5 systems.
reformat	Performs a low-level reformatting of a SCSI disk drive and remaps bad sectors.  Caution Use this command with extreme caution to avoid loss of data. Note This option is not available on RAID-5 systems.
<i>diskname</i>	Name of the disk to be reformatted (disk00, disk01).
scan-errors	Scans SCSI or IDE disks for errors and remaps the bad sectors, if they are unused. For RAID-5 systems, this command scans the logical RAID device for errors. On these systems, there is no <i>diskname</i> option.
<i>diskname</i>	Name of the disk to be reformatted (disk00, disk01).

Command Modes EXEC

Device Modes

application-accelerator
 replication-accelerator
 central-manager

Usage Guidelines**Logical Disk Handling with RAID-5**

Logical disk handling with Redundant Array of Independent Disks-5 (RAID-5) is implemented in WAAS as a hardware feature. RAID-5 devices can create a single logical disk drive that may contain up to six physical hard disk drives, providing increased logical disk capacity. (The WAE-7341 supports four disks, and the WAE-7371 supports six disks.)

Systems with RAID-5 continue operating if one of the physical drives fails (RAID-5 moves the drive to the Defunct state). RAID-5 also permits hot-swapping of the disk hardware after the failed drive is properly shutdown. (For the disk removal and replacement procedure for RAID-5 systems, see the *Cisco Wide Area Application Services Configuration Guide*, Chapter 14.)

Logical Disk Handling with RAID-1

RAID-1 is implemented in WAAS as a software feature. A RAID-1 WAAS device can use two disk drives to increase reliability. RAID-1 provides disk mirroring (data is written redundantly to two or more drives). The goal is higher reliability through redundancy. With RAID-1, file system write performance may be affected because each disk write must be executed against two disk drives. RAID-1 (mirroring) is used for all file systems on the RAID-1 device. This setup ensures reliable execution of the software in all cases.

**Note**

The WAAS software uses the CONTENT file system for both the Wide Area File Services (WAFS) file system and the data redundancy elimination (DRE) cache.

Hot Swap for WAE-612, WAE-7326, WAE-7341, and WAE-7371 Disk Drives

This release of WAAS supports hot swap functionality for both failed disk replacement and scheduled disk maintenance. On the WAE-612 and WAE-7326, use the **disk disk-name diskxx shutdown** global configuration command to shut down a disk for scheduled disk maintenance. On the WAE-7341 and WAE-7371, use the **disk disk-name diskxx replace EXEC** command to shut down a disk. (For the scheduled disk maintenance procedure, see the *Cisco Wide Area Application Services Configuration Guide*, Chapter 14.)

You must wait for the disk to be completely shut down before you physically remove the disk from the WAE. When the RAID removal process is complete, WAAS generates a disk failure alarm and trap. In addition, a syslog ERROR message is logged.

If the software removes a failed disk during the RAID rebuild process, a RAID rebuild failure alarm is generated. If you administratively shut down the disk during the RAID rebuild process, a RAID rebuild abort alarm is generated instead.

If the removal event occurs while the RAID is in the rebuild process, the RAID removal process may take up to one minute before it is successful. The exact duration of this process depends on the size of the disk.

Automatic Failed Disk Handling

The disk hot swap functionality automatically disables a failed disk if the system detects one critical disk alarm. The software removes the failed disk automatically regardless of the setting for **disk error-handling**.

Replacing a Failed Disk

For WAE-7341 and WAE-7371 models, when you replace a failed disk that was automatically disabled by the software, the disk automatically returns to service. For WAE-612 and WAE-7326 models, when you replace a failed disk that was automatically disabled by the software, use the **disk insert** command in EXEC mode to bring the disk back into service. For all other models, see the [\(config\) disk disk-name](#) command section.

Recreating the RAID-5 Disk Array

To recreate the logical disk array for RAID-5 systems, use the EXEC mode **disk recreate-raid** command, as shown in following configuration sequence:

```
WAE-7341(config)# disk logical shutdown
WAE-7341# reload
WAE-7341# copy running-config startup-config
```

Wait for the system to boot up.

```
WAE-7341# disk recreate-raid
WAE-7341(config)# no disk logical shutdown
WAE-7341# reload
WAE-7341# copy running-config startup-config
```

After the system boots, wait approximately half an hour for all of the filesystems to be recreated.



Caution

When you recreate the RAID-5 disk array, you lose all data on the drives.

Reinstall the software by entering **copy ftp install** in EXEC mode.

For 300 GB SAS drives, recreating and synchronizing the RAID array may take up to five hours. While the RAID-5 synchronization is running in the background, the system will be fully functional; however, performance may be affected by the background operation.

Disk Information

To identify which disks have been identified as failed or bad, use the **show disks failed-disk-id** EXEC command. Do not reinsert any disk with a serial number shown in this list.



Note

This command is not available on WAE-7341 and WAE-7371 models.

Reformatting a SCSI Disk Drive

Use the **disk reformat** EXEC command to reformat a SCSI disk drive on a WAAS device. The SCSI drive cannot be in use when you execute this command.



Caution

To avoid loss of data, use this command with extreme caution.



Note

This command is only available on WAE-612 systems with SCSI drives. This command is removed for WAE-611 and WAE-7326 systems in WAAS 4.0.13.

The following scenario shows how to reformat a SCSI drive:

1. Unmount the filesystem and remove the disk from the RAID-1 array by using the **disk disk-name diskxx shutdown** command in global configuration mode.

```
WAE611(config)# disk disk-name disk01 shutdown
```

2. Reformat the disk. On completion of this command the drive is blank.

```
WAE611# disk reformat disk01
```

3. Bring the disk back into service by using the **no disk disk-name diskxx shutdown** command in global configuration mode.

```
WAE611(config)# no disk disk-name disk01 shutdown
```

To use the **disk scan errors** command, follow the same procedure as for the **disk reformat** command.

Removing All Disk Partitions on a Single Disk Drive and Removing the Disk Partition on the Logical Drive for RAID-5 Systems

Use the **disk delete-partitions EXEC** command to remove all disk partitions on a single disk drive on a WAAS device or to remove the disk partition on the logical drive for RAID-5 systems.



Caution

After using the **disk delete-partitions EXEC** command, the WAAS software treats the specified disk drive as blank. All previous data on the drive is inaccessible.

Use this command when you want to add a new disk drive that was previously used with another operating system (for example, a Microsoft Windows or Linux operating system). When asked if you want to erase everything on the disk, specify “yes” to proceed, as follows:

```
WAE# disk delete-partitions disk01
This will erase everything on disk. Are you sure? [no] yes
```



Note

When you use the **disk delete-partitions EXEC** command on the WAE-7341 or WAE-7371 models, the command deletes the entire logical volume. The individual disk name option is not available on these platforms.

Related Commands

(config) [disk disk-name](#)
 (config) [disk error-handling](#)
 (config) [disk logical shutdown](#)
[show disks](#)

dnslookup

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

```
dnslookup {hostname | domainname}
```

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

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator
 replication-accelerator
 central-manager

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

```
WAE# dnslookup myhost
official hostname: myhost.abc.com
address: 172.31.69.11
```

```
WAE# dnslookup abc.com
official hostname: abc.com
address: 192.168.219.25
```

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

enable

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

enable

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines Use the WAAS software CLI EXEC mode for setting, viewing, and testing system operations. This command mode is divided into two access levels: user and privileged. To access privileged-level EXEC mode, enter the **enable** EXEC command at the user access level prompt and specify a privileged EXEC password (superuser or admin-equivalent password) when prompted for a password.

In TACACS+, there is an enable password feature that allows an administrator to define a different enable password per administrative-level user. If an administrative-level user logs in to the WAAS device with a normal-level user account (privilege level of 0) instead of an admin or admin-equivalent user account (privilege level of 15), that user must enter the admin password to access privileged-level EXEC mode.

```
WAE> enable
Password:
```



Note

This caveat applies even if the WAAS users are using TACACS+ for login authentication.

The **disable** command takes you from privileged EXEC mode to user EXEC mode.

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

```
WAE> enable
WAE#
```

Related Commands [disable](#)
[exit](#)

exit

To terminate privileged-level EXEC mode and return to the user-level EXEC mode, use the **exit** command.

exit

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes All modes

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines This command is equivalent to the **Ctrl-Z** or the **end** command. The **exit** command issued in the user level EXEC shell terminates the console or Telnet session.

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

```
WAE# exit  
WAE>
```

find-pattern

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

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

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

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator
 replication-accelerator
 central-manager

Usage Guidelines Use this EXEC 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:

```
WAE# find-pattern case recursive admin removed_core
-rw----- 1 admin root 95600640 Oct 12 10:27 /local/local1/core_dir/
core.3.0.0.b5.eh.2796
-rw----- 1 admin root 97054720 Jan 11 11:31 /local/local1/core_dir/
core.cache.3.0.0.b131.cnbuild.14086
-rw----- 1 admin root 96845824 Jan 11 11:32 /local/local1/core_dir/
core.cache.3.0.0.b131.cnbuild.14823
-rw----- 1 admin root 101580800 Jan 11 12:01 /local/local1/core_dir/
core.cache.3.0.0.b131.cnbuild.15134
-rw----- 1 admin root 96759808 Jan 11 12:59 /local/local1/core_dir/
core.cache.3.0.0.b131.cnbuild.20016
```

```
-rw----- 1 admin root 97124352 Jan 11 13:26 /local/local1/core_dir/  
core.cache.3.0.0.b131.cnbuild.8095
```

The following example shows how to search a file for a pattern and print the matching lines:

```
WAE# 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/  
core.3.0.0.b5.eh.2796  
-rw----- 1 admin root 101580800 Jan 11 12:01 /local/local1/core_dir/  
core.cache.3.0.0.b131.cnbuild.15134
```

The following example shows how to search a file for a pattern and print the number of matching lines:

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

Related Commands

[cd](#)
[dir](#)
[lls](#)
[ls](#)

help

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

help

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC and global configuration

Device Modes application-accelerator
replication-accelerator
central-manager

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

Two styles of help are provided:

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

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

```
WAE# 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.
2. Partial help is provided when an abbreviated argument is entered.

install

To install a new software image (such as the WAAS software) into flash on the WAAS device, use the **install EXEC** command.

```
install imagefilename
```

Syntax Description

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

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator
 replication-accelerator
 central-manager

Usage Guidelines

The **install** command loads the system image into flash memory and copies components of the optional software to the software file system (swfs) partition.



Note

If you are installing a system image that contains optional software, make sure that an SWFS partition is mounted on disk00.

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



Note

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

Examples

The following example loads the system image contained in the *wae511-cache-300.bin* file:

```
WAE# install wae511-cache-300.bin
```

Related Commands

[copy disk](#)

reload

less

To display a file using the LESS application, use the **less** EXEC command.

```
less file_name
```

Syntax Description

<i>file_name</i>	Name of the file to be displayed.
------------------	-----------------------------------

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator
 replication-accelerator
 central-manager

Usage Guidelines

LESS is an application that displays text files a page at a time. You can use LESS to view the contents of a file, but not edit it. LESS offers some additional features when compared to conventional text file viewer applications such as type. These features are as follows:

- **Backward movement**—LESS allows you to move backward in the displayed text. Use **k**, **Ctrl-k**, **y**, or **Ctrl-y** to move backward. See the summary of LESS commands for more details; to view the summary, press **h** or **H** while displaying a file in LESS.
- **Searching and highlighting**—LESS allows you to search for text in the file that you are viewing. You can search forward and backward. LESS highlights the text that matches your search to make it easy to see where the match is.
- **Multiple file support**—LESS allows you to switch between different files, remembering your position in each file. You can also do a search that spans all the files you are working with.

Examples

The following example shows how to display the text of the *syslog.txt* file using the LESS application:

```
WAE# less syslog.txt
```

lls

To view a long list of directory names, use the **lls** EXEC command.

lls [*directory*]

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

Defaults	No default behavior or values
-----------------	-------------------------------

Command Modes	EXEC
----------------------	------

Device Modes	application-accelerator replication-accelerator central-manager
---------------------	-----------------------------------------------------------------------

Usage Guidelines	This command provides detailed information about files and subdirectories stored in the present working directory (including size, date, time of creation, SYSFS name, and long name of the file). This information can also be viewed with the dir command.
-------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Examples	The following example provides a detailed list of the files in the current directory:
-----------------	---------------------------------------------------------------------------------------

```
WAE# lls
size          time of last change          name
-----
      4096  Fri Feb 24 14:40:00 2006 <DIR>  actona
      4096  Tue Mar 28 14:42:44 2006 <DIR>  core_dir
      4096  Wed Apr 12 20:23:10 2006 <DIR>  crash
      4506  Tue Apr 11 13:52:45 2006      dbupgrade.log
      4096  Tue Apr  4 22:50:11 2006 <DIR>  downgrade
      4096  Sun Apr 16 09:01:56 2006 <DIR>  errorlog
      4096  Wed Apr 12 20:23:41 2006 <DIR>  logs
     16384  Thu Feb 16 12:25:29 2006 <DIR>  lost+found
      4096  Wed Apr 12 03:26:02 2006 <DIR>  sa
     24576  Sun Apr 16 23:54:30 2006 <DIR>  service_logs
      4096  Thu Feb 16 12:26:09 2006 <DIR>  spool
     9951236 Sun Apr 16 23:54:20 2006      syslog.txt
    10026298 Thu Apr  6 12:25:00 2006      syslog.txt.1
    10013564 Thu Apr  6 12:25:00 2006      syslog.txt.2
    10055850 Thu Apr  6 12:25:00 2006      syslog.txt.3
    10049181 Thu Apr  6 12:25:00 2006      syslog.txt.4
      4096  Thu Feb 16 12:29:30 2006 <DIR>  var
       508  Sat Feb 25 13:18:35 2006      wdd.sh.signed
```

Related Commands [dir](#)
 [lls](#)
 [ls](#)

ls

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

ls [*directory*]

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

Defaults	No default behavior or values
-----------------	-------------------------------

Command Modes	EXEC
----------------------	------

Device Modes	application-accelerator replication-accelerator central-manager
---------------------	-----------------------------------------------------------------------

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

Examples	The following example shows the files and subdirectories that are listed within the root directory:
-----------------	-----------------------------------------------------------------------------------------------------

```
WAE# ls
actona
core_dir
crash
dbupgrade.log
downgrade
errorlog
logs
lost+found
sa
service_logs
spool
syslog.txt
syslog.txt.1
syslog.txt.2
syslog.txt.3
syslog.txt.4
var
wdd.sh.signed
```

Related Commands	dir
-------------------------	---------------------

lls
pwd

mkdir

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

mkdir *directory*

Syntax Description

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

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator
 replication-accelerator
 central-manager

Usage Guidelines

Use this EXEC command to create a new directory or subdirectory in the WAAS file system.

Examples

The following example shows how to create a new directory, *oldpaxfiles*:

```
WAE# mkdir /oldpaxfiles
```

Related Commands

[cpfile](#)
[dir](#)
[lls](#)
[ls](#)
[pwd](#)
[rename](#)
[rmdir](#)

mkfile

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

mkfile *filename*

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

Defaults	No default behavior or values
-----------------	-------------------------------

Command Modes	EXEC
----------------------	------

Device Modes	application-accelerator replication-accelerator central-manager
---------------------	-----------------------------------------------------------------------

Usage Guidelines	Use this EXEC command to create a new file in any directory of the WAAS device.
-------------------------	---------------------------------------------------------------------------------

Examples	The following example shows how to create a new file, <i>traceinfo</i> , in the root directory: WAE# mkfile traceinfo
-----------------	---------------------------------------------------------------------------------------------------------------------------------

Related Commands	cpfile dir lls ls mkdir pwd rename
-------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------

ntpdate

To set the software clock (time and date) on a WAAS device using a NTP server, use the **ntpdate** EXEC command.

```
ntpdate {hostname | ip-address} [key {authentication-key}]
```

Syntax Description

<i>hostname</i>	NTP hostname.
<i>ip-address</i>	NTP server IP address.
key	Add this argument to use authentication with the NTP server.
<i>authentication-key</i>	The authentication key string to use with the NTP server authentication. This value must be between 0 and 4294967295.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator
 replication-accelerator
 central-manager

Usage Guidelines

Use NTP to find the current time of day and set the current time on the WAAS device to match. The time must be saved to the hardware clock using the **clock save** command if it is to be restored after a reload.

Examples

The following example shows how to set the software clock on the WAAS device using an NTP server:

```
WAE# ntpdate 10.11.23.40
```

Related Commands

[clock](#)
[\(config\) clock](#)
[\(config\) ntp](#)
[show clock](#)
[show ntp](#)

ping

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

```
ping {hostname | ip-address}
```

Syntax Description

<i>hostname</i>	Hostname of system to ping.
<i>ip-address</i>	IP address of system to ping.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator
 replication-accelerator
 central-manager

Usage Guidelines

To use this command with the *hostname* argument, be sure that DNS functionality is configured the WAAS device. To force the timeout of a nonresponsive host, or to eliminate a loop cycle, press **Ctrl-C**.

Examples

The following example shows how to send echo packets to a machine with address 172.19.131.189 to verify its availability on the network:

```
WAE# 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
WAE#
```

pwd

To view the present working directory on a WAAS device, use the **pwd** EXEC command.

pwd

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines Use this EXEC command to display the present working directory of the WAAS device.

Examples The following example shows how to display the current working directory:

```
WAE# pwd
/local1
```

Related Commands [cd](#)
[dir](#)
[lls](#)
[ls](#)

reload

To halt and perform a cold restart on a WAAS device, use the **reload** EXEC command.

reload [force]

Syntax Description	force (Optional) Forces a reboot without further prompting.
Defaults	No default behavior or values
Command Modes	EXEC
Device Modes	application-accelerator replication-accelerator central-manager
Usage Guidelines	To reboot a WAAS device, use the reload command. If no configurations are saved to flash memory, you are prompted to enter configuration parameters upon restart. Any open connections are dropped after you issue this command, and the file system is reformatted upon restart.
Examples	The following example shows how to halt operation of the WAAS device and reboot it with the configuration saved in flash memory. You are not prompted for confirmations during the process. WAE# reload force
Related Commands	write

rename

To rename a file on a WAAS device, use the **rename** EXEC command.

```
rename oldfilename newfilename
```

Syntax Description

<i>oldfilename</i>	Original filename.
<i>newfilename</i>	New filename.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator
 replication-accelerator
 central-manager

Usage Guidelines

Use this command to rename any SYSFS file without making a copy of the file.

Examples

The following example shows how to rename the *errlog.txt* file to *old_errlog.txt*:

```
WAE# rename errlog.txt old_errlog.txt
```

Related Commands

[cpfile](#)

restore

To restore the device to its manufactured default status, removing user data from disk and flash memory, use the **restore** EXEC command.

```
restore { factory-default [preserve basic-config] | rollback }
```

Syntax Description		
factory-default		Resets the device configuration and data to their manufactured default status.
preserve	(Optional)	Preserves certain configurations and data on the device.
basic-config	(Optional)	Selects basic network configurations.
rollback		Roll back configuration to the last functional software and device configuration.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines Use this EXEC command to restore data on disk and in flash memory to the factory default, while preserving particular time stamp evaluation data, or to roll back the configuration to the last functional data and device configuration.

This command erases all existing content on the device; however, your network settings are preserved and the device is accessible through a Telnet and Secure Shell (SSH) session after it reboots.

Backing up the Central Manager Database

Before you use the **restore factory-default** command on your primary WAAS Central Manager or change over from the primary to a standby WAAS Central Manager, be sure to back up the WAAS Central Manager database and copy the backup file to a safe location that is separate from that of the WAAS Central Manager. You must halt the operation of the WAAS Central Manager before you enter the backup and restore commands.



Caution

This command erases user-specified configuration information stored in the flash image, removes data on disk, user-defined disk partitions, and the entire Central Manager database. User-defined disk partitions that are removed include the SYSFS, WAAS, and PRINTSPOOLFS partitions. The configuration being removed includes the starting configuration of the device.

By removing the WAAS Central Manager database, all configuration records for the entire WAAS network are deleted. If you do not have a valid backup file or a standby WAAS Central Manager, you must reregister every WAE with the WAAS Central Manager because all previously configured data is lost.

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

If you created a backup file while you configured the primary WAAS Central Manager, you can copy the backup file to this newly reconfigured WAAS Central Manager.

Rolling Back the Configuration

You can roll back the software and configuration of a WAAS device to a previous version using the **restore rollback** command. You would roll back software only in cases in which a newly installed version of the WAAS software is not functioning properly.

The **restore rollback** command installs the last saved WAAS.bin image on the system disk. A WAAS.bin image is created during software installation and stored on the system disk. If the WAAS device does not have a saved version, the software is not rolled back.



Note

While WAFS to WAAS migration is supported, rollback from WAAS to WAFS is not supported.

Examples

The following two examples show how to use 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.

```
WAE# restore factory-default
```

```
This command will wipe out all of data on the disks
and wipe out WAAS 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]
```

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

```
This command will wipe out all of data on the disks
and all of WAAS 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 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 details** command after the **restore** command is used verifies that the **restore** command has removed data from the partitioned file systems SYSFS, WAAS, and PRINTSPOOLFS:

```
WAE# show disks details
```

```
Physical disk information:
```

```
disk00: Normal                (h00 c00 i00 100 - DAS)    140011MB(136.7GB)
disk01: Normal                (h00 c00 i01 100 - DAS)    140011MB(136.7GB)
```

```
Mounted filesystems:
```

MOUNT POINT	TYPE	DEVICE	SIZE	INUSE	FREE	USE%
/	root	/dev/root	35MB	30MB	5MB	85%
/swstore	internal	/dev/md1	991MB	333MB	658MB	33%
/state	internal	/dev/md2	3967MB	83MB	3884MB	2%
/disk00-04	CONTENT	/dev/md4	122764MB	33MB	122731MB	0%
/local/local1	SYSFS	/dev/md5	3967MB	271MB	3696MB	6%
.../local1/spool	PRINTSPOOL	/dev/md6	991MB	16MB	975MB	1%
/sw	internal	/dev/md0	991MB	424MB	567MB	42%

```
Software RAID devices:
```

DEVICE NAME	TYPE	STATUS	PHYSICAL DEVICES AND STATUS	
/dev/md0	RAID-1	NORMAL OPERATION	disk00/00 [GOOD]	disk01/00 [GOOD]
/dev/md1	RAID-1	NORMAL OPERATION	disk00/01 [GOOD]	disk01/01 [GOOD]
/dev/md2	RAID-1	NORMAL OPERATION	disk00/02 [GOOD]	disk01/02 [GOOD]
/dev/md3	RAID-1	NORMAL OPERATION	disk00/03 [GOOD]	disk01/03 [GOOD]
/dev/md4	RAID-1	NORMAL OPERATION	disk00/04 [GOOD]	disk01/04 [GOOD]
/dev/md5	RAID-1	NORMAL OPERATION	disk00/05 [GOOD]	disk01/05 [GOOD]
/dev/md6	RAID-1	NORMAL OPERATION	disk00/06 [GOOD]	disk01/06 [GOOD]

```
Currently content-filefilesystems RAID level is not configured to change.
```

The following example shows how to upgrade or restore an older version of the WAAS software. In the first example below, version Y of the software is installed (using the **copy** command), but the administrator has not switched over to it yet, so the current version is still version X. The system is then reloaded (using the **reload** command), and it verifies that version Y is the current version running.

The following example shows that the software is rolled back to version X (using the **restore rollback** command), and the software is reloaded again:

```
WAE# copy ftp install server path waas.versionY.bin
```

```
WAE# show version
```

```
Cisco Wide Area Application Services Software (WAAS)
```

```
Copyright (c) 1999-2006 by Cisco Systems, Inc.
```

```
Cisco Wide Area Application Services Software Release 4.0.0 (build b340 Mar 25 2006)
```

```
Version: fe611-4.0.0.340
```

```
Compiled 17:26:17 Mar 25 2006 by cnbuild
```

```
System was restarted on Mon Mar 27 15:25:02 2006.
```

```
The system has been up for 3 days, 21 hours, 9 minutes, 17 seconds.
```

```
WAE# show version last
```

```
Nothing is displayed.
```

```
WAE# show version pending
```

```
WAAS 4.0.1 Version Y
```

```
WAE# reload
```

```
..... reloading .....
```

```
WAE# show version
Cisco Wide Area Application Services Software (WAAS)
...
WAE# restore rollback
WAE# reload
..... reloading .....
```

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.

Related Commands[reload](#)[show disks](#)[show running-config](#)[show startup-config](#)[show version](#)

rmdir

To delete a directory on a WAAS device, use the **rmdir** EXEC command.

rmdir *directory*

Syntax Description	<i>directory</i>	Name of the directory that you want to delete.
---------------------------	------------------	------------------------------------------------

Defaults	No default behavior or values
-----------------	-------------------------------

Command Modes	EXEC
----------------------	------

Device Modes	application-accelerator replication-accelerator central-manager
---------------------	-----------------------------------------------------------------------

Usage Guidelines	Use this EXEC command to remove any directory from the WAAS file system. The rmdir command only removes empty directories.
-------------------------	-----------------------------------------------------------------------------------------------------------------------------------

Examples	The following example shows how to delete the <i>oldfiles</i> directory from the <i>local1</i> directory: WAE# rmdir /local1/oldfiles
-----------------	-------------------------------------------------------------------------------------------------------------------------------------------------

Related Commands	cpfile dir lls ls mkdir pwd rename
-------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------

scp

To copy files between network hosts, use the **scp** command.

```
scp [1][2][4][6][B][C][p][q][r][v] [c cipher] [F config-file] [i id-file] [l limit]
    [o ssh_option] [P port] [S program] [[user @] host : file] [...] [[user-n @] host-n : file-n]
```

Syntax Description

1	(Optional) Forces this command to use protocol 1.
2	(Optional) Forces this command to use protocol 2.
4	(Optional) Forces this command to use only IPv4 addresses.
6	(Optional) Forces this command to use only IPv6 addresses.
B	(Optional) Specifies the batch mode. In this mode, the scp command does not ask for passwords or passphrases.
C	(Optional) Enables compression. The scp command passes this option to the ssh command to enable compression.
p	(Optional) Preserves the following information from the source file: modification times, access times, and modes.
q	(Optional) Disables the display of progress information.
r	(Optional) Recursively copies directories and their contents.
v	(Optional) Specifies the verbose mode. Causes the scp and ssh commands to print debugging messages about their progress. This option can be helpful when troubleshooting connection, authentication, and configuration problems.
c	(Optional) Specifies the cipher to use for encrypting the data being copied. The scp command directly passes this option to the ssh command.
<i>cipher</i>	The cipher to use for encrypting the data being copied.
F	(Optional) Specifies an alternative per-user configuration file for Secure Shell (SSH). The scp command directly passes this option to the ssh command.
<i>config-file</i>	Name of the configuration file.
i	(Optional) Specifies the file containing the private key for RSA authentication. The scp command directly passes this information to the ssh command.
<i>id-file</i>	The name of the file containing the private key for RSA authentication.
l	(Optional) Limits the use of bandwidth.
<i>limit</i>	The bandwidth to use for copying files in kbps.
o	(Optional) Passes options to the ssh command in the format used in <code>ssh_config5</code> .
<i>ssh_option</i>	See the ssh command for more information about the possible options.
P	(Optional) Specifies the port to connect to on the remote host.
<i>port</i>	The port to connect to on the remote host.
S	(Optional) Specifies the program to use for the encrypted connection.
<i>program</i>	Name of the program to use for the encrypted connection.
<i>user</i>	(Optional) Username.

<i>host</i>	(Optional) Hostname.
<i>file</i>	(Optional) Name of the file to copy.

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines The **scp** command uses SSH for transferring data between hosts.
This command prompts you for passwords or pass phrases when needed for authentication.

Related Commands [ssh](#)

script

To execute a script provided by Cisco or check the script for errors, use the **script EXEC** command.

```
script {check | execute} file_name
```

Syntax Description	check	execute
	Checks the validity of the script.	Executes the script. The script file must be a SYSFS file in the current directory.
	<i>file_name</i>	Name of the script file.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines The **script EXEC** command opens the script utility, which allows you to execute Cisco-supplied scripts or check errors in those scripts. The script utility can read standard terminal input from the user if the script you run requires input from the user.



Note The script utility is designed to run only Cisco-supplied scripts. You cannot execute script files that lack Cisco signatures or that have been corrupted or modified.

Examples The following example shows how to check for errors in the script file *test_script.pl*:

```
WAE# script check test_script.pl
```

setup

To configure basic configuration settings (general settings, device network settings, and disk configuration) on the WAAS device or to complete basic configuration after upgrading to WAAS software, use the **setup** EXEC command.

setup

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator
replication-accelerator
central-manager

Usage Guidelines

For instructions on using the **setup** command, see the *Cisco Wide Area Application Services Quick Configuration Guide*.

Examples

The following example shows the first screen of the wizard when you enter the **setup** EXEC command on a WAAS device that is running the WAAS software:

```
WAE# setup
Please choose an interface to configure from the following list:
1: GigabitEthernet 1/0
2: GigabitEthernet 2/0

Enter choice:
.
.
.
Press the ESC key at any time to quit this session
```

show aaa accounting

To display the AAA accounting configuration information for a WAAS device, use the **show aaa EXEC** command.

show aaa accounting

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator
replication-accelerator
central-manager

Usage Guidelines

Use this EXEC command to display configuration information for the following AAA accounting types:

- Exec shell
- Command (for normal users and superusers)
- System

Examples

[Table 3-1](#) describes the fields shown in the **show aaa accounting** display.

Table 3-1 Field Descriptions for the show aaa accounting Command

Field	Description
Accounting Type	Displays the AAA accounting configuration for the following types of user accounts: Exec Command level 0 Command level 15 System
Record Event(s)	Displays the configuration of the AAA accounting notice that is sent to the accounting server.
stop-only	The WAAS device sends a stop record accounting notice at the end of the specified activity or event to the TACACS+ accounting server.

Table 3-1 *Field Descriptions for the show aaa accounting Command (continued)*

Field	Description
start-stop	<p>The WAAS device sends a start record accounting notice at the beginning of an event and a stop record at the end of the event to the TACACS+ accounting server.</p> <p>The start accounting record is sent in the background. The requested user service begins regardless of whether or not the start accounting record was acknowledged by the TACACS+ accounting server.</p>
wait-start	<p>The WAAS device sends both a start and a stop accounting record to the TACACS+ accounting server. However, the requested user service does not begin until the start accounting record is acknowledged. A stop accounting record is also sent.</p>
disabled	<p>Accounting is disabled for the specified event.</p>
Protocol	<p>Displays the accounting protocol that is configured.</p>

Related Commands [\(config\) aaa accounting](#)

show adapter

To display the status and configuration of the EndPoint Mapper (EPM) adapter, use the **show adapter EXEC** command.

show adapter epm

Syntax Description	epm	Specifies the Microsoft PortMapper adapter.
---------------------------	------------	---------------------------------------------

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator

Usage Guidelines This command is valid for the WAE application-accelerator appliances; it is not valid for the Central Manager (CM) appliance.

Examples [Table 3-2](#) describes the fields shown in the **show adapter epm** display.

Table 3-2 *Field Description for the show adapter epm Command*

Field	Description
EPM (MS-PortMapper) adapter is enabled.	Configuration status of the EPM adapter.
EPM (MS-PortMapper) adapter is disabled.	

Related Commands [\(config\) adapter](#)
[show statistics epm](#)

show alarms

To display information on various types of alarms, their status, and history on a WAAS device, use the **show alarms EXEC** command.

```
show alarms [critical [detail [support]] | detail [support] | history [start_num [end_num [detail [support]]]] | critical [start_num [end_num [detail [support]]]] | detail [support] | major [start_num [end_num [detail [support]]]] | minor [start_num [end_num [detail [support]]]]] | detail [support] | major [detail [support]] | minor [detail [support]] | status]
```

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

EXEC

Device Modes

application-accelerator
 replication-accelerator
 central-manager

Usage Guidelines

The Node Health Manager in the WAAS software enables WAAS applications to raise alarms to draw attention in error/significant conditions. The Node Health Manager, which is the data repository for such alarms, aggregates the health and alarm information for the applications, services, and resources (for example, disk drives) that are being monitored on the WAAS device. For example, this feature gives you a mechanism to determine if a WAE is receiving overwhelming number of alarms. These alarms are referred to as “WAAS software alarms.”

The WAAS software uses SNMP to report error conditions by generating SNMP traps. The following WAAS applications can generate a WAAS software alarm:

- Node Health Manager (Alarm overload condition)
- System Monitor (sysmon) for disk failures

The three levels of alarms in WAAS software are as follows:

- **Critical**—Alarms that affect the existing traffic through the WAE, and are considered fatal (the WAE cannot recover and continue to process traffic).
- **Major**—Alarms which 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 which indicate that a condition that will not affect a service has occurred, but that corrective action is required to prevent a serious fault from occurring.

You can configure alarms using the **snmp-server enable traps alarms** global configuration command.

Use the **show alarms critical EXEC** command to display the current critical alarms being generated by WAAS software applications. Use the **show alarms critical detail EXEC** command to display additional details for each of the critical alarms being generated. Use the **show alarms critical detail support EXEC** command to display an explanation about the condition that triggered the alarm and how you can find out the cause of the problem. Similarly, you can use the **show alarms major** and **show alarms minor EXEC** commands to display the details of major and minor alarms.

Use the **show alarms history EXEC** command to display a history of alarms that have been raised and cleared by WAAS software on the WAAS device since the last software reload. The WAAS software retains the last 100 alarm raise and clear events only.

Use the **show alarms status EXEC** command to display the status of current alarms, and the WAAS device's alarm overload status and alarm overload configuration.

Examples

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

Table 3-3 Field Descriptions for the **show alarms history** Command

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. For example: wafs_edge_down, wafs_core_down.
Module/Submodule	Software module affected. For example: wafs.
Instance	Object that this alarm event is associated with. For example, for an alarm event with the Alarm ID disk_failed, the instance would be the name of the disk that failed. The Instance field does not have pre-defined values and is application specific.

Table 3-4 describes the fields shown in the **show alarms status** display.

Table 3-4 Field Descriptions for the **show alarms status** Command

Field	Description
Critical Alarms	Number of critical alarms.
Major Alarms	Number of major alarms.
Minor Alarms	Number of minor alarms.
Overall Alarm Status	Aggregate status of alarms.

Table 3-4 *Field Descriptions for the show alarms status Command (continued)*

Field	Description
Device is NOT in alarm overload state.	Status of the device alarm overload state.
Device enters alarm overload state @ 999 alarms/sec.	Threshold number of alarms per second at which the device enters the alarm overload state.
Device exits alarm overload state @ 99 alarms/sec.	Threshold number of alarms per second at which the device exits the alarm overload state.
Overload detection is ENABLED.	Status of whether overload detection is enabled on the device.

Related Commands[\(config\) alarm overload-detect](#)[\(config\) snmp-server enable traps](#)

show arp

To display the ARP table for a WAAS device, use the **show arp** EXEC command.

show arp

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Device Modes

- application-accelerator
- replication-accelerator
- central-manager

Usage Guidelines Use the **show arp** command to display the Internet-to-Ethernet address translation tables of the Address Resolution Protocol. Without flags, the current ARP entry for the host name is displayed.

Examples [Table 3-5](#) describes the fields shown in the **show arp** display.

Table 3-5 *Field Descriptions for the show arp Command*

Field	Description
Protocol	Type of protocol.
Address	IP address of the hostname.
Flags	Current ARP flag status.
Hardware Addr	Hardware IP address given as six hexadecimal bytes separated by colons.
Type	Type of wide-area network.
Interface	Name and slot/port information for the interface.

show authentication

To display the authentication configuration for a WAAS device, use the **show authentication EXEC** command.

show authentication {user | content-request}

Syntax Descriptions

user	Displays authentication configuration for user login to the system.
content-request	Displays content request authentication configuration information in the disconnected mode.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator
replication-accelerator
central-manager

Usage Guidelines

When the WAAS device authenticates a user through an NTLM, LDAP, TACACS+, RADIUS, or Windows domain server, a record of the authentication is stored locally. As long as the entry is stored, subsequent attempts to access restricted Internet content by the same user do not require additional server lookups. To display the local and remote authentication configuration for user login, use the **show authentication user EXEC** command.

To display the content request authentication configuration information in the disconnected mode, use the **show authentication content-request EXEC** command.

Examples

[Table 3-6](#) describes the fields shown in the **show authentication user** display.

Table 3-6 *Field Descriptions for the show authentication user Command*

Field	Description
Login Authentication: Console/Telnet/Ftp/SSH Session	Displays which authentication service is enabled for login authentication and the configured status of the service.
Windows domain	Operation status of the authentication service. Values are enabled or disabled.
RADIUS	
TACACS+	Priority status of each authentication service. Values are primary, secondary, or tertiary.
Local	

Table 3-6 *Field Descriptions for the show authentication user Command (continued)*

Field	Description
Configuration Authentication: Console/Telnet/Ftp/SSH Session	Displays which authentication service is enabled for configuration authentication and the configured status of the service.
Windows domain	Operation status of the authentication service. Values are enabled or disabled.
RADIUS	
TACACS+	Priority status of each authentication service. Values are primary, secondary, or tertiary.
Local	

Table 3-7 describes the field in the **show authentication content-request** display.

Table 3-7 *Field Description for the show authentication content-request Command*

Field	Description
The content request authentication in disconnected mode is XXX.	Operation status of content request authentication in disconnected mode. Values are enabled or disabled.

Related Commands

[\(config\) authentication](#)

[clear](#)

[show statistics authentication](#)

show auto-register

To display the status of a WAE's automatic registration feature, use the **show auto-register EXEC** command.

show auto-register

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator

Examples [Table 3-8](#) describes the output in the **show auto-register** display.

Table 3-8 *Field Description for the show auto-register Command*

Field	Description
Auto registration is enabled.	Configuration status of the autoregistration feature.
Auto registration is disabled.	

Related Commands [\(config\) auto-register](#)

show banner

To display the message of the day (MOTD), login, and EXEC banner settings, use the **show banner EXEC** command.

show banner

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Examples [Table 3-9](#) describes the fields shown in the **show banner** display.

Table 3-9 *Field Descriptions for the show banner Command*

Field	Description
Banner is enabled.	Configuration status of the banner feature.
MOTD banner is: abc	(Message of the day) 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 [\(config\) auto-register](#)

show bypass

To display static bypass configuration information for a WAE, use the **show bypass EXEC** command.

show bypass list

Syntax Description	list	Displays the bypass list entries. Maximum of 50.
---------------------------	-------------	--------------------------------------------------

Defaults	No default behavior or values
-----------------	-------------------------------

Command Modes	EXEC
----------------------	------

Device Modes	application-accelerator
---------------------	-------------------------

Usage Guidelines	The maximum number of static bypass entries is 50.
-------------------------	----------------------------------------------------

Examples	Table 3-10 describes the fields shown in the show bypass list display.
-----------------	-----------------------------------------------------------------------------------------------

Table 3-10 *Field Descriptions for the show bypass list Command*

Field	Description
Client	IP address and port of the client. For any client with this IP address, the WAE will not process the packet, but will bypass it and send it back to the router.
Server	IP address and port of the server.
Entry type	Type of bypass list entry. The Entry type field contains one of the following values: static-config, auth-traffic, server-error, or accept. A static-config entry is a bypass list entry that is user-configured. An auth-traffic entry is a type of dynamic entry that the internal software adds automatically when the server requests authentication.

Related Commands	(config) bypass
-------------------------	---------------------------------

show cdp

To display CDP configuration information, use the **show cdp** EXEC command.

```
show cdp [entry neighbor [protocol | version [protocol]] | holdtime | interface [FastEthernet
slot/port | GigabitEthernet slot/port] | neighbors [detail | FastEthernet slot/port [detail] |
```

```
GigabitEthernet slot/port [detail]] | run | timer | traffic]
```

Syntax Description

entry	(Optional) Displays information for a specific neighbor entry.
<i>neighbor</i>	Name of CDP neighbor entry.
protocol	(Optional) Displays the CDP protocol information.
version	(Optional) Displays the CDP version.
holdtime	(Optional) Displays length of time that CDP information is held by neighbors.
interface	(Optional) Displays interface status and configuration.
FastEthernet	(Optional) Displays Fast Ethernet configuration.
<i>slot/port</i>	Fast Ethernet slot (0–3) and port number.
GigabitEthernet	(Optional) Displays Gigabit Ethernet configuration.
<i>slot/port</i>	Gigabit Ethernet slot (1–2) and port number.
neighbors	(Optional) Displays CDP neighbor entries.
detail	(Optional) Displays detailed neighbor entry information.
FastEthernet	(Optional) Displays neighbor Fast Ethernet information.
<i>slot/port</i>	Neighbor Fast Ethernet slot (0–3) and port number.
detail	Displays detailed neighbor Fast Ethernet network information.
GigabitEthernet	(Optional) Displays neighbor Gigabit Ethernet information.
<i>slot/port</i>	Neighbor Gigabit Ethernet slot (1–2) and port number.
detail	(Optional) Displays detailed Gigabit Ethernet neighbor network information.
run	(Optional) Displays the CDP process status.
timer	(Optional) Displays the time when CDP information is resent to neighbors.
traffic	(Optional) Displays CDP statistical information.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator
 replication-accelerator
 central-manager

Usage Guidelines

The **show cdp** command displays information regarding how frequently CDP packets are resent to neighbors, the length of time that CDP packets are held by neighbors, the disabled status of CDP Version 2 multicast advertisements, CDP Ethernet interface ports, and general CDP traffic information.

Examples

Table 3-11 describes the fields shown in the **show cdp** display.

Table 3-11 Field Descriptions for the show cdp Command

Field	Description
Sending CDP packets every XX seconds	Interval (in seconds) between transmissions of CDP advertisements. This field is controlled by the cdp timer command.
Sending a holdtime value of XX seconds	Time (in seconds) that the device directs the neighbor to hold a CDP advertisement before discarding it. This field is controlled by the cdp holdtime command.
Sending CDPv2 advertisements is XX	Transmission status for sending CDP Version-2 type advertisements. Possible values are enabled or disabled.

Table 3-12 describes the fields shown in the **show cdp entry neighbor** display.

Table 3-12 Field Descriptions for the show cdp entry Command

Field	Description
Device ID	Name of the neighbor device and either the MAC address or the serial number of this device.
Entry address(es)	
IP address	IP address of the neighbor device.
CLNS address	Non-IP network address. Depends on type of neighbor.
DECnet address	Non-IP network address. Depends on type of neighbor.
Platform	Product name and number of the neighbor device.
Interface	Protocol being used by the connectivity media.
Port ID (outgoing port)	Port number of the port on the neighbor device.
Capabilities	Capability code discovered on the neighbor device. This is the type of the device listed in the CDP Neighbors table. Possible values are as follows: R—Router T—Transparent bridge B—Source-routing bridge S—Switch H—Host I—IGMP device r—Repeater

Table 3-12 Field Descriptions for the `show cdp entry` Command (continued)

Field	Description
Holdtime	Time (in seconds) that the current device will hold the CDP advertisement from a transmitting router before discarding it.
Version	Software version running on the neighbor device.

Table 3-13 describes the fields shown in the `show cdp entry neighbor protocol` display.

Table 3-13 Field Descriptions for the `show cdp entry protocol` Command

Field	Description
Protocol information for XX	Name or identifier of the neighbor device.
IP address	IP address of the neighbor device.
CLNS address	Non-IP network address. Depends on type of neighbor.
DECnet address	Non-IP network address. Depends on type of neighbor.

Table 3-14 describes the fields shown in the `show cdp entry neighbor version` display.

Table 3-14 Field Descriptions for the `show cdp entry version` Command

Field	Description
Version information for XX	Name or identifier of the neighbor device.
Software, Version	Software and version running on the neighbor device.
Copyright	Copyright information for the neighbor device.

Table 3-15 describes the field in the `show cdp holdtime` display.

Table 3-15 Field Descriptions for the `show cdp holdtime` Command

Field	Description
XX seconds	Time (in seconds) that the current device will hold the CDP advertisement from a transmitting router before discarding it.

Table 3-16 describes the fields shown in the `show cdp interface` display.

Table 3-16 Field Descriptions for the `show cdp interface` Command

Field	Description
Interface_slot/port is XX	Operation status of the CDP interface. Values are up or down.
CDP protocol is XX	Protocol being used by the connectivity media.

Table 3-17 describes the fields shown in the **show cdp neighbors** display.

Table 3-17 Field Descriptions for the **show cdp neighbors** Command

Field	Description
Device ID	Configured ID (name), MAC address, or serial number of the neighbor device.
Local Intfrfce	(Local Interface) Protocol being used by the connectivity media.
Holdtime	Time (in seconds) that the current device will hold the CDP advertisement from a transmitting router before discarding it.
Capability	Capability code discovered on the device. This is the type of the device listed in the CDP Neighbors table. Possible values are as follows: R—Router T—Transparent bridge B—Source-routing bridge S—Switch H—Host I—IGMP device r—Repeater
Platform	Product number of the device.
Port ID (outgoing port)	Port number of the device.

Table 3-18 describes the fields shown in the **show cdp neighbors detail** display.

Table 3-18 Field Descriptions for the **show cdp neighbors detail** Command

Field	Description
Device ID	Configured ID (name), MAC address, or serial number of the neighbor device.
Entry address (es)	List of network addresses of neighbor devices.
Platform	Product name and number of the neighbor device.
Capabilities	Device type of the neighbor. This device can be a router, a bridge, a transparent bridge, a source-routing bridge, a switch, a host, an IGMP device, or a repeater.
Interface	Protocol being used by the connectivity media.
Port ID (outgoing port)	Port number of the port on the neighbor device.
Holdtime	Time (in seconds) that the current device will hold the CDP advertisement from a transmitting router before discarding it.
Version	Software version running on the neighbor device.
Copyright	Copyright information for the neighbor device.
advertisement version	Version of CDP being used for CDP advertisements.

Table 3-18 *Field Descriptions for the show cdp neighbors detail Command (continued)*

Field	Description
VTP Management Domain	VLAN trunk protocol management domain. The VLAN information is distributed to all switches that are part of the same domain.
Native VLAN	VLAN to which the neighbor interface belongs.

Table 3-19 describes the field in the **show cdp run** display.

Table 3-19 *Field Description for the show cdp run Command*

Field	Description
CDP is XX.	Shows whether CDP is enabled or disabled.

Table 3-20 describes the field in the **show cdp timer** display.

Table 3-20 *Field Description for the show cdp timer Command*

Field	Description
cdp timer XX	Time when CDP information is resent to neighbors.

Table 3-21 describes the fields shown in the **show cdp traffic** display.

Table 3-21 *Field Descriptions for the show cdp traffic Command*

Field	Description
Total packets Output	(Total number of packets sent) Number of CDP advertisements sent by the local device. Note this value is the sum of the CDP Version 1 advertisements output and CDP Version 2 advertisements output fields.
Input	(Total number of packets received) Number of CDP advertisements received by the local device. Note this value is the sum of the CDP Version-1 advertisements input and CDP Version 2 advertisements input fields.
Hdr syntax	(Header Syntax) Number of CDP advertisements with bad headers, received by the local device.
Chksum error	(Checksum Error) Number of times the checksum (verifying) operation failed on incoming CDP advertisements.
Encaps failed	(Encapsulations Failed) Number of times CDP failed to transmit advertisements on an interface because of a failure caused by the bridge port of the local device.
No memory	Number of times the local device did not have enough memory to store the CDP advertisements in the advertisement cache table when the device was attempting to assemble advertisement packets for transmission and parse them when receiving them.
Invalid packet	Number of invalid CDP advertisements received and sent by the local device.
Fragmented	Number of times fragments or portions of a single CDP advertisement were received by the local device instead of the complete advertisement.

Table 3-21 Field Descriptions for the *show cdp traffic* Command (continued)

Field	Description
CDP version 1 advertisements Output	Number of CDP Version 1 advertisements sent by the local device.
Input	Number of CDP Version 1 advertisements received by the local device.
CDP version 2 advertisements Output	Number of CDP Version 2 advertisements sent by the local device.
Input	Number of CDP Version 2 advertisements received by the local device.

Related Commands[\(config\) cdp](#)[\(config-if\) cdp](#)[clear](#)

show cifs

To display CIFS run-time information, use the **show cifs** EXEC command.

```
show cifs {auto-discovery [enabled | host-db | last] | cache {disk-use | entry-count} |
connectivity peers | mss | requests {count | waiting} | sessions {count | list}}
```

Syntax Description

auto-discovery	CIFS auto-discovery status and run-time data.
enabled	Displays current state of CIFS auto-discovery.
host-db	Displays currently known hosts.
last	Displays last auto-discovered entries.
cache	Displays CIFS cache information.
disk-use	Displays total disk usage for CIFS cache.
entry-count	Count of cached file and directory entries.
connectivity	Displays Run-time information on Edge-Core connectivity.
peers	Displays list of connected Cores.
mss	Displays the TCP maximum segment size (MSS) for CIFS adapter. The segment size range is 512–1460.
requests	Displays run-time information on active CIFS requests.
count	Number of pending CIFS requests.
waiting	Number of waiting CIFS requests.
sessions	Displays run-time information on active CIFS sessions.
count	Connected session count.
list	List of connected CIFS sessions.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

Use the **show cifs cache** command to view information about caching efficiency. You might use this command to determine if the cache contains sufficient space or if more space is needed. If you have a performance issue, you might use this command to see whether or not the cache is full.

Use the **show cifs connectivity peers** command to validate the WAN link state and the Edge to Core connectivity. This command is useful for general monitoring and debugging.

Use the **show cifs requests count** or **show cifs requests waiting** command to monitor the load for CIFS traffic. You might also use this command for debugging purposes to isolate requests that are not processing.

Use the **show cifs sessions count** or **show cifs sessions list** command to view session information. You might use this command to monitor connected users during peak and off-peak hours.

Related Commands [cifs](#)

show clock

To display information about the system clock on a WAAS device, use the **show clock** EXEC command.

```
show clock [detail | standard-timezones { all | details timezone | regions | zones region-name }]
```

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

Defaults No default behavior or values

Command Modes EXEC

Device Modes

- application-accelerator
- replication-accelerator
- central-manager

Usage Guidelines The WAAS device has several predefined “standard” time zones. Some of these time zones have built-in summer time information while others do not. For example, if you are in an eastern region of the United States (US), you must use US/Eastern time zone that includes summer time information for the system clock to adjust automatically every April and October. There are about 1500 “standard” time zone names.

Strict checking disables the **clock summertime** command when a standard time zone is configured. You can only configure summertime if the time zone is not a standard time zone (that is, if the time zone is a “customized zone”).

The **show clock standard-timezones all** EXEC command enables you to browse through all standard timezones and choose from these predefined time zones. This enables you to 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. To display all first level time zone names organized into directories by region, use the **show clock standard-timezones region** EXEC command.

The **show clock** command displays the local date and time information and the **show clock detail** command shows optional detailed date and time information.

Examples

Table 3-22 describes the field in the **show clock** display.

Table 3-22 *Field Description for the show clock Command*

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 3-23 describes the fields shown in the **show clock detail** display.

Table 3-23 *Field Descriptions for the show clock detail Command*

Field	Description
Local time	Local time relative to UTC.
UTC time	Universal time clock date and time.
Epoch	Number of seconds since Jan. 1, 1970.
UTC offset	UTC offset in seconds, hours, and minutes.

Related Commands

[clock](#)

[\(config\) clock](#)

show cms

To display Centralized Management System (CMS) embedded database content and maintenance status and other information for a WAAS device, use the **show cms** EXEC command.

```
show cms {database content {dump filename | text | xml} | info | processes}
```

Syntax Description	Parameter	Description
	database	Displays embedded database maintenance information.
	content	Writes the database content to a file.
	dump	Dumps all database content to a text file.
	<i>filename</i>	Name of the file to be saved under local1 directory.
	text	Writes the database content to a file in text format.
	xml	Writes the database content to a file in XML format.
	info	Displays CMS application information.
	processes	Displays CMS application processes.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Examples [Table 3-24](#) describes the fields shown in the **show cms info** display for WAAS application engines.

Table 3-24 *Field Descriptions for the show cms info Command for WAAS Application Engines*

Field	Description
Device registration information	
Device Id	Unique identifier given to the device by the Central Manager at registration, which is used to manage the device.
Device registered as	Type of device used during registration: WAAS Application Engine or WAAS Central Manager.
Current WAAS Central Manager	Address of the Central Manager as currently configured in the central-manager address global configuration command. This address may differ from the registered address if a standby Central Manager is managing the device instead of the primary Central Manager with which the device is registered.

Table 3-24 *Field Descriptions for the show cms info Command for WAAS Application Engines (continued)*

Field	Description
Registered with WAAS Central Manager	Address of the Central Manager with which the device is registered.
Status	Connection status of the device to the Central Manager. This field may contain one of 3 values: online, offline, or pending.
Time of last config-sync	Time when the device management service last contacted the Central Manager for updates.
CMS services information	
Service cms_ce is running	Status of the WAE device management service (running or not running). This field is specific to the WAE only.

Table 3-25 describes the fields shown in the **show cms info** display for WAAS Central Managers.

Table 3-25 *Field Descriptions for the show cms info Command for WAAS Central Managers*

Field	Description
Device registration information	
Device Id	Unique identifier given to the device by the Central Manager at registration, which is used to manage the device.
Device registered as	Type of device used during registration: WAAS Application Engine or WAAS Central Manager.
Current WAAS Central Manager role	Role of the current Central Manager: Primary or Standby. Note The output for primary and standby Central Manager devices is different. On a standby, the output includes the following additional information: Current WAAS Central Manager and Registered with WAAS Central Manager.
Current WAAS Central Manager	Address of the standby Central Manager as currently configured in the central-manager address global configuration command.
Registered with WAAS Central Manager	Address of the standby Central Manager with which the device is registered.
CMS services information	
Service cms_httpd is running	Status of the management service (running or not running). This field is specific to the Central Manager only.
Service cms_cdm is running	Status of the management service (running or not running). This field is specific to the Central Manager only.

Table 3-26 describes the field in the **show cms database content text** display.

Table 3-26 *Field Description for the show cms database content text Command*

Field	Description
Database content can be found in /local1/cms-db-12-12-2002-17:06:08:070.txt.	Name and location of the database content text file. This command requests the management service to write its current configuration to an automatically generated file in text format.

Table 3-27 describes the field in the **show cms database content xml** display.

Table 3-27 *Field Description for the show cms database content xml Command*

Field	Description
Database content can be found in /local1/cms-db-12-12-2002-17:07:11:629.xml.	Name and location of the database content XML file. This command requests the management service to write its current configuration to an automatically generated file in XML format.

Related Commands

[cms](#)
[\(config\) cms](#)

show cms secure-store

To display secure disk encryption status, use the **show cms secure-store** EXEC command.

show cms secure-store

Syntax Description This command has no keywords or arguments.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Examples The following example, shows that secure disk encryption is fully operational (both initialized and open):

```
WAE# show cms secure-store
secure-store initialized and open
```

The command will display one of the following status messages:

secure-store not initialized	Secure disk encryption is not initialized.
secure-store initialized. use secure-store open command to open	Secure disk encryption is initialized but not open.
secure-store initialized and open	Secure disk encryption is initialized and open.

Related Commands [cms secure-store](#)

show debugging

To display the state of each debugging option that was previously enabled on a WAAS device, use the **show debugging EXEC** command.

show debugging

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Device Modes application-accelerator
 replication-accelerator
 central-manager

Usage Guidelines This command shows which debug options have been enabled or disabled. If there are no debug options configured, this command shows no output.

The **dre**, **epm**, **flow**, **print-spooler**, **rbcp**, **tfo**, **translog**, **wafs**, and **wccp** command options are supported in the application-accelerator device mode only. The **emdb** and **rpc** command options are supported in the central manager device mode only.

This command displays only the type of debugging enabled, not the specific subset of the command.

Examples The following example shows that the **debug tfo buffer-mgr** and the **debug tfo connection** commands coupled with the **show debugging** command display the states of **tfo buffer-mgr** and **tfo connection** debugging options:

```
WAE# debug tfo buffer-mgr
WAE# debug tfo connection
WAE# show debugging
tfo bufmgr debugging is on
tfo compmgr debugging is on
tfo connmgr debugging is on
tfo netio debugging is on
tfo statmgr debugging is on
tfo translog debugging is on
```

Related Commands [debug](#)
[undebug](#)

show device-mode

To display the configured or current device mode of a WAAS device, use the **show device-mode EXEC** command.

```
show device-mode {configured | current}
```

Syntax Description

configured	Displays the configured device mode, which has not taken effect yet.
current	Displays the current device mode.

Command Modes

EXEC

Device Modes

application-accelerator
 replication-accelerator
 central-manager

Usage Guidelines

You must deploy the WAAS Central Manager on a dedicated appliance. The device mode feature allows you to deploy a WAAS device as either a WAAS Central Manager or a WAE. Because you must deploy a WAAS Central Manager on a dedicated appliance, a WAAS device can only operate in one device mode; either in central-manager mode or application-accelerator mode.

If the configured and current device modes differ, a reload is required for the configured device mode to take effect.

To display the current device mode of a WAAS device, enter the **show device mode EXEC** command:

```
WAE# show device-mode
```

To display the current mode in which the WAAS device is operating, enter the **show device-mode current EXEC** command:

```
WAE# show device-mode current
Current device mode: application-accelerator
```

To display the configured device mode that has not yet taken effect, enter the **show device-mode configured EXEC** command. For example, if you had entered the **device mode central-manager** global configuration command on a WAAS device to change its device mode to central manager but have not yet entered the **copy run start EXEC** command to save the running configuration on the device, then if you were to enter the **show device-mode configured** command on the WAAS device, the command output would indicate that the configured device mode is central-manager:

```
WAE# show device-mode configured
Configured device mode: central-manager
```

Examples

[Table 3-28](#) describes the field in the **show device-mode current** display.

Table 3-28 *Field Description for the show device-mode current Command*

Field	Description
Current device mode	Current mode in which the WAAS device is operating.

[Table 3-29](#) describes the field in the **show device-mode configured** display.

Table 3-29 *Field Description for the show device-mode configured Command*

Field	Description
Configured device mode	Device mode that has been configured, but has not yet taken effect.

Related Commands

[\(config\) device mode](#)

show disks

To view information about the WAAS device disks, use the **show disks** EXEC command.

```
show disks { details | failed-disk-id | failed-sectors [disk_name] | tech-support [details]}
```

Syntax Description		
details		Displays currently effective configurations with more details.
failed-disk-id		Displays a list of disk serial numbers that have been identified as failed. Note This option is not available on WAE-7341 and WAE-7371 models.
failed-sectors		Displays a list of failed sectors on all the disks.
<i>disk_name</i>		(Optional) Name of the disk for which failed sectors are displayed (disk00 or disk01).
tech-support		Displays hard drive diagnostic information and information about impending disk failures. Displays all available information from the RAID controller, including disk status (logical and physical), disk vendor ID, and serial numbers. This command replaces the show disk smart-info EXEC command.
details		(Optional) Displays more detailed SMART disk monitoring information.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines The **show disks details** EXEC command displays the percentage or amount of disk space allocated to each file system, and the operational status of the disk drives, after reboot.

The WAAS software supports filtering of multiple syslog messages for a single, failed section on IDE, SCSI, and SATA disks. Enter the **show disks failed-sectors** EXEC command to display a list of failed sectors on all disk drives.

```
WAE# show disks failed-sectors
disk00
=====
89923
9232112

disk01
=====
(None)
```

To display a list of failed sectors for only a specific disk drive, specify the name of the disk when entering the **show disks failed-sectors** command. The following example shows how to display a list of failed sectors for disk01:

```
WAE# show disks failed-sectors disk01
disk01
=====
(None)
```

If there are disk failures, a message is displayed, notifying you about this situation when you log in.

Proactively Monitoring Disk Health with SMART

The ability to proactively monitor the health of disks is available using SMART. 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 how healthy a disk is. SMART attributes include several read-only attributes (for example, the power on hours attribute, the load and unload count attribute) that provide the WAAS software with information regarding the operating and environmental conditions that may indicate an impending disk failure.

SMART support is vendor and drive technology (IDE or SCSI disk drives) dependent. Each disk vendor has a different set of supported SMART attributes.

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 to have “failed.” The WAAS software monitors the SMART attributes and reports any impending failure through syslog messages, SNMP traps, and alarms.

To display SMART information, use the **show disks tech-support** EXEC command. To display more detailed SMART information, enter the **show disks tech-support details** EXEC command. The output from the **show tech-support** EXEC command also includes SMART information.

Examples

[Table 3-30](#) describes the fields shown in the **show disks failed-disk-id** display.

Table 3-30 Field Description for the **show disks failed-disk-id** Command

Field	Description
Diskxx	Number and location of the physical disk.
<i>Alpha-numeric string</i>	Serial number of the disk.

[Table 3-31](#) describes the fields shown in the **show disks details** display.

Table 3-31 Field Descriptions for the show disks details Command

Field	Description
Physical disk information	Lists the disks by number. WAE 7300 series appliances show information for 6 disk drives and WAE 500 and 600 series appliances show information for 2 disk drives.
disk00	Availability of the disk: Present, Not present or Not responding, or Not used (*). Disk identification number and type, for example: (h00 c00i00 100 - DAS). Disk size in megabytes and gigabytes, for example: 140011MB (136.7GB).
disk01	Same type of information is shown for each disk.
Mounted filesystems	Table containing the following column heads:
Mount point	Mount point for the file system. For example, the mount point for SYSFS is /local/local1.
Type	Type of the file system. Values include root, internal, CONTENT, SYSFS, and PRINTSPOOL.
Device	Path to the partition on the disk.
Size	Total size of the file system in megabytes.
Inuse	Amount of disk space being used by the file system.
Free	Amount of unused disk space for the file system.
Use%	Percentage of the total available disk space being used by the file system.
Software RAID devices	If present, lists the software RAID devices and provides the following information for each:
Device name	Path to the partition on the disk. The partition name “md1” indicates that the partition is a RAIDed partition and that the RAID type is RAID-1.
Type	Type of RAID, for example RAID-1.
Status	Operational status of the RAID device. Status may contain NORMAL OPERATION or REBUILDING.
Physical devices and status	Disk number and operational status of the disk, such as [GOOD] or [BAD].

In the following example, the output shows that partition 04 and partition 05 on disks disk00 and disk01 are GOOD, and the RAIDed partitions /dev/md4 & /dev/md5 are in NORMAL OPERATION. However, the RAIDed partition /dev/md8 has an issue with one of the drives. Disk04 with partition 00 is GOOD, but the status shows ONE OR MORE DRIVES ABNORMAL because there is no pair on this partition.

```
/dev/md4      RAID-1    NORMAL OPERATION    disk00/04 [GOOD]
disk01/04 [GOOD]
/dev/md5      RAID-1    NORMAL OPERATION    disk00/05 [GOOD]
disk01/05 [GOOD]
...
/dev/md8      RAID-1    ONE OR MORE DRIVES ABNORMAL  disk04/00 [GOOD]
```

Table 3-32 describes some typical fields in the **show disks tech-support** display for a RAID-1 appliance that supports SMART. SMART attributes are vendor dependent; each disk vendor has a different set of supported SMART attributes.

Table 3-32 Field Descriptions for the **show disks tech-support** Command

Field	Description
disk00—disk05	WAE 7300 series appliances show information for 6 disk drives, and WAE 500 and 600 series appliances show information for 2 disk drives.
Device	Vendor number and version number of the disk.
Serial Number	Serial number for the disk.
Device type	Type of device is disk.
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. For example, Mon Mar 19 23:33:12 2007 UTC.
Device supports SMART and is Enabled	Status of SMART support: Enabled or Disabled.
Temperature Warning Enabled	Temperature warning status: Enabled or Disabled.
SMART Health Status:	Health status of the disk: OK or Failed.

Table 3-33 describes the fields in the **show disks tech-support details** display for a RAID-1 appliance that supports SMART. Details in this display depend on the drive manufacturer and vary between drives.

Table 3-33 Field Descriptions for the **show disks tech-support details** Command

Field	Description
disk00—disk05	WAE 7300 series appliances show information for 6 disk drives and WAE 500 and 600 series appliances show information for 2 disk drives.
Device	Vendor number and version number of the disk.
Serial Number	Serial number for the disk.
Device type	Type of device is disk.
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. For example, Mon Mar 19 23:33:12 2007 UTC.
Device supports SMART and is Enabled	Status of SMART support: Enabled or Disabled.
Temperature Warning Enabled	Temperature warning status: Enabled or Disabled.
SMART Health Status:	Health status of the disk: OK or Failed.
Current Drive Temperature	Temperature of the drive in degrees Celsius.
Manufactured in week XX of year	Manufacturing details.

Table 3-33 Field Descriptions for the `show disks tech-support details` Command (continued)

Field	Description
Current start stop count	Number of times the device has stopped or started.
Recommended maximum start stop count	Maximum recommended count used to gauge the life expectancy of the disk.
Error counter log	Table displaying the error counter log. Counters for various types of disk errors.

Table 3-34 describes the fields shown in the `show disks tech-support` display for a RAID-5 appliance.

Table 3-34 Field Descriptions for the `show disks tech-support` Command

Field	Description
Controllers found	Number of RAID controllers found.
Controller information	
Controller Status	Functional status of the controller.
Channel description	Description of the channel transport protocols.
Controller Model	Make and model of the controller.
Controller Serial Number	Serial number of the ServeRAID controller
Physical Slot	Slot number.
Installed memory	Amount of memory for the disk.
Copyback	Status of whether copyback is enabled or disabled.
Data scrubbing	Status of whether data scrubbing is enabled or disabled.
Defunct disk drive count	Number of defunct disk drives.
Logical drives/Offline/Critical	Number of logical drives, number of drives that are offline, and number of critical alarms.
Controller Version Information	
BIOS	Version number of the BIOS.
Firmware	Version number of the Firmware.
Driver	Version number of the Driver.
Boot Flash	Version number of the Boot Flash.
Controller Battery Information	
Status	Functional status of the controller battery.
Over temperature	Over temperature condition of the battery.
Capacity remaining	Percent of remaining battery capacity.
Time remaining (at current draw)	Number of days, hours, and minutes of battery life remaining based on the current draw.
Controller Vital Product Data	
VPD Assigned#	Number assigned to the controller vital product data (VPD).
EC Version#	Version number.

Table 3-34 Field Descriptions for the show disks tech-support Command (continued)

Field	Description
Controller FRU#	Number assigned to the controller field-replaceable part.
Battery FRU#	Number assigned to the battery field-replaceable part.
Logical drive information	
Logical drive number	Number identifying the logical drive to which the information applies.
Logical drive name	Name of the logical drive.
RAID level	RAID level of the logical drive.
Status of logical drive	Functional status of the logical drive.
Size	Size (in megabytes) of the logical drive.
Read-cache mode	Configuration status of read-cache mode: Enabled or Disabled.
Write-cache mode	Configuration status of write-cache mode for write-back: Enabled or Disabled.
Write-cache setting	Configuration status of the write-cache setting for write-back: Enabled or Disabled.
Partitioned	Partition state. Values are Yes or No.
Number of chunks	Number of disks participating in the RAID-5 array.
Stripe-unit size	Amount of data storage per stripe unit. The default is 256 KB per disk in the logical array. This parameter is not configurable.
Stripe order (Channel,Device)	Order in which data is striped across a group of physical drives that are grouped in a RAID array.
Bad stripes	Flag for bad stripes. Flag values are Yes or No.
Physical drive information	
Device #	Device number for which the information applies.
Device is a xxxx	Type of device.
State	State of the device: Online or Offline.
Supported	Status showing if the device is supported.
Transfer Speed	Device transfer speed.
Reported Channel,Device	Provides channel information for all the disks participating in the RAID-5 array.
Reported Enclosure,Slot	Device number and slot number.
Vendor	Vendor identification number.
Model	Model number.
Firmware	Firmware number.
Serial number	Serial number.
Size	Size (in megabytes) of the physical drive.
Write Cache	Status of whether the write cache is enabled.

Table 3-34 *Field Descriptions for the show disks tech-support Command (continued)*

Field	Description
FRU	Field Replaceable Unit number. A RAID defunct drive FRU event occurs when a specified hard disk drive with the provided FRU number fails in a RAID configuration. The default value for this field is NONE.
PFA	Predictive Failure Analysis flag. The flag default value is No. If the RAID predicts a drive failure, this field is set to Yes and a critical alarm is raised on the WAE.

Related Commands

[disk](#)
[\(config\) disk error-handling](#)
[show tech-support](#)

show egress-methods

To view the egress method that is configured and that is being used on a particular WAE, use the **show egress-methods EXEC** command.

```
show egress-methods
```

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Device Modes application-accelerator

Examples [Table 3-35](#) describes the fields shown in the **show egress-methods** display.

Table 3-35 *Field Descriptions for the show egress-methods Command*

Field	Description
Intercept method	Intercept method used by router to send packets to the WAE.
TCP Promiscuous 61 or 62	WCCP service number.
WCCP negotiated return method	WCCP return method being used by the router. Values include WCCP_GRE, WCCP_L2, NEG_RTN_PENDING (negotiation is pending), and UNKNOWN.
Destination	This value is not configurable. The value of this field is always ANY.
Egress Method Configured	Egress method configured in the CLI.
Egress Method Used	Egress method being used.

Related Commands [show tfo egress-methods connection](#)
[\(config\) egress-method](#)

show flash

To display the flash memory version and usage information for a WAAS device, use the **show flash EXEC** command.

show flash

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Examples [Table 3-36](#) describes the fields shown in the **show flash** display.

Table 3-36 Field Descriptions for the show flash Command

Field	Description
WAAS software version (disk-based code)	WAAS software version and build number that is running on the device.
System image on flash:	
Version	Version and build number of the software that is stored in flash memory.
System flash directory:	
System image	Number of sectors used by the system image.
Bootloader, rescue image, and other reserved areas	Number of sectors used by the bootloader, rescue image, and other reserved areas.
XX sectors total, XX sectors free	Total number of sectors. Number of free sectors.

show hardware

To display system hardware status for a WAAS device, use the **show hardware** EXEC command.

show hardware

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines The **show hardware** command lists the system hardware status, including the version number, the startup date and time, the run time since startup, the microprocessor type and speed, the amount of physical memory available, and a list of disk drives.

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

Table 3-37 Field Descriptions for the show hardware Command

Field	Description
Cisco Wide Area Application Services Software (WAAS) Copyright (c) year by Cisco Systems, Inc. Cisco Wide Area Application Services Software Release XXX (build bXXX month day year)	Software application, copyright, release, and build information.
Version	Version number of the software that is running on the device.
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.

Table 3-37 Field Descriptions for the show hardware Command (continued)

Field	Description
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 GigabitEthernet interfaces	Number of Gigabit Ethernet interfaces on the device.
X InlineGroup interfaces	Number of InlineGroup interfaces on the device.
X Console interface	Number of console interfaces on the device.
Manufactured As	Product identification information.
BIOS Information	Information about the BIOS.
Vendor	Name of the BIOS vendor.
Version	BIOS version number.
Rel. Date	(Release date) Date that the BIOS was released.
Cookie info	
SerialNumber	Serial number of the WAE.
SerialNumber (raw)	Serial number of the WAE as an ASCII value.
TestDate	Date that the WAE was tested.
ExtModel	Hardware model of the device, for example: WAE612.
ModelNum (raw)	Internal model number (ASCII value) that corresponds to the ExtModel number.
HWVersion	Number of the current hardware version.
PartNumber	Not implemented.
BoardRevision	Number of revisions for the current system board.
ChipRev	Number of revisions for the current chipset.
VendID	Vendor ID of the cookie.
CookieVer	Version number of the cookie.
Chksum	Checksum of the cookie. showing whether the cookie is valid.
List of all disk drives	
Physical disk information	Disks listed by number. WAE 7300 series appliances show information for 6 disk drives and WAE 500 and 600 series appliances show information for 2 disk drives.
disk00	Availability of the disk: Present, Not present or not responding, or Not used (*). Disk identification number and type, for example:(h00 c00i00 100 - DAS). Disk size in megabytes and gigabytes, for example: 140011MB (136.7GB).
disk01	Same type of information is shown for each disk.
Mounted filesystems	Table containing the following column heads:

Table 3-37 Field Descriptions for the show hardware Command (continued)

Field	Description
Mount point	Mount point for the file system. For example the mount point for SYSFS is /local/local1.
Type	Type of the file system. Values include root, internal, CONTENT, SYSFS, and PRINTSPOOL.
Device	Path to the partition on the disk.
Size	Total size of the file system in megabytes.
Inuse	Amount of disk space being used by the file system.
Free	Amount of unused disk space for the file system.
Use%	Percentage of the total available disk space being used by the file system.
Software RAID devices	If present, lists the software RAID devices and provides the following information for each:
Device name	Path to the partition on the disk. The partition name “md1” indicates that the partition is a RAIDed partition and that the RAID type is RAID-1. (RAID-1 is the only RAID type supported in WAAS.)
Type	Type of RAID, for example RAID-1.
Status	Operational status of the RAID device. Status may contain NORMAL OPERATION or REBUILDING.
Physical devices and status	Disk number and operational status of the disk, such as [GOOD] or [BAD].

Related Commands[show disks](#)[show version](#)

show hosts

To view the hosts on a WAAS device, use the **show hosts** EXEC command.

show hosts

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines The **show hosts** command lists the name servers and their corresponding IP addresses. It also lists the host names, their corresponding IP addresses, and their corresponding aliases (if applicable) in a host table summary.

Examples [Table 3-38](#) describes the fields shown in the **show hosts** display.

Table 3-38 *field Descriptions for the show hosts Command*

Field	Description
Domain names	Domain names used by the WAE to resolve the IP address.
Name Server(s)	IP address of the DNS name server or servers.
Host Table	
hostname	FQDN (hostname and domain) of the current device.
inet address	IP address of the current host device.
aliases	Name configured for the current device based on the host global configuration command.

show inetd

To display the status of TCP/IP services on a WAAS device, use the **show inetd** EXEC command.

show inetd

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines The **show inetd** EXEC command displays the enabled or disabled status of TCP/IP services on the WAAS device. You can ignore the TFTP service status because TFTP is not supported on WAAS.

Examples [Table 3-39](#) describes the fields shown in the **show inetd** display.

Table 3-39 *Field Descriptions for the show inetd Command*

Field	Description
Inetd service configurations:	
ftp	Status of whether the FTP service is enabled or disabled.
rcp	Status of whether the RCP service is enabled or disabled.
tftp	Status of whether the TFTP service is enabled or disabled.

Related Commands [\(config\) inetd enable](#)

show interface

To display the hardware interface information for a WAAS device, use the **show interface** EXEC command.

```
show interface { GigabitEthernet slot/port } | { ide control_num } | { InlineGroup slot/grpnumber }
| { InlinePort slot/grpnumber/{ lan | wan } } | { PortChannel port-num } | { scsi device_num }
| { Standby group_num | usb }
```

Syntax Description		
GigabitEthernet		Displays the Gigabit Ethernet interface device information (only on suitably equipped systems).
<i>slot/port</i>		Slot and port number for the Gigabit Ethernet interface. The slot range is 0–3; the port range is 0–3. The slot number and port number are separated with a forward slash character (/).
ide		Displays the IDE interface device information.
<i>control_num</i>		IDE controller number (0–1).
InlineGroup		Displays the inline group information.
<i>slot/grpnumber</i>		Slot and inline group number for the selected interface.
InlinePort		Displays the inline port information.
<i>slot/grpnumber/</i>		Slot and inline group number for the selected interface.
lan		Displays the inline port information for the LAN port.
wan		Displays the inline port information for the WAN port.
PortChannel		Displays the port channel interface device information.
<i>port-num</i>		Port number for the port channel interface (1–2).
scsi		Displays the SCSI interface device information.
<i>device_num</i>		SCSI device number (0–7).
Standby		Displays the standby group information.
<i>group_num</i>		Standby group number (1–4).
usb		Displays the USB interface device information.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator
 replication-accelerator
 central-manager

Examples

Table 3-40 describes the fields shown in the **show interface GigabitEthernet** display.

Table 3-40 Field Descriptions for the show interface GigabitEthernet Command

Field	Description
Description	Description of the device, as configured by using the description option of the interface global configuration command.
Type	Type of interface. Always Ethernet.
Ethernet address	Layer-2 MAC address.
Internet address	Internet IP address configured for this interface.
Broadcast address	Broadcast address configured for this interface.
Netmask	Netmask configured for this interface.
Maximum Transfer Unit Size	Current configured MTU value.
Metric	Metric setting for the interface. The default is 1. The routing metric is used by the routing protocol 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 packet interrupts at this interface.
Base address	Base address. hexadecimal value.
Flags	Interface status indicators. Values include Up, Broadcast, Running, and Multicast.
Mode	Speed setting, transmission mode, and transmission speed for this interface.

The following example displays information for inlineGroup 0 in slot 1 configured on the WAE inline network adapter:

```
WAE612# show interface inlineGroup 1/0
Interface is in intercept operating mode.
Standard NIC mode is off.
Disable bypass mode is off.
VLAN IDs configured for inline interception: All
Watchdog timer is enabled.
Timer frequency: 1600 ms.
Autoreset frequency 500 ms.
The watchdog timer will expire in 1221 ms.
```

Table 3-41 describes the fields shown in the **show interface InlinePort** display.

Table 3-41 Field Descriptions for the show interface InlinePort Command

Field	Description
Device name	Number identifier for this inlineport interface, such as eth0, eth1, and so forth.
Packets Received	Total number of packets received on this inlineport interface.
Packets Intercepted	Total number of packets intercepted. (Only TCP packets are intercepted.)
Packets Bridged	Number of packets that are bridged. Packets which are not intercepted are bridged.
Packets Forwarded	Number of packets sent from the inline interface.
Packets Dropped	Number of packets dropped.
Packets Received on native	Number of packets forwarded by the inline module that are received on the native (GigabitEthernet 1/0) interface.
<i>n</i> flows through this interface	Number of active TCP connections on this inlineport interface.
Ethernet Driver Status	
Type	Type of interface. Always Ethernet.
Ethernet address	Layer-2 MAC address.
Maximum Transfer Unit Size	Current configured MTU value.
Metric	Metric setting for the interface. The default is 1. The routing metric is used by the routing protocol to determine the most favorable route. Metrics are counted as additional hops to the destination network or host; the higher the metric value, the less favorable the route.
Packets Received	Total number of packets received by this interface.
Input Errors	Number of incoming errors on this interface.
Input Packets Dropped	Number of incoming packets that were dropped on this interface.
Input Packets Overruns	Number of incoming packet overrun errors.
Input Packets Frames	Number of incoming packet frame errors.
Packet Sent	Total number of packets sent from this interface.
Output Errors	Number of outgoing packet errors.

Table 3-41 Field Descriptions for the show interface InlinePort Command (continued)

Field	Description
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.
Base address	Base address. hexadecimal value.
Flags	Interface status indicators. Values include Up, Broadcast, Running, and Multicast.
Mode	Speed setting, transmission mode, and transmission speed for this interface.

Table 3-42 describes the fields shown in the **show interface PortChannel** display.

Table 3-42 Field descriptions for the show interface PortChannel Command

Field	Description
Type	Type of interface. Always Ethernet.
Ethernet address	Layer-2 MAC address.
Maximum Transfer Unit Size	Current configured MTU value.
Metric	Metric setting for the interface. The default is 1. The routing metric is used by the routing protocol. Higher metrics have the effect of making a route less favorable; metrics are counted as addition hops to the destination network or host.
Packets Received	Total number of packets received by this interface.
Input Errors	Number of incoming errors on this interface.
Input Packets Dropped	Number of incoming packets that were dropped on this interface.
Input Packets Overruns	Number of incoming packet overrun errors.
Input Packets Frames	Number of incoming packet frame errors.
Packet Sent	Total number of packets sent from this interface.
Output Errors	Number of outgoing packet errors.
Output Packets Dropped	Number of outgoing packets that were dropped by this interface.
Output Packets Overruns	Number of outgoing packet overrun errors.
Output Packets Carrier	Number of outgoing packet carrier errors.
Output Queue Length	Output queue length in bytes.
Collisions	Number of packet collisions at this interface.
Flags	Interface status indicators. Values include Up, Broadcast, Running, and Multicast.

Table 3-43 describes the field shown in the **show interface scsi** display.

Table 3-43 *Field Description for the show interface scsi Command*

Field	Description
SCSI interface X	Information for SCSI device number X. Shows the make, device ID number, model number, and type of SCSI device.

Table 3-44 describes the fields shown in the **show interface standby** display.

Table 3-44 *Field Descriptions for the show interface standby Command*

Field	Description
Standby Group	Number that identifies the standby group.
Description	Description of the device, as configured by using the description option of the interface global configuration command.
IP address, netmask	IP address and netmask of the standby group.
Member interfaces	Member interfaces of the standby group. Shows which physical interfaces are part of the standby group. Shows the interface definition, such as GigabitEthernet 1/0.
Active interface	Interfaces that are currently active in the standby group.

Related Commands

(config) interface
 show running-config
 show startup-config

show inventory

To display the system inventory information for a WAAS device, use the **show inventory** EXEC command.

show inventory

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines The **show inventory** EXEC command allows you to view the UDI for a WAAS device. This identity information is stored in the WAAS device's nonvolatile memory.

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 WAAS device'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.

You can also use the **show tech-support** EXEC command to display the WAAS device UDI.

Examples [Table 3-45](#) describes the fields shown in the **show inventory** display.

Table 3-45 *Field Descriptions for the show inventory Command*

Field	Description
PID	Product identification (ID) number of the device.
VID	Version ID number of the device. Displays as 0 if the version number is not available.
SN	Serial number of the device.

Related Commands [show tech-support](#)

show ip access-list

To display the access lists that are defined and applied to specific interfaces or applications on a WAAS device, use the **show ip access-list EXEC** command.

```
show ip access-list [acl-name | acl-num]
```

Syntax Description		
<i>acl-name</i>	(Optional) Information for a specific access list, using an alphanumeric identifier up to 30 characters, beginning with a letter.	
<i>acl-num</i>	(Optional) Information for a specific access list, using a numeric identifier (0–99 for standard access lists and 100–199 for extended access lists).	

Defaults Displays information about all defined access lists.

Command Modes EXEC

Device Modes application-accelerator
 replication-accelerator
 central-manager

Usage Guidelines Use the **show ip access-list EXEC** command to display the access lists that have been defined on the WAAS device. Unless you identify a specific access list by name or number, the system displays information about all the defined access lists, including the following sections:

- Available space for new lists and conditions
- Defined access lists
- References by interface and application

Examples [Table 3-46](#) describes the fields shown in the **show ip access-list** display.

Table 3-46 Field Descriptions for the show ip access-list Command

Field	Description
Space available:	
XX access lists	Number of access lists remaining out of 50 maximum lists allowed.
XXX access list conditions	Number of access list conditions remaining out of 500 maximum conditions allowed.
Standard IP access list	Name of a configured standard IP access list. Displays a list of the conditions configured for this list.

Table 3-46 Field Descriptions for the show ip access-list Command (continued)

Field	Description
Extended IP access list	Name of a configured extended IP access list. Displays a list of the conditions configured for this list.
Interface access list references	List of interfaces and the access lists with which they are associated, displayed in the following format: <i>interface slot/port</i> <i>interface direction</i> <i>access list number</i>
Application access list references	List of applications and the access lists with which they are associated, displayed in the following format: <i>application type</i> <i>access list type and number</i> <i>associated port</i>

Related Commands[clear](#)[\(config\) ip access-list](#)

show ip routes

To display the IP routing table for a WAAS device, use the **show ip routes** EXEC command.

show ip routes

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines This command displays the IP route table, which lists all of the different routes that are configured on the WAE. The WAE uses this table to determine the next hop. This table includes routes from three sources: the WAE GigabitEthernet interfaces, any user-configured static routes, and the default gateway. The last line in this table shows the default route.

Examples [Table 3-47](#) describes the fields shown in the **show ip routes** display.

Table 3-47 *Field Descriptions for the show ip routes Command*

Field	Description
Destination	Destination IP addresses for each route.
Gateway	Gateway addresses for each route.
Netmask	Netmasks for each route.
Number of route cache entries	Number of entries in the route cache. The route cache is a separate entity and this field is not associated with the entries in the IP route table. The number of entries in the route cache can vary depending on the number of connections that are open.

Related Commands [\(config\) ip](#)
[\(config-if\) ip](#)

show kerberos

To display the Kerberos authentication configuration for a WAAS device, use the **show kerberos EXEC** command.

show kerberos

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines Use the system message log to view information about events that have occurred on a WAAS device. The *syslog.txt* file is contained in the */local1* directory.

Examples [Table 3-48](#) describes the fields shown in the **show kerberos** display.

Table 3-48 Field Descriptions for the show kerberos Command

Field	Description
Kerberos Configuration	
Local Realm	Local realm name.
DNS suffix	DNS suffix for the realm.
Realm for DNS suffix	DNS addresses of the computers that are part of this realm.
Name of host running KDC for realm	Name of the host running the Key Distribution Center for the realm.
Master KDC	Primary or main Key Distribution Center.
Port	Port that the Kerberos server is using for incoming requests from clients. The default is port 88.

Related Commands [clear](#)
[\(config\) logging](#)

show key-manager

To display key manager information for each WAAS device, use the **show key-manager EXEC** command.

show key-manager {key | status}

Syntax Description	key	status
	Shows detailed key manager information for each WAE device that is registered to the Central Manager.	Displays the overall encryption status information

Defaults No default behavior or values

Command Modes EXEC

Device Modes central-manager

Examples [Table 3-49](#) describes the fields shown in the **show key-manager key** display.

Table 3-49 Field Descriptions for the show key-manager status Command

Field	Description
WAE Device	Device name.
Key ID	Encryption key identification number.
Creation Time	Time the key was created.
Encryption Algorithm	Encryption algorithm.

Related Commands [show statistics key-manager](#)

show logging

To display the system message log configuration for a WAAS device, use the **show logging** EXEC command.

show logging

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines Use the system message log to view information about events that have occurred on a WAAS device. The *syslog.txt* file is contained in the */local1* directory.

Examples The following example displays the syslog host configuration on a WAAS device:

```
WAE# 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 1000000
```

Related Commands [clear](#)
[\(config\) logging](#)
[show sysfs volumes](#)

show memory

To display memory blocks and statistics for a WAAS device, use the **show memory** EXEC command.

show memory

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Examples [Table 3-50](#) describes the fields shown in the **show memory** display.

Table 3-50 *Field Descriptions for the show memory Command*

Field	Description
Total physical memory	Total amount of physical memory in kilobytes (KB).
Total free memory	Total available memory (in kilobytes).
Total buffer memory	Total amount of memory (in kilobytes) in the memory buffer.
Total cached memory	Total amount of memory (in kilobytes) in the memory cache.
Total swap	Total amount of memory (in kilobytes) for swap purposes.
Total free swap	Total available memory (in kilobytes) for swap purposes.

show ntp

To display the NTP parameters for a WAAS device, use the **show ntp** EXEC command.

show ntp status

Syntax Description	status	Displays NTP status.
---------------------------	---------------	----------------------

Defaults	No default behavior or values
-----------------	-------------------------------

Command Modes	EXEC
----------------------	------

Device Modes	application-accelerator replication-accelerator central-manager
---------------------	-----------------------------------------------------------------------

Examples [Table 3-51](#) describes the fields shown in the **show ntp status** display.

Table 3-51 *Field Descriptions for the show ntp status Command*

Field	Description
NTP	Indicates 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. In this example, stratum 1 is the top layer.
t	Type of peer (l ocal, u nicast, m ulticast, or b roadcast).
when	Indicates 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.

Table 3-51 *Field Descriptions for the show ntp status Command (continued)*

Field	Description
delay	Estimated delay (in milliseconds) between the requester and the server.
offset	Clock offset relative to the server.
jitter	Clock jitter.

Related Commands[clock](#)[\(config\) clock](#)[\(config\) ntp](#)

show policy-engine application

To display application policy information for a WAE, use the **show policy-engine application EXEC** command.

```
show policy-engine application {classifier [app-classifier] | dynamic | name}
```

Syntax Description	classifier	Description
		Displays information about the specified application classifier. If no classifier is specified, this command displays information about all classifiers. Every application classifier with a single match is displayed in one line.
	<i>app-classifier</i>	(Optional) Name of an application classifier. The name should not exceed 30 characters.
	dynamic	Shows the application dynamic match information.
	name	Shows the application names list.

Command Modes EXEC

Device Modes application-accelerator

Usage Guidelines Use the **show policy-engine application dynamic** command to display auto-discovered CIFS file servers that are added to the list. The servers are visible in the dynamic listing for a limited time (3 minutes by default) after any activity stops, and then they are dropped from the dynamic list until another client request causes them to be auto-discovered again.

Examples [Table 3-52](#) describes the fields shown in the **show policy-engine application classifier** display.

Table 3-52 Field Descriptions for the show policy-engine application classifier Command

Field	Description
Number of Application Classifiers:	Number of application classifiers configured.
0 to N	Numbered list that includes the application name and the match statement that defines which traffic is interesting. For example: 0) AFS match dst port range 7000 7009 1) Altiris-CarbonCopy match dst port eq 1680

Table 3-53 describes the fields shown in the **show policy-engine application dynamic** display.

Table 3-53 Field Descriptions for the show policy-engine application dynamic Command

Field	Description
Dynamic Match Freelist Information	
Allocated	Total number dynamic policies that can be allocated.
In Use	Number of dynamic matches that are currently in use.
Max In Use	Maximum number of dynamic matches that have been used since the last reboot.
Allocations	Number times that the dynamic match entries have been added.
Individual Dynamic Match Information:	
Number	Number of the match condition in the list.
Type	Type of traffic to match. For example, Any-->Local tests traffic from any source to the local WAE.
User Id	Name of the accelerator that inserted the entry.
Src	Value for the source match condition. Values can be ANY, LOCAL, an IP address, or a port to which the application applies.
Dst	Value for the destination match condition. Values can be ANY, LOCAL, an IP address, or a port to which the application applies.
Map Name	Policy engine application map that is invoked if the dynamic match entry matches a connection.
Flags	Operation flags specifying different connection handling options.
Seconds	Number of seconds specified as the time limit for the dynamic match entry to exist.
Remaining	Number of seconds remaining before the dynamic match entry expires and is deleted.
Hits	Number of connections that have matched.

Table 3-54 describes the fields shown in the **show policy-engine application name** display.

Table 3-54 Field Descriptions for the **show policy-engine application name** Command

Field	Description
Number of Applications: X	Number of applications defined on the WAE, including all of the default applications. WAAS includes over 150 default application policies. (For a list of default application policies, see the <i>Cisco Wide Area Application Services Configuration Guide</i> , Appendix A.) The display next lists each application that is defined on the WAE by name:
1) Authentication (15)	Name of the application and its internal numerical identifier, which is used to manage the application name in the policy engine.
2) Backup (18)	
3) Call-Management (17)	
4) Conferencing (8)	
5) Console (4)	
6) Content-Management (21)	
7) Directory-Services (6)	
8) Email-and-Messaging (12)	
9) Enterprise-Applications (13)	
10) File-System (2)	
11) File-Transfer (16)	
12) Instant-Messaging (22)	
13) Name-Services (25)	
14) Network-Analysis (26)	
15) P2P (7)	
16) Printing (14)	
17) Remote-Desktop (5)	
18) Replication (20)	
19) SQL (1)	
20) SSH (24)	
21) Storage (27)	
22) Streaming (11)	
23) Systems-Management (3)	
24) VPN (23)	
25) Version-Management (9)	
26) WAFS (10)	
27) Web (19)	
28) Other (0)	

Related Commands

(config) policy-engine application classifier
(config) policy-engine application map adaptor EPM
(config) policy-engine application map adaptor WAFS transport
(config) policy-engine application map basic delete
(config) policy-engine application map basic disable
(config) policy-engine application map basic insert
(config) policy-engine application map basic list
(config) policy-engine application map basic move
(config) policy-engine application map basic name
(config) policy-engine application map other optimize DRE
(config) policy-engine application map other optimize full
(config) policy-engine application map other pass-through
(config) policy-engine application name
(config) policy-engine config

show policy-engine status

To display high-level information about a WAE's policy engine, use the **show policy-engine status EXEC** command. This information includes the usage of the available resources, which include application names, classifiers, and conditions.

show policy-engine status

Command Modes EXEC

Device Modes application-accelerator

Examples [Table 3-55](#) describes the fields shown in the **show policy-engine status** display.

Table 3-55 *Field Descriptions for the show policy-engine status Command*

Field	Description
Policy-engine resources usage:	Table columns are Total, Used, and Available.
Application names	Total number of application names. Number of application names being used. Number of application names available.
Classifiers	Total number of classifiers configured. Number of classifiers being used. Number of classifiers available. The maximum number of classifiers allowed is 512.
Conditions	Total number of conditions configured. Number of conditions being used. Number of conditions available. The maximum number of match conditions allowed is 1024.
Policies	Total number of policies configured. Number of policies being used. Number of policies available. The maximum number of policies allowed is 512.

Related Commands

- (config) [policy-engine application classifier](#)
- (config) [policy-engine application map adaptor EPM](#)
- (config) [policy-engine application map adaptor WAFS transport](#)
- (config) [policy-engine application map basic delete](#)
- (config) [policy-engine application map basic disable](#)
- (config) [policy-engine application map basic insert](#)
- (config) [policy-engine application map basic list](#)
- (config) [policy-engine application map basic move](#)
- (config) [policy-engine application map basic name](#)
- (config) [policy-engine application map other optimize DRE](#)
- (config) [policy-engine application map other optimize full](#)

(config) policy-engine application map other pass-through

(config) policy-engine application name

(config) policy-engine config

show print-services

To display administrative users who have access to configuration privileges, print services, or print service processes on a WAAS device, use the **show print-services** EXEC command.

```
show print-services { drivers user username | process }
```

Syntax Description

process	Displays information about the print server and print spooler.
drivers	Displays printer drivers on this print server.
user <i>username</i>	Specifies a username that belongs to the print admin group.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator
 replication-accelerator
 central-manager

Examples

[Table 3-56](#) describes the fields shown in the **show print-services process** display.

Table 3-56 Field Descriptions for the show print-services process Command

Field	Description
Print server is running.	Operation status of the print server.
Print spooler is running.	Operation status of the print spooler.
Print Server Status	
Samba version 3.0.20	Samba version being used.
PID	Process ID. Process identification number of the Samba process on the WAE Linux appliance.
Username	UNIX user that has started the Samba process.
Group	UNIX group to which the user belongs.
Machine	Machine name and IP address. The machine name is the same as the NetBIOS name.
Service	Remote procedure call (RPC) port that is used by clients to connect to the print server. Value is always IPC\$.
pid	Process ID. Process identification number of the Samba process on the WAE Linux appliance.
machine	Machine name.

Table 3-56 *Field Descriptions for the show print-services process Command (continued)*

Field	Description
Connected at	Date and time of connection to the print server.
No locked files	Comment line.
Print Spooler Status	
scheduler is running	Operation status of the print spooler scheduler.
system default destination	Default print destination for WAAS (VistaPrinterOnWAAS).
device for (VistaPrinterOnWAAS)	Socket address for the system default print destination.
(VistaPrinterOnWAAS) accepting requests	Availability status of the system default print destination.
printer (VistaPrinterOnWAAS) is idle. enabled	Operation status of the system default printer.

Related Commands[\(config\) authentication](#)[\(config\) print-services](#)[show authentication](#)[windows-domain](#)[\(config\) windows-domain](#)

show processes

To display CPU or memory processes for a WAAS device, use the **show processes EXEC** command.

```
show processes [cpu | debug pid | memory | system [delay 1-60 | count 1-100]]
```

Syntax Description		
cpu	(Optional)	Displays CPU utilization.
debug	(Optional)	Prints the system call and signal traces for a specified process identifier to display system progress.
<i>pid</i>		Process identifier.
memory	(Optional)	Displays memory allocation processes.
system	(Optional)	Displays system load information in terms of updates.
delay	(Optional)	Specifies the delay between updates, in seconds (1–60).
count	(Optional)	Specifies the number of updates that are displayed (1–100).

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines Use the EXEC commands shown in this section to track and analyze system CPU utilization.

The **show processes debug** command displays extensive internal system call information and a detailed account of each system call (along with arguments) made by each process and the signals it has received.

Use the **show processes system** command to display system load information in terms of updates. The **delay** option specifies the delay between updates, in seconds. The **count** option specifies the number of updates that are displayed. This command displays these items:

- A list of all processes in wide format.
- Two tables listing the processes that utilize CPU resources. The first table displays the list of processes in descending order of utilization of CPU resources based on a snapshot taken after the processes system (ps) output is displayed. The second table displays the same processes based on a snapshot taken 5 seconds after the first snapshot.
- Virtual memory used by the corresponding processes in a series of five snapshots, each separated by 1 second.

**Note**

CPU utilization and system performance are severely affected when you use these commands. We therefore recommend that you avoid using these commands, especially the **show processes debug** command, unless it is absolutely necessary.

Examples

Table 3-57 describes the fields shown in the **show processes** display.

Table 3-57 *Field Descriptions for the show processes Command*

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.
SwapTotal	Total available memory in bytes for swap purposes.

show radius-server

To display RADIUS configuration information for a WAAS device, use the **show radius-server EXEC** command.

show radius-server

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Examples [Table 3-58](#) describes the fields shown in the **show radius-server** display.

Table 3-58 Field Descriptions for the show radius-server Command

Field	Description
Login Authentication for Console/Telnet Session	Indicates whether a RADIUS server is enabled for login authentication.
Configuration Authentication for Console/Telnet Session	Indicates whether a RADIUS server is enabled for authorization or configuration authentication.
Authentication scheme fail-over reason	Indicates whether the WAAS devices fail over to the secondary method of administrative login authentication whenever the primary administrative login authentication method.
RADIUS Configuration	RADIUS authentication settings.
Key	Key used to encrypt and authenticate all communication between the RADIUS client (the WAAS device) and the RADIUS server.
Timeout	Number of seconds that the WAAS device waits for a response from the specified RADIUS authentication server before declaring a timeout.
Servers	RADIUS servers that the WAAS device is to use for RADIUS authentication.
IP	Hostname or IP address of the RADIUS server.
Port	Port number on which the RADIUS server is listening.

Related Commands [\(config\) radius-server](#)

show running-config

To display a WAAS device's current running configuration information on the terminal, use the **show running-config** EXEC command. This command replaces the **write terminal** command.

show running-config

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines Use this EXEC command in conjunction with the **show startup-config** command to compare the information in running memory to the startup configuration used during bootup.

Examples The following example displays the currently running configuration of a WAAS device:

```
WAE# show running-config
! WAAS version 4.0.0
!
device mode central-manager
!
!
hostname waas-cm
!
!
!
!
exec-timeout 60
!
!
primary-interface GigabitEthernet 1/0
!
!
...
```

Related Commands [configure](#)
[copy running-config](#)

copy startup-config

show services

To display services-related information for a WAAS device, use the **show services** EXEC command.

```
show services { ports [port-num] | summary }
```

Syntax Description

ports	Displays services by port number.
<i>port-num</i>	(Optional) Up to 8 port numbers (1–65535).
summary	Displays the services summary.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator
 replication-accelerator
 central-manager

Examples

The following example displays a summary of the services:

```
WAE# show services summary
```

```
Service      Ports
-----
           CMS      1100  5256
           NLM      4045
           WAFS     1099
           emdb     5432
           MOUNT    3058
           MgmtAgent 5252
           WAFS_tunnel 4050
           CMS_db_vacuum 5257
```

show smb-conf

To view a WAAS device's current values of the Samba configuration file, *smb.conf*, use the **show smb-conf** EXEC command.

show smb-conf

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines This command displays the global, print\$, and printers parameters values of the *smb.conf* file for troubleshooting purposes. For a description of these parameters and their values, see the “(config) [smb-conf](#)” command.

Examples The following example displays all of the parameter values for the current configuration:

```
WAE# show smb-conf

Current smb-conf configurations -->

smb-conf section "global" name "ldap ssl" value "start_tls"
smb-conf section "printers" name "printer admin" value "root"

Output of current smb.conf file on disk -->

=====

# File automatically generated

[global]
idmap uid = 70000-200000
idmap gid = 70000-200000
winbind enum users = no
winbind enum groups = no
winbind cache time = 10
winbind use default domain = yes
printcap name = cups
load printers = yes
```

```

printing = cups
cups options = "raw"
force printername = yes
lpq cache time = 0
log file = /local/local1/errorlog/samba.log
max log size = 50
socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
smb ports = 50139
local master = no
domain master = no
preferred master = no
dns proxy = no
template homedir = /local/local1/
template shell = /admin-shell
ldap ssl = start_tls
comment = Comment:
netbios name = MYFILEENGINE
realm = ABC
wins server = 10.10.10.1
password server = 10.10.10.10
security = domain

[print$]
path = /state/samba/printers
guest ok = yes
browseable = yes
read only = yes
write list = root

[printers]
path = /local/local1/spool/samba
browseable = no
guest ok = yes
writable = no
printable = yes
printer admin = root

```

```

=====

```

Related Commands[\(config\) smb-conf](#)[windows-domain](#)[\(config\) windows-domain](#)

show snmp

To check the status of SNMP communications for a WAAS device, use the **show snmp** EXEC command.

```
show snmp {alarm-history | engine ID | event | group | stats | user}
```

Syntax Description	Parameter	Description
	alarm-history	Displays SNMP alarm history information.
	engineID	Displays local SNMP engine identifier.
	event	Displays events configured through the Event MIB.
	group	Displays SNMP groups.
	stats	Displays SNMP statistics.
	user	Displays SNMP users.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines This EXEC command provides information on various SNMP variables and statistics on SNMP operations.

Examples [Table 3-59](#) describes the fields shown in the **show snmp alarm-history** display.

Table 3-59 Field Descriptions for the show snmp alarm-history Command

Field	Description
Index	Displays the serial number of the listed alarms.
Type	Indicates whether the alarm has been Raised (R) or Cleared (C).
Sev	Levels of alarm severity: Critical (Cr), Major (Ma), or Minor (Mi).
Alarm ID	Traps sent by a WAE contain numeric alarm IDs.
ModuleID	Traps sent by a WAE contain numeric module IDs. (See Table 3-60 to map module names to module IDs.)

Table 3-59 Field Descriptions for the show snmp alarm-history Command (continued)

Field	Description
Category	Traps sent by a WAE contain numeric category IDs. (See Table 3-61 to map category names to category IDs.)
Descr	Provides description of the WAAS software alarm and the application that generated the alarm.

[Table 3-60](#) summarizes the mapping of module names to module IDs.

Table 3-60 Summary of Module Names to ID Numbers

Module Name	Module ID
AD_DATABASE	8000
NHM	1
NHM/NHM	2500
nodemgr	2000
standby	4000
sysmon	1000
UNICAST_DATA_RECEIVER	5000
UNICAST_DATA_SENDER	6000

[Table 3-61](#) summarizes the mapping of category names to category IDs.

Table 3-61 Summary of Category Names to ID Numbers

Category Name	Category ID
Communications	1
Service Quality	2
Processing Error	3
Equipment	4
Environment	5
Content	6

[Table 3-62](#) describes the fields shown in the show snmp engineID display.

Table 3-62 Field Descriptions for the show snmp engineID

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

[Table 3-63](#) describes the fields shown in the show snmp event display. The show snmp event command displays information about the SNMP events that were set using the “snmp trigger” command:

Table 3-63 Field Descriptions for the show snmp event Command

Field	Description
Mgmt Triggers	Output for management triggers, which are numbered 1, 2, 3, and so on in the output.
(1): Owner:	Name of the person who configured the trigger. “CLI” is the default owner; the system has a default trigger configured.
(1):	Name for the trigger. This name is locally-unique and administratively assigned. For example, this field might contain the “isValid” trigger name. Numbering indicates that this is the first management trigger listed in the show output.
Comment:	Description of the trigger’s function and use. For example: WAFS license file is not valid.
Sample:	Basis on which the test sample is being evaluated. For example: Abs (Absolute) or Delta.
Freq:	Frequency. Number of seconds to wait between trigger samplings. To encourage consistency in sampling, the interval is measured from the beginning of one check to the beginning of the next and the timer is restarted immediately when it expires, not when the check completes.
Test:	Type of trigger test to perform based on the SNMP trigger configured. The Test field may contain the following types of tests: Absent—Absent existence of a test Boolean—Boolean value test Equal—Equality threshold test Falling—Falling threshold test Greater-than—Greater-than threshold test Less-than—Less-than threshold test On-change—Changed existence test Present—Present present test Rising—Rising threshold test
ObjectOwner:	Name of the object owner who created the trigger using the snmp trigger create global configuration command or by using an SNMP interface. “CLI” is the default owner.
Object:	String identifying the object.
Boolean Entry:	
Value:	Object identifier of the MIB object to sample to see whether the trigger should fire.

Table 3-63 Field Descriptions for the `show snmp event` Command (continued)

Field	Description
Cmp:	Comparison. Type of boolean comparison to perform. The numbers 1–6 correspond to these Boolean comparisons: unequal (1) equal (2) less (3) lessOrEqual (4) greater (5) greaterOrEqual (6)
Start:	Starting value for which this instance will be triggered.
ObjOwn:	Object owner.
Obj:	Object.
EveOwn:	Event owner.
Eve:	Event. Type of SNMP event. For example: CLI_EVENT.
Delta Value Table:	Table containing trigger information for delta sampling.
(0):	
Thresh:	Threshold value to check against if the trigger type is threshold.
Exis:	Type of existence test to perform. Values are 1 or 0.
Read:	Indicates whether the MIB instance has been queried or not.
OID:	Object ID (Same as MIB instance).
val:	Value ID.
(2):	MIB instance on which the trigger is configured. This is the second management trigger listed in the show output. The fields are repeated for each instance listed in this show command.

Table 3-64 describes the fields shown in the `show snmp group` display.

Table 3-64 Field Descriptions for the `show snmp group` Command

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 (either 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 3-65 describes the fields shown in the `show snmp stats` display.

Table 3-65 *Field Descriptions for the show snmp stats Command*

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.
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 3-66 describes the fields shown in the **show snmp user** display.

Table 3-66 *Field Descriptions for the show snmp user Command*

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

(config) snmp-server community

(config) snmp-server contact

(config) snmp-server enable traps

(config) snmp-server group
(config) snmp-server host
(config) snmp-server location
(config) snmp-server mib persist event
(config) snmp-server notify inform
(config) snmp-server user
(config) snmp-server view
snmp trigger

show ssh

To display the status and configuration information of the Secure Shell (SSH) service for a WAAS device, use the **show ssh** EXEC command.

show ssh

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Examples [Table 3-67](#) describes the fields shown in the **show ssh** display.

Table 3-67 Field Descriptions for the show ssh Command

Field	Description
SSH server supports SSH2 protocol (SSH1 compatible).	Protocol support statement.
SSH service is not enabled.	Status of whether the SSH service is enabled or not enabled.
Currently there are no active SSH sessions.	Number of active SSH sessions.
Number of successful SSH sessions since last reboot:	Number of successful SSH sessions since last reboot.
Number of failed SSH sessions since last reboot:	Number of failed SSH sessions since last reboot.
SSH key has not been generated or previous key has been removed.	Status of the SSH key.
SSH login grace time value is 300 seconds.	Time allowed for login.
Allow 3 password guess(es).	Number of password guesses allowed.

Related Commands [\(config\) ssh-key-generate](#)
[\(config\) sshd](#)

show standby

To display information about a standby interface on a WAAS device, use the **show standby** EXEC command.

show standby

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines To display information about a specific standby group configuration, enter the **show interface standby standby group_num** EXEC command.

Examples [Table 3-68](#) describes the fields shown in the **show standby** display.

Table 3-68 Field Descriptions for the show standby Command

Field	Description
Standby Group	Number that identifies the standby group.
Description	Description of the device, as configured by using the description option of the interface global configuration command.
IP address	IP address of the standby group.
netmask	Netmask of the standby group.
Member interfaces	Member interfaces of the standby group. Shows which physical interfaces are part of the standby group. Shows the interface definition, such as GigabitEthernet 1/0.
priority	Priority status of each interface.
Active interface	Interfaces that are currently active in the standby group.
Maximum errors allowed on the active interface	Maximum number of errors allowed on the active interface.

Related Commands[show interface](#)[show running-config](#)[show startup-config](#)[\(config-if\) standby](#)

show startup-config

To display the startup configuration for a WAAS device, use the **show startup-config EXEC** command.

show startup-config

Syntax Description This command has no keywords or arguments.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines Use this EXEC command to display the configuration used during an initial bootup, stored in NVRAM. Note the difference between the output of this command versus the **show running-config** command.

Examples The following example displays the configuration saved for use on startup of the WAAS device:

```
WAE# show startup-config
! WAAS version 4.0.0
!
device mode central-manager
!
!
hostname Edge-WAE1
!
!
!
!
!
exec-timeout 60
!
!
primary-interface GigabitEthernet 1/0
!
!
!
interface GigabitEthernet 1/0
 ip address 10.10.10.33 255.255.255.0
 exit
interface GigabitEthernet 2/0
 shutdown
...

```

Related Commands[configure](#)[copy running-config](#)[show running-config](#)

show statistics authentication

To display authentication statistics for a WAAS device, use the **show statistics authentication EXEC** command.

show statistics authentication

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator
 replication-accelerator
 central-manager

Usage Guidelines Use the **show statistics authentication** command to display the number of authentication access requests, denials, and allowances recorded.

Examples The following example displays the statistics related to authentication on the WAAS device:

```
WAE# show statistics authentication
Authentication Statistics
-----
Number of access requests:      115
Number of access deny responses: 12
Number of access allow responses: 103
```

Related Commands [\(config\) authentication](#)
[clear](#)
[show authentication](#)

show statistics cifs

To display the CIFS statistics information, use the **show statistics cifs** EXEC command.

```
show statistics cifs {cache eviction | requests}
```

Syntax Description		
cache		Displays the statistics for CIFS cache.
eviction		Displays the status of CIFS cache eviction.
requests		Displays the statistics for CIFS requests.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator

Usage Guidelines Use the **show statistics cifs** EXEC command to view the CIFS traffic details itemized by request type. This command is useful when you want to understand how the system is being used. For example, are requests mostly for data transfer, browsing, database activity, or for some other purpose? You might correlate these statistics with performance issues for troubleshooting purposes, or you may use them to determine what specific performance optimizations to configure.

Examples [Table 3-69](#) describes the fields in the **show statistics cifs requests** display.

Table 3-69 Field Descriptions for the show statistics cifs requests Command

Field	Description
Statistics gathering period	Number of hours, minutes, seconds, and milliseconds of the statistics gathering period.
Total	Total number of CIFS requests.
Remote	Number of CIFS requests that were not handled from the local cache.
ALL_COMMANDS	Alias for all of the CIFS commands shown.
total	Total number of requests for all commands.
remote	Number of remote requests for all commands.
async	Number of async requests for all commands.
avg local	Average local request time in milliseconds for all commands.
avg remote	Average remote request time in milliseconds for all commands.

Table 3-69 Field Descriptions for the show statistics cifs requests Command (continued)

Field	Description
CONNECT	Connection check command.
total	Total number of requests for this command.
remote	Number of remote requests for this command.
async	Number of async requests for this command.
avg local	Average local request time in milliseconds for this command.
avg remote	Average remote request time in milliseconds for this command.
NB_SESSION_REQ	NetBIOS session request command.
VFN_LIVELINESS	Liveliness check command.

Related Commands[cifs](#)[show cifs](#)

show statistics content-distribution-network

To display the status of a WAE or device group that is registered with a WAAS Central Manager, use the **show statistics content-distribution-network EXEC** command. This command is available on only WAAS Central Managers.

show statistics content-distribution-network device status *device_id*

Syntax Description	device status	Displays the status of a WAE or device group that is registered with the WAAS Central Manager.
	<i>device_id</i>	Name or ID of the device or device group.

Defaults No default behavior or values

Command Modes EXEC

Device Modes central-manager

Usage Guidelines Use the **show statistics content-distribution-network EXEC** command to display the identification details about a WAE or WAEs in a device group, and verify if a WAE is online.

Examples The following example displays the identification details of a WAE that is registered with the WAAS Central Manager:

```
WAE# show statistics content-distribution-network device status edge-wae-11
Device id="CdmConfig_142" name="edge-wae-11" status="Online";
```

show statistics dre

To display Data Redundancy Elimination (DRE) general statistics for a WAE, use the **show statistics dre** EXEC command.

show statistics dre

Command Modes EXEC

Device Modes application-accelerator

Examples [Table 3-70](#) describes the fields shown in the **show statistics dre** display. This command shows the aggregated statistics for all connections.

Table 3-70 Field Descriptions for the show statistics dre Command

Field	Description
Cache	Aggregated DRE cache data statistics.
Status	Current DRE status. Status values include: Initializing, Usable, Temporarily Fail, and Fail.
Oldest Data (age)	Time that the DRE data has been in the cache in days (d), hours (h), minutes (m), and seconds (s). For example, "1d1h" means 1 day, 1 hour.
Total usable disk size	Total disk space allocated to the DRE cache.
Used (%)	Percentage of the total DRE cache disk space being used.
Hash table RAM size	Amount of memory allocated for the DRE hash table.
Used (%)	Percentage of allocated memory being used for the DRE hash table.
Completed Connections	
Total (cumulative):	Number of cumulative connections that have been processed.
Active:	Number of connections that are still open.
Encode	Statistics for compressed messages.
Overall: [msg in out ratio]	Aggregated statistics for compressed messages. msg = Total number of messages. in = Number of bytes before compression. out = Number of bytes after compression. ratio = Percentage of the total number of bytes that were compressed.
DRE: [msg in out ratio]	Number of DRE messages.
DRE bypass	Number of DRE messages that were bypassed for compression.

Table 3-70 Field Descriptions for the *show statistics dre* Command (continued)

Field	Description
LZ: [msg in out ratio]	Number of LZ messages. Note LZ compression is applied after DRE compression is applied. (DRE compression is always applied first.)
LZ Bypass: [msg in out ratio]	Number of LZ messages that were bypassed for compression.
Average Latency	Average time to compress one message for both DRE and LZ in milliseconds (ms).
Message size distribution	Percentage of messages that fall into each size grouping. (The message size field is divided into 6 size groups.)
Decode	Statistics for decompressed messages.
Overall: [msg in out ratio]	Aggregated statistics for decompressed messages: msg = Total number of messages. in = Number of bytes before decompression. out = Number of bytes after decompression. ratio = Percentage of the total number of bytes that were decompressed.
DRE: [msg in out ratio]	Number of DRE messages.
DRE Bypass [msg in]	Number of DRE messages that were bypassed for decompression.
LZ: [msg in out ratio]	Number of LZ messages.
LZ Bypass: [msg in]	Number of LZ messages that were bypassed for decompression.
Latency (Last 3 sec): [max avg]	Maximum time to decompress one message for both DRE and LZ in milliseconds (ms). Average time to decompress one message for both DRE and LZ in milliseconds (ms).
Message size distribution	Percentage of messages that fall into each size grouping. (The message size field is divided into 6 size groups.)

Related Commands

[debug](#)
[show statistics dre connection](#)
[show statistics dre peer](#)

show statistics dre connection

To display Data Redundancy Elimination (DRE) connection statistics for a WAE, use the **show statistics dre connection** EXEC command.

```
show statistics dre connection [active [client-ip {ip_address | hostname} | client-port port |
id connection_id | last | peer-no peer_id | server-ip {ip_address | hostname} | server-port port]
| client-ip {ip_address | hostname} | client-port port | id connection_id | last | peer-no peer_id
| server-ip {ip_address | hostname} | server-port port]
```

Syntax Description

active	(Optional) Displays all active connection statistics.
client-ip	(Optional) Displays the connection statistics for the client with the specified IP address or hostname.
<i>ip_address</i>	IP address of a client or server.
<i>hostname</i>	Hostname of a client or server.
client-port	(Optional) Displays the connection statistics for the client with the specified port number.
<i>port</i>	Port number of a client or server (1–65535).
id	(Optional) Displays the connection statistics for the connection with the specified identifier.
<i>connection_id</i>	Number from 0 to 4294967295 identifying a connection.
last	(Optional) Displays the last connection statistics.
peer-no	(Optional) Displays the connection statistics for the peer with the specified identifier.
<i>peer_id</i>	Number from 0 to 4294967295 identifying a peer.
server-ip	(Optional) Displays the connection statistics for the server with the specified IP address or hostname.
server-port	(Optional) Displays the connection statistics for the server with the specified port number.

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

This command displays the statistics for individual TCP connections on which DRE compression is being applied. This information is updated in real time.

Using this command without any options displays a one-line summary of all the TCP connections on the WAE for which DRE is applied. To obtain detailed statistics for a connection, use the command options to filter the connection. While most filters show detail statistics, some filters (such as, peer no.) show summary information and not details.

Examples

Table 3-71 describes the fields shown in the **show statistics dre connection** display.

Table 3-71 Field Descriptions for the **show statistics dre connection** Command

Field	Description
Conn-ID	Connection ID assigned by the device for each connection.
Peer No.	Number assigned to the peer compression device.
Client-ip:port	IP address and port of the client device that initialized the TCP connection, such as the user's PC or laptop.
Server-ip:port	IP address and port of the server.
Encode-in	Number of bytes in for compression.
Decode-in	Number of bytes in for decompression.
PID	Peer ID. MAC address of the peer device.
Status	State of the connection and the duration of that state. Possible values are Active or Closed. A = active C = closed For example, C(22h) shows that the connection has been closed for 22 hours.

Related Commands

[debug](#)

[show statistics dre connection](#)

show statistics dre peer

To display Data Redundancy Elimination (DRE) peer statistics for a WAE, use the **show statistics dre peer EXEC** command.

```
show statistics dre peer {context context-value [ip ip-address | peer-id peer-id |
peer-no peer-no] | ip ip-address [context context-value | ip ip-address | peer-id peer-id |
peer-no peer-no] | peer-id peer-id [context context-value | ip ip-address | peer-no peer-no] |
peer-no peer-no [context context-value | ip ip-address | peer-id peer-id]}
```

Syntax Description

context	Displays peer statistics for the specified context.
<i>context-value</i>	Context value (0–4294967295).
ip	(Optional) Specifies the IP address of the peer.
<i>ip_address</i>	IP address of the peer.
peer-id	(Optional) Specifies the MAC address of the peer.
<i>peer-id</i>	Peer ID (0–4294967295).
peer-no	(Optional) Specifies the peer number.
<i>peer-no</i>	Peer number.

Command Modes

EXEC

Device Modes

application-accelerator

Examples

[Table 3-72](#) describes the fields shown in the **show statistics dre peer** display. This command shows the DRE peer device connection information.

Table 3-72 Field Descriptions for the **show statistics dre peer** Command

Field	Description
Peer-No	Number assigned to the peer compression device.
Context	Context ID for the DRE debugging trace.
Peer-ID	MAC address of the peer device.
Hostname	Hostname of the peer device.
Cache	DRE cache data statistics as shown by the peer.
Used disk:	Number of megabytes (MB) used on the disk for the DRE cache.
Age:	Time that the DRE data has been in the cache in days (d), hours (h), minutes (m), and seconds (s).
Connections:	
Total (cumulative):	Number of cumulative connections that have been processed.
Active:	Number of connections that are still open.

Table 3-72 Field Descriptions for the *show statistics dre peer* Command (continued)

Field	Description
Concurrent connections (Last 2 min):	
max	Maximum number of concurrent connections in the last two minutes.
avg	Average number of concurrent connections in the last two minutes.
Encode	
Overall: [msg in out ratio]	Aggregated statistics for compressed messages: msg = Total number of messages. in = Number of bytes before decompression. out = Number of bytes after decompression. ratio = Percentage of the total number of bytes that were compressed.
DRE: [msg in out ratio]	Number of DRE messages.
DRE Bypass: [msg in]	Number of DRE messages that were bypassed for compression.
LZ: [msg in out ratio]	Number of LZ messages.
LZ Bypass: [msg in]	Number of LZ messages that were bypassed for compression.
Message size distribution	Percentage of messages that fall into each size grouping. (The message size field is divided into 6 size groups.)
Decode	
Overall: [msg in out ratio]	Aggregated statistics for decompressed messages: msg = Total number of messages. in = Number of bytes before decompression. out = Number of bytes after decompression. ratio = Percentage of the total number of bytes that were decompressed.
DRE: [msg in out ratio]	Number of DRE messages.
DRE Bypass: [msg in]	Number of DRE messages that were bypassed for decompression.
LZ: [msg in out ratio]	Number of LZ messages.
LZ Bypass: [msg in]	Number of LZ messages that were bypassed for decompression.
Latency (Last 3 sec): [max avg]	Maximum time to decompress one message for both DRE and LZ in milliseconds (ms). Average time to decompress one message for both DRE and LZ in milliseconds (ms).
Message size distribution	Percentage of messages that fall into each size grouping. (The message size field is divided into 6 size groups.)

■ show statistics dre peer

Related Commands [debug](#)

[show statistics dre connection](#)

show statistics epm

To display EndPoint Mapper (EPM) statistics for a WAE, use the **show statistics epm** EXEC command.

show statistics epm

Command Modes EXEC

Device Modes application-accelerator

Usage Guidelines This command displays the number of total requests and responses recorded.

Examples [Table 3-73](#) describes the fields shown in the **show statistics epm** display.

Table 3-73 *Field Descriptions for the show statistics epm Command*

Field	Description
Total requests	Number of requests processed by the EPM adaptor (incremented once for each connection).
success	Number of EPM requests which were successfully parsed by the EPM adaptor.
fault	Number of connections which were not successfully handled because of a bad client request (or a valid request that does not require processing by the EPM adaptor).
Total responses	Number of responses processed by the EPM adaptor (incremented once for each connection).
policy match	Number of connections which were successfully handled by the EPM adaptor, such as “dynamic match created,” for example.
UUID not configured	Number of times that a client requested a service that is not configured in the policy engine.
service unavailable	Number of times that a client requested a service, which the server reported to be unavailable.
fault	Number of connections which were not successfully handled because of a bad client response or because of an internal error which occurred while processing the client response.

Related Commands [\(config\) policy-engine application map adaptor EPM](#)

show statistics flow

To display flow statistics for a WAAS device, use the **show statistics flow** EXEC command.

```
show statistics flow { filters | monitor tcpstat-v1 }
```

Syntax Description	filters	Displays flow filter statistics.
	monitor	Displays flow performance statistics.
	tcpstat-v1	Displays tcpstat-v1 collector statistics.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator

Examples [Table 3-76](#) describes the fields shown in the **show statistics flow filters** display.

Table 3-74 *Field Descriptions for the show statistics flow filters Command*

Field	Description
Number of Filters	Number of filters.
Status	Status of whether the filters are enabled or disabled.
Capture Mode	Operation of the filter. Values include FILTER or PROMISCUOUS. The promiscuous operation is not available in WAAS.
Server	IP address list of the servers for which flows are being monitored.
Flow Hits	Number of flow hits for each server.
Flags	Flags identifying the flows: CSN: Client-Side Non-Optimized (Edge) SSO: Server-Side Optimized (Edge) CSO: Client-Side Optimized (Core) SSN: Server-Side Non-Optimized (Core) PT: Pass Through (Edge/Core/Intermediate) IC: Internal Client

Table 3-75 describes the fields shown in the **show statistics flow monitor** display.

Table 3-75 Field Descriptions for the **show statistics flow monitor** Command

Field	Description
Host Connection	
Configured host address	IP address of the tcpstat-v1 console for the connection.
Connection State	State of the connection.
Connection Attempts	Number of connection attempts.
Connection Failures	Number of connection failures.
Last connection failure	Date and time of the last connection failure.
Last configuration check sent	Date and time that the last configuration check was sent.
Last registration occurred	Date and time that the last registration occurred.
Host Version	Version number of the tcpstat-v1 console for the connection.
Collector Connection	
Collector host address:port	IP address and port number of the tcpstat-v1 aggregator identified through the host connection.
Connection State	State of the connection.
Connection Attempts	Number of connection attempts.
Connection Failures	Number of connection failures.
Last connection failure	Date and time of the last connection failure.
Last configuration check sent	Date and time that the last configuration check was sent.
Last update sent	Date and time that the last update was sent.
Updates sent	Number of updates sent.
Summaries discarded	Number of summaries that were discarded because disk space allocated for storage has reached its limit. The numbers in this field indicate when summaries are being collected faster than they are able to be transferred to the collector. Counters in this field generate a data_update alarm.
Last registration occurred	Date and time that the last registration occurred.
Host Version	Version number of the tcpstat-v1 aggregator for the connection.
Collection Statistics	
Collection State	State of the summary collection operation.
Summaries collected	Number of summaries collected. Summaries are packet digests of the traffic that is being monitored.
Summaries dropped	Total number of summaries dropped. This is the sum of the following subcategories.
Dropped by TFO	Number of packets that were dropped by TFO because of an error, such as not being able to allocate memory.

Table 3-75 *Field Descriptions for the show statistics flow monitor Command (continued)*

Field	Description
Dropped due to backlog	Number of packets that were dropped because the queue limit has been reached. This counter indicates whether the flow monitor application can keep up with the number of summaries being received.
Summary backlog	Number of packets that are waiting in the queue to be read by the collector module on the WAE,
Last drop occurred	Date and time that the last packet drop occurred.

Related Commands [clear](#)

show statistics icmp

To display ICMP statistics for a WAAS device, use the **show statistics icmp** EXEC command.

show statistics icmp

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Examples [Table 3-76](#) describes the fields shown in the **show statistics icmp** display.

Table 3-76 Field Descriptions for the show statistics icmp Command

Field	Description
ICMP messages received	Total number of Internet Control Message Protocol (ICMP) messages which the entity received, including all those counted as ICMP input errors.
ICMP messages receive failed	Number of ICMP messages which the entity received but determined as having ICMP-specific errors, such as bad ICMP checksums, bad length, and so forth.
Destination unreachable	Number of ICMP messages of this type received.
Timeout in transit	Number of ICMP messages of this type received.
Wrong parameters	Number of ICMP messages of this type received.
Source quenches	Number of ICMP messages of this type received.
Redirects	Number of ICMP messages of this type received.
Echo requests	Number of ICMP messages of this type received.
Echo replies	Number of ICMP messages of this type received.
Timestamp requests	Number of ICMP messages of this type received.
Timestamp replies	Number of ICMP messages of this type received.
Address mask requests	Number of ICMP messages of this type received.
Address mask replies	Number of ICMP messages of this type received.

Table 3-76 Field Descriptions for the show statistics icmp Command (continued)

Field	Description
ICMP messages sent	Total total number of ICMP messages which this entity attempted to send. This counter includes all those counted as ICMP output errors.
ICMP messages send failed	Number of number of ICMP messages which this entity did not send because of problems discovered within ICMP, such as a lack of buffers.
Destination unreachable	Number of ICMP messages of this type sent out.
Time exceeded	Number of ICMP messages of this type sent out.
Wrong parameters	Number of ICMP messages of this type sent out.
Source quenches	Number of ICMP messages of this type sent out.
Redirects	Number of ICMP messages of this type sent out.
Echo requests	Number of ICMP messages of this type sent out.
Echo replies	Number of ICMP messages of this type sent out.
Timestamp requests	Number of ICMP messages of this type sent out.
Timestamp replies	Number of ICMP messages of this type sent out.
Address mask requests	Number of ICMP messages of this type sent out.
Address mask replies	Number of ICMP messages of this type sent out.

Related Commands [clear](#)

show statistics ip

To display IP statistics for a WAAS device, use the **show statistics ip EXEC** command.

show statistics ip

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Examples [Table 3-77](#) describes the fields shown in the **show statistics ip** display.

Table 3-77 *Field Descriptions for the show statistics ip Command*

Field	Description
IP statistics	
Total packets in	Total number of input datagrams received from interfaces, including all those counted as input errors.
with invalid address	Number of input datagrams discarded because the IP address in their IP header destination field was not a valid address to be received at this entity. This count includes invalid addresses (such as, 0.0.0.0) and addresses of unsupported Classes (such as, Class E). For entities that are not IP gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
with invalid header	Number of input datagrams discarded because of errors in their IP headers, including bad checksums, version number mismatches other format errors, time-to-live exceeded errors, and errors discovered in processing their IP options.
forwarded	Number of input datagrams for which this entity was not their final IP destination, and as a result, an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP gateways, this counter includes only those packets which were source-routed by way of this entity, and the source-route option processing was successful.

Table 3-77 Field Descriptions for the show statistics ip Command (continued)

Field	Description
unknown protocol	Number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
discarded	Number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (such as, for lack of buffer space). 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 which 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 for which no problem was encountered to prevent their transmission to their destination, but which were discarded (such as, for lack of buffer space). This counter includes datagrams counted in the forwarded field if any such packets meet this (discretionary) discard criterion.
dropped (no route)	Number of IP datagrams discarded because no route could be found to transmit them to their destination. This counter includes any packets counted in the forwarded field which meet this no-route criterion, including any datagrams that a host cannot route because all of its default gateways are down.
Fragments dropped after timeout	Maximum number of seconds that received fragments are held while they are awaiting reassembly at this entity.
Reassemblies required	Number of IP fragments received which needed to be reassembled at this entity.
Packets reassembled	Number of IP datagrams successfully reassembled.
Packets reassemble failed	Number of number of failures detected by the IP reassembly algorithm (for whatever reason: timed out, errors, and so forth). This count 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	Total 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 because their Don't Fragment flag was set.
Fragments created	Number of IP datagram fragments that have been generated as a result of fragmentation at this entity.

Related Commands

[clear](#)
[\(config\) ip](#)

```
(config-if) ip  
show ip routes
```

show statistics key-manager

To display key manager information for each WAAS device, use the **show statistics key-manager EXEC** command.

show statistics key-manager

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Device Modes central-manager

Examples [Table 3-78](#) describes the fields shown in the **show statistics key-manager** display.

Table 3-78 *Field Descriptions for the show statistics key-manager Command*

Field	Description
Count of Retrieve key	Number of encryption keys retrieved.
Count of Create new key	Number of new keys created.

Related Commands **show statistics key-manager**

show statistics netstat

To display Internet socket connection statistics for a WAAS device, use the **show statistics netstat EXEC** command.

show statistics netstat

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Examples [Table 3-79](#) describes the fields shown in the **show statistics netstat** display.

Table 3-79 Field Descriptions for the show statistics netstat Command

Field	Description
Active Internet connections (w/o servers)	A list of all open Internet connections to and from this WAE.
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 precool stack in the send direction on a connection.
Local Address	IP address and Layer 4 port used at the WAE 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 RADIUS authentication statistics for a WAAS device, use the **show statistics radius EXEC** command.

show statistics radius

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Examples [Table 3-80](#) describes the fields shown in the **show statistics radius** display.

Table 3-80 Field Descriptions for the show statistics radius Command

Field	Description
RADIUS Statistics	
Authentication	
Number of access requests	Number of access requests.
Number of access deny responses	Number of access deny responses.
Number of access allow responses	Number of access allow responses.
Authorization	
Number of authorization requests	Number of authorization requests.
Number of authorization failure responses	Number of authorization failure responses.
Number of authorization success responses	Number of authorization success responses.
Accounting	
Number of accounting requests	Number of accounting requests.

Table 3-80 *Field Descriptions for the show statistics radius Command (continued)*

Field	Description
Number of accounting failure responses	Number of accounting failure responses.
Number of accounting success responses	Number of accounting success responses.

Related Commands[clear](#)[\(config\) radius-server](#)[show radius-server](#)

show statistics services

To display services statistics for a WAAS device, use the **show statistics services EXEC** command.

show statistics services

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator
 replication-accelerator
 central-manager

Examples [Table 3-81](#) describes the fields shown in the **show statistics services** display.

Table 3-81 *Field Descriptions for the show statistics services Command*

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

Related Commands [show services](#)

show statistics snmp

To display SNMP statistics for a WAAS device, use the **show statistics snmp** EXEC command.

show statistics snmp

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Examples [Table 3-82](#) describes the fields shown in the **show statistics snmp** display.

Table 3-82 Field Descriptions for the show statistics snmp Command

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.

Table 3-82 *Field Descriptions for the show statistics snmp Command (continued)*

Field	Description
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.

Related Commands[show snmp](#)[\(config\) snmp-server user](#)[\(config\) snmp-server view](#)

show statistics tacacs

To display TACACS+ authentication and authorization statistics for a WAAS device, use the **show statistics tacacs EXEC** command.

show statistics tacacs

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Examples [Table 3-83](#) describes the fields shown in the **show statistics tacacs** display.

Table 3-83 Field Descriptions for the show statistics tacacs Command

Field	Description
TACACS+ Statistics	
Authentication	
Number of access requests	Number of access requests.
Number of access deny responses	Number of access deny responses.
Number of access allow responses	Number of access allow responses.
Authorization	
Number of authorization requests	Number of authorization requests.
Number of authorization failure responses	Number of authorization failure responses.
Number of authorization success responses	Number of authorization success responses.
Accounting	
Number of accounting requests	Number of accounting requests.

Table 3-83 *Field Descriptions for the show statistics tacacs Command (continued)*

Field	Description
Number of accounting failure responses	Number of accounting failure responses.
Number of accounting success responses	Number of accounting success responses.

Related Commands[clear](#)[\(config\) tacacs](#)[show tacacs](#)

show statistics tcp

To display TCP statistics for a WAAS device, use the **show statistics tcp** EXEC command.

show statistics tcp

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Examples [Table 3-84](#) describes the fields shown in the **show statistics tcp** display.

Table 3-84 *Field Descriptions for the show statistics tcp Command*

Field	Description
TCP statistics	
Server connection openings	Number of times that TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.
Client connection openings	Number of times that TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.
Failed connection attempts	Number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.
Connections established	Number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.
Connections resets received	Number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.
Connection resets sent	Number of TCP segments sent containing the RST flag.
Segments received	Total number of segments received, including those received in error. This count includes segments received on currently established connections.

Table 3-84 Field Descriptions for the show statistics tcp Command (continued)

Field	Description
Segments sent	Total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
Bad segments received	Number of bad segments received.
Segments retransmitted	Total number of segments retransmitted, that is, the number of TCP segments transmitted containing one or more previously transmitted octets.
Retransmit timer expirations	Number of TCP packets retransmitted due to retransmit timer expiry.
Server segments received	Number of TCP packets received from the server.
Server segments sent	Number of TCP packets sent to the server.
Server segments retransmitted	Number of TCP packets retransmitted to the server.
Client segments received	Number of TCP packets received from the client.
Client segments sent	Number of TCP packets sent to the client.
Client segments retransmitted	Number of TCP packets retransmitted to the client.
TCP extended statistics	
Sync cookies sent	Number of SYN-ACK packets sent with SYN cookies in response to SYN packets.
Sync cookies received	Number of ACK packets received with the correct SYN cookie that was sent in the SYN-ACK packet by the device.
Sync cookies failed	Number of ACK packets received with the incorrect SYN cookie that was sent in the SYN-ACK packet by the device.
Embryonic connection resets	Number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-RCVD state, the SYN-SENT state, or the SYN-ACK-SENT state.
Prune message called	Number of times that the device exceeded the memory pool allocated for the connection.
Packets pruned from receive queue	Number of packets dropped from the receive queue of the connection because of a memory overrun.
Out-of-order-queue pruned	Number of times that the out-of-order queue was pruned because of a memory overrun.
Out-of-window Icmp messages	Number of ICMP packets received on a TCP connection that were out of the received window.
Lock dropped Icmp messages	Number of ICMP packets dropped because the socket is busy.
Arp filter	Number of ICMP responses dropped because of the ARP filter.
Time-wait sockets	Number of times that the TCP connection made a transition to the CLOSED state from the TIME-WAIT state.
Time-wait sockets recycled	Number of times that the TCP connection made a transition to the CLOSED state from the TIME-WAIT state.
Time-wait sockets killed	Number of times that the TCP connection made a transition to the CLOSED state from TIME-WAIT state.

Table 3-84 Field Descriptions for the *show statistics tcp* Command (continued)

Field	Description
PAWS passive	Number of incoming SYN packets dropped because of a PAWS check failure.
PAWS active	Number of incoming SYN-ACK packets dropped because of a PAWS check failure.
PAWS established	Number of packets dropped in ESTABLISHED state because of a PAWS check failure.
Delayed acks sent	Number of delayed ACKs sent.
Delayed acks blocked by socket lock	Number of delayed ACKs postponed because the socket is busy.
Delayed acks lost	Number of delayed ACKs lost.
Listen queue overflows	Number of incoming TCP connections dropped because of a listening server queue overflow.
Connections dropped by listen queue	Number of incoming TCP connections dropped because of an internal error.
TCP packets queued to prequeue	Number of incoming TCP packets prequeued to a process.
TCP packets directly copied from backlog	Number of incoming TCP packets copied from the backlog queue directly to a process.
TCP packets directly copied from prequeue	Number of incoming TCP packets copied from the prequeue directly to a process.
TCP prequeue dropped packets	Number of packets removed from the TCP prequeue.
TCP header predicted packets	Number of TCP header-predicted packets.
Packets header predicted and queued to user	Number of TCP packets header-predicted and queued to the user.
TCP pure ack packets	Number of ACK packets received with no data.
TCP header predicted acks	Number of header-predicted TCP ACK packets.
TCP Reno recoveries	Number of TCP Reno recoveries.
TCP SACK recoveries	Number of TCP SACK recoveries.
TCP SACK renegeing	Number of TCP SACK renegeing.
TCP FACK reorders	Number of TCP FACK reorders.
TCP SACK reorders	Number of TCP SACK reorders.
TCP Reno reorders	Number of TCP Reno reorders.
TCP TimeStamp reorders	Number of TCP TimeStamp reorders.
TCP full undos	Number of TCP full undos.
TCP partial undos	Number of TCP partial undos.
TCP DSACK undos	Number of TCP DSACK undos.
TCP loss undos	Number of TCP loss undos.
TCP losses	Number of TCP losses.
TCP lost retransmit	Number of TCP lost retransmit.
TCP Reno failures	Number of TCP Reno failures.

Table 3-84 Field Descriptions for the `show statistics tcp` Command (continued)

Field	Description
Segments sent	Total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
Bad segments received	Number of bad segments received.
Segments retransmitted	Total number of segments retransmitted, that is, the number of TCP segments transmitted containing one or more previously transmitted octets.
Retransmit timer expirations	Number of TCP packets retransmitted due to retransmit timer expiry.
Server segments received	Number of TCP packets received from the server.
Server segments sent	Number of TCP packets sent to the server.
Server segments retransmitted	Number of TCP packets retransmitted to the server.
Client segments received	Number of TCP packets received from the client.
Client segments sent	Number of TCP packets sent to the client.
Client segments retransmitted	Number of TCP packets retransmitted to the client.
TCP extended statistics	
Sync cookies sent	Number of SYN-ACK packets sent with SYN cookies in response to SYN packets.
Sync cookies received	Number of ACK packets received with the correct SYN cookie that was sent in the SYN-ACK packet by the device.
Sync cookies failed	Number of ACK packets received with the incorrect SYN cookie that was sent in the SYN-ACK packet by the device.
Embryonic connection resets	Number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-RCVD state, the SYN-SENT state, or the SYN-ACK-SENT state.
Prune message called	Number of times that the device exceeded the memory pool allocated for the connection.
Packets pruned from receive queue	Number of packets dropped from the receive queue of the connection because of a memory overrun.
Out-of-order-queue pruned	Number of times that the out-of-order queue was pruned because of a memory overrun.
Out-of-window Icmp messages	Number of ICMP packets received on a TCP connection that were out of the received window.
Lock dropped Icmp messages	Number of ICMP packets dropped because the socket is busy.
Arp filter	Number of ICMP responses dropped because of the ARP filter.
Time-wait sockets	Number of times that the TCP connection made a transition to the CLOSED state from the TIME-WAIT state.
Time-wait sockets recycled	Number of times that the TCP connection made a transition to the CLOSED state from the TIME-WAIT state.
Time-wait sockets killed	Number of times that the TCP connection made a transition to the CLOSED state from TIME-WAIT state.

Table 3-84 Field Descriptions for the show statistics tcp Command (continued)

Field	Description
PAWS passive	Number of incoming SYN packets dropped because of a PAWS check failure.
PAWS active	Number of incoming SYN-ACK packets dropped because of a PAWS check failure.
PAWS established	Number of packets dropped in ESTABLISHED state because of a PAWS check failure.
Delayed acks sent	Number of delayed ACKs sent.
Delayed acks blocked by socket lock	Number of delayed ACKs postponed because the socket is busy.
Delayed acks lost	Number of delayed ACKs lost.
Listen queue overflows	Number of incoming TCP connections dropped because of a listening server queue overflow.
Connections dropped by listen queue	Number of incoming TCP connections dropped because of an internal error.
TCP packets queued to prequeue	Number of incoming TCP packets prequeued to a process.
TCP packets directly copied from backlog	Number of incoming TCP packets copied from the backlog queue directly to a process.
TCP packets directly copied from prequeue	Number of incoming TCP packets copied from the prequeue directly to a process.
TCP prequeue dropped packets	Number of packets removed from the TCP prequeue.
TCP header predicted packets	Number of TCP header-predicted packets.
Packets header predicted and queued to user	Number of TCP packets header-predicted and queued to the user.
TCP pure ack packets	Number of ACK packets received with no data.
TCP header predicted acks	Number of header-predicted TCP ACK packets.
TCP Reno recoveries	Number of TCP Reno recoveries.
TCP SACK recoveries	Number of TCP SACK recoveries.
TCP SACK renegeing	Number of TCP SACK renegeing.
TCP FACK reorders	Number of TCP FACK reorders.
TCP SACK reorders	Number of TCP SACK reorders.
TCP Reno reorders	Number of TCP Reno reorders.
TCP TimeStamp reorders	Number of TCP TimeStamp reorders.
TCP full undos	Number of TCP full undos.
TCP partial undos	Number of TCP partial undos.
TCP DSACK undos	Number of TCP DSACK undos.
TCP loss undos	Number of TCP loss undos.
TCP losses	Number of TCP losses.
TCP lost retransmit	Number of TCP lost retransmit.
TCP Reno failures	Number of TCP Reno failures.

Table 3-84 Field Descriptions for the show statistics tcp Command (continued)

Field	Description
TCP SACK failures	Number of TCP SACK failures.
TCP loss failures	Number of TCP loss failures.
TCP fast retransmissions	Number of TCP fast retransmissions.
TCP forward retransmissions	Number of TCP forward retransmissions.
TCP slowstart retransmissions	Number of TCP slow start retransmissions.
TCP Timeouts	Number of TCP timeouts.
TCP Reno recovery fail	Number of TCP Reno recovery fail.
TCP Sack recovery fail	Number of TCP Sack recovery failures.
TCP scheduler failed	Number of TCP scheduler failures.
TCP receiver collapsed	Number of TCP receiver collapsed failures.
TCP DSACK old packets sent	Number of TCP DSACK old packets sent.
TCP DSACK out-of-order packets sent	Number of TCP DSACK out-of-order packets sent.
TCP DSACK packets received	Number of TCP DSACK packets received.
TCP DSACK out-of-order packets received	Number of TCP DSACK out-of-order packets received.
TCP connections abort on sync	Number of TCP connections aborted on sync.
TCP connections abort on data	Number of TCP connections aborted on data.
TCP connections abort on close	Number of TCP connections aborted on close.
TCP connections abort on memory	Number of TCP connections aborted on memory.
TCP connections abort on timeout	Number of TCP connections aborted on timeout.
TCP connections abort on linger	Number of TCP connections aborted on linger.
TCP connections abort failed	Number of TCP connections abort failed.
TCP memory pressures	Number of times the device approaches the allocated memory pool for the TCP stack.

Related Commands

clear
show tcp
(config) tcp

show statistics tfo

To display Traffic Flow Optimization (TFO) statistics for a WAE, use the **show statistics tfo** EXEC command.

```
show statistics tfo [application app-name | pass-through | peer | saving app-name]
```

Syntax Description		
application	(Optional)	Displays statistics per application.
<i>app-name</i>		Application name.
pass-through	(Optional)	Displays the pass-through statistics.
peer	(Optional)	Displays peer information.
saving	(Optional)	Displays savings for all applications.

Command Modes EXEC

Device Modes application-accelerator

Examples [Table 3-85](#) describes the fields shown in the **show statistics tfo** command.

Table 3-85 Field Descriptions for the show statistics tfo Command

Field	Description
Total number of optimized connections	Total number of TCP connections that were optimized since the last TFO statistics reset.
No. of active connections	Total number of TCP optimized connections.
No. of pending (to be accepted) connections	Number of TCP connections that will be optimized but are currently in the setup stage.
No. of connections closed normally	Number of optimized connections closed without any issues using TCP FIN.
No. of connections closed with error	Number of optimized connection closed with some issues or using TCP RST.
Total number of peers	Number of active peer WAEs. (Every connection is optimized between two WAEs: this one and a peer WAE.)
No. of entries into overload mode	Number of times the WAE entered into an overload state. (In the overload state, new connections are set to pass-through. This state occurs for various reasons, such as reaching the maximum number of concurrent connections.
No. of connections reset due to	Details for number of connections closed with error.
Socket write failure	Failed to write on a socket (either on the LAN or WAN side).
Socket read failure	Failed to read from a socket (either LAN or WAN side).

Table 3-85 Field Descriptions for the show statistics tfo Command (continued)

Field	Description
Opt socket close while waiting to write	The socket between two WAEs (WAN socket) closed before completing writing into it.
Unopt socket close while waiting to write	The socket between the WAE and the client/server (LAN socket) closed before completing writing into it.
Opt socket error close while waiting to read	The socket between two WAEs (WAN socket) closed before completing reading from it.
Unopt socket error close while waiting to read	The socket between the WAE and the client/server (LAN socket) closed before completing reading from it.
DRE decode failure	DRE internal error while decoding data. (Should not happen.)
DRE encode failure	DRE internal error while encoding data. (Should not happen.)
Connection init failure	Failed to setup the connection although auto-discovery finished successfully.
Opt socket unexpected close while waiting to read	The socket between two WAEs (WAN socket) closed before completing reading from it.
Exceeded maximum number of supported connections	Connection closed ungracefully because the WAE reached its scalability limit.
Buffer allocation or manipulation failed	Internal memory allocation failure. (Should not happen.)
Peer received reset from end host	TCP RST sent by the server or client. (Can be normal behavior and does not necessarily indicate a problem.)
DRE connection state out of sync	DRE internal error. (Should not happen.)
Memory allocation failed for buffer heads	Internal memory allocation failure. (Should not happen.)

Related Commands

[show tfo accelerators](#)
[show tfo bufpool](#)
[show tfo connection](#)
[show tfo status](#)

show statistics udp

To display User Datagram Protocol (UDP) statistics for a WAAS device, use the **show statistics udp EXEC** command.

show statistics udp

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Examples [Table 3-86](#) describes the fields shown in the **show statistics udp** display.

Table 3-86 *Field Descriptions for the show statistics udp Command*

Field	Description
UDP statistics	
Packets received	Total number of UDP datagrams delivered to UDP users.
Packets to unknown port received	Total number of received UDP datagrams for which there was no application at the destination port.
Packet receive error	Number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
Packet sent	Total number of UDP datagrams sent from this entity.

show statistics wccp

To display WCCP statistics for a WAE, use the **show statistics wccp EXEC** command.

show statistics wccp gre

Syntax Description	gre	Displays WCCP generic routing encapsulation packet-related statistics.
--------------------	-----	------------------------------------------------------------------------

Defaults	No default behavior or values
----------	-------------------------------

Command Modes	EXEC
---------------	------

Device Modes	application-accelerator
--------------	-------------------------

Usage Guidelines GRE is a Layer 3 technique that allows datagrams to be encapsulated into IP packets at the WCCP-enabled router and then redirected to a WAE (the transparent proxy server). At this intermediate destination, the datagrams are decapsulated and then routed to an origin server to satisfy the request if a cache miss occurs. In doing so, the trip to the origin server appears to the inner datagrams as one hop. Usually, the redirected traffic using GRE is referred to as GRE tunnel traffic. With GRE, all redirection is handled by the router software.

With WCCP redirection, a Cisco router does not forward the TCP SYN packet to the destination because the router has WCCP enabled on the destination port of the connection. Instead, the WCCP-enabled router encapsulates the packet using GRE tunneling and sends it to the WAE that has been configured to accept redirected packets from this WCCP-enabled router.

After receiving the redirected packet, the WAE does the following:

1. Strips the GRE layer from the packet.
2. Decides whether it should accept this redirected packet and process the request for the content as follows:
 - a. If the WAE accepts the request, it sends a TCP SYN ACK packet to the client. In this response packet, the WAE uses the IP address of the original destination (origin server) that was specified as the source address so that the WAE can be invisible (transparent) to the client; it acts as if it is the destination that the client's TCP SYN packet was trying to reach.
 - b. If the WAE does not accept the request, it reencapsulates the TCP SYN packet in GRE and sends it back to the WCCP-enabled router. The router identifies that the WAE is not interested in this connection and forwards the packet to its original destination (the origin server).

For example, a WAE would not accept the request because it is configured to bypass requests that originate from a certain set of clients or that are destined to a particular set of servers.

Examples [Table 3-87](#) describes the fields shown in the **show statistics wccp gre** display.

Table 3-87 Field Descriptions for the `show statistics wccp gre` Command

Field	Description
Transparent GRE packets received	Total number of GRE packets received by the WAE, regardless of whether or not they have been intercepted by WCCP. GRE is a Layer 3 technique that allows packets to reach the WAE, even if there are any number of routers in the path to the WAE.
Transparent non-GRE packets received	Number of non-GRE packets received by the WAE, either using the traffic interception and redirection functions of WCCP in the router hardware at Layer 2 or Layer 4 switching (a Content Switching Module [CSM]) that redirects requests transparently to the WAE.
Transparent non-GRE packets passed through	Number of non-GRE packets transparently intercepted by a Layer 4 switch and redirected to the WAE.
Total packets accepted	Total number of packets that are transparently intercepted and redirected to the WAE to serve client requests for content.
Invalid packets received	Number of packets that are dropped either because the redirected packet is a GRE packet and the WCCP GRE header has invalid data or the IP header of the redirected packet is invalid.
Packets received with invalid service	Number of WCCP version 2 GRE redirected packets that contain an invalid WCCP service number.
Packets received on a disabled service	Number of WCCP version 2 GRE redirected packets that specify the WCCP service number for a service that is not enabled on the WAE. For example, an HTTPS request redirected to the WAE when the HTTPS-caching service (service 70) is not enabled.
Packets received too small	Number of GRE packets redirected to the WAE that do not contain the minimum amount of data required for a WCCP GRE header.
Packets dropped due to zero TTL	Number of GRE packets that are dropped by the WAE because the redirected packet's IP header has a zero TTL.
Packets dropped due to bad buckets	Number of packets that are dropped by the WAE because the WCCP flow redirection could not be performed due to a bad mask or hash bucket determination. Note A bucket is defined as a certain subsection of the allotted hash assigned to each WAE in a WAE cluster. If only one WAE exists in this environment, it has 256 buckets assigned to it.
Packets dropped due to no redirect address	Number of packets that are dropped because the flow redirection destination IP address could not be determined.
Packets dropped due to loopback redirect	Number of packets that are dropped by the WAE when the destination IP address is the same as the loopback address.
Pass-through pkts dropped on assignment update	Number of packets that were targeted for TFO pass-through, but were dropped instead because the bucket was not owned by the device.

Table 3-87 Field Descriptions for the show statistics wccp gre Command (continued)

Field	Description
Connections bypassed due to load	Number of connection flows that are bypassed when the WAE is overloaded. When the overload bypass option is enabled, the WAE bypasses a bucket and reroutes the overload traffic. If the load remains too high, another bucket is bypassed, and so on, until the WAE can handle the load.
Packets sent back to router	Number of requests that are passed back by the WAE to the WCCP-enabled router from which the request was received. The router then sends the flow toward the origin web server directly from the web browser, which bypasses the WAE.
Packets sent to another WAE	Number of packets that are redirected to another WAE in the WCCP service group. Service groups consist of up to 32 WAEs and 32 WCCP-enabled routers. In both packet-forwarding methods, the hash parameters specify how redirected traffic should be load balanced among the WAEs in the various WCCP service groups.
GRE fragments redirected	Number of GRE packets received by the WAE that are fragmented. These packets are redirected back to the router.
GRE encapsulated fragments received	Number of GRE encapsulated fragments received by the WAE. The tcp-promiscuous service does not inspect port information and therefore the router or switch may GRE encapsulate IP fragments and redirect them to the WAE. These fragments are then reassembled into packets before being processed.
Packets failed encapsulated reassembly	Number of reassembled GRE encapsulated packets that were dropped because they failed the reassembly sanity check. Reassembled GRE encapsulated packets are composed of two or more GRE encapsulated fragments. This field is related to the previous statistic.
Packets failed GRE encapsulation	Number of GRE packets that are dropped by the WAE because they could not be redirected due to problems while encapsulating the packet with a GRE header.
Packets dropped due to invalid fwd method	Number of GRE packets that are dropped by the WAE because it was redirected using GRE but the WCCP service was configured for Layer 2 redirection.
Packets dropped due to insufficient memory	Number of GRE packets that are dropped by the WAE due to the failure to allocate additional memory resources required to handle the GRE packet.
Packets bypassed, no conn at all	Number of packets that failed to be associated with an existing flow because no TCP port was listening. WCCP can also handle asymmetric packet flows and always maintains a consistent mapping of web servers to caches regardless of the number of switches or routers used in a WCCP service group (up to 32 routers or switches communicating with up to 32 WAEs in a cluster).
Packets bypassed, no pending connection	Number of packets that failed to be associated with a pending connection because the initial handshake was not completed.

Table 3-87 Field Descriptions for the *show statistics wccp gre* Command (continued)

Field	Description
Packets due to clean wccp shutdown	Number of connection flows that are bypassed due to a clean WCCP shutdown. During a proper shutdown of WCCP, the WAE continues to service the flows it is handling but starts to bypass new flows. When the number of flows goes down to zero, the WAE takes itself out of the cluster by having its buckets reassigned to other WAEs by the lead WAE.
Packets bypassed due to bypass-list lookup	Number of connection flows that are bypassed due to a bypass list entry. When the WAE receives an error response from an origin server, it adds an entry for the server to its bypass list. When it receives subsequent requests for the content residing on the bypassed server, it redirects packets to the bypass gateway. If no bypass gateway is configured, then the packets are returned to the redirecting Layer 4 switch.
Packets received with client IP addresses	Number of packets that are associated to a connection flow that is being spoofed. By spoofing a client's IP address, the WAE can receive packets with the client IP (which is different from the WAE's own IP address) and send the packet to the correct application that is waiting for the packet.
Conditionally Accepted connections	Number of connection flows that are accepted by the WAE due to the conditional accept feature.
Conditionally Bypassed connections	Number of connection flows that are bypassed by the WAE due to the conditional accept feature.
Packets dropped due to received on loopback	Number of packets that were dropped by the WCCP L2 intercept layer because they were received on the loopback interface but were not destined to a local address of the device. There is no valid or usable route for the packet.
Packets w/WCCP GRE received too small	Number of packets transparently intercepted by the WCCP-enabled router at Layer 2 and sent to the WAE that need to be fragmented for the packets to be redirected using GRE. The WAE drops the packets since it cannot encapsulate the IP header.
Packets dropped due to IP access-list deny	Number of packets that are dropped by the WAE when an IP access list that the WAE applies to WCCP GRE encapsulated packets denies access to WCCP applications (the wccp access-list command).
Packets fragmented for bypass	Number of GRE packets that do not contain enough data to hold an IP header.
Packet pullups needed	Number of times a packet had to be consolidated as part of its processing. Consolidation is required when a packet is received as fragments and the first fragment does not contain all the information needed to process it.
Packets dropped due to no route found	Number of packets that are dropped by the WAE because it cannot find the route.

Related Commands[\(config\) wccp access-list](#)[\(config\) wccp flow-redirect enable](#)

(config) wccp router-list
(config) wccp shutdown
(config) wccp tcp-promiscuous
(config) wccp tcp-promiscuous

show statistics windows-domain

To display Windows domain server information for a WAAS device, use the **show statistics windows-domain** EXEC command.

show statistics windows-domain

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines Use the **show statistics windows-domain** EXEC command to view the Windows domain server statistics, then clear the counters for these statistics by entering the **clear statistics windows-domain** EXEC command.

Examples [Table 3-88](#) describes the fields shown in the **show statistics windows-domain** display.

Table 3-88 *Field Descriptions for the show statistics windows-domain Command*

Field	Description
Windows Domain Statistics	
Authentication	
Number of access requests	Number of access requests.
Number of access deny responses	Number of access deny responses.
Number of access allow responses	Number of access allow responses.
Authorization	
Number of authorization requests	Number of authorization requests.
Number of authorization failure responses	Number of authorization failure responses.

Table 3-88 *Field Descriptions for the show statistics windows-domain Command (continued)*

Field	Description
Number of authorization success responses	Number of authorization success responses.
Accounting	
Number of accounting requests	Number of accounting requests.
Number of accounting failure responses	Number of accounting failure responses.
Number of accounting success responses	Number of accounting success responses.

Related Commands[windows-domain](#)[\(config\) windows-domain](#)

show sysfs volumes

To display system file system (sysfs) information for a WAAS device, use the **show sysfs volumes** EXEC command.

show sysfs volumes

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines The system file system (sysfs) stores log files, including transaction logs, syslogs, and internal debugging logs. It also stores system image files and operating system files.

Examples [Table 3-89](#) describes the fields shown in the **show sysfs volumes** display.

Table 3-89 Field Descriptions for the show sysfs volumes Command

Field	Description
sysfs 00–04	System file system and disk number.
/local/local1–5	Mount point of the volume.
nnnnnnKB	Size of the volume in kilobytes.
nn% free	Percentage of free space in the SYSFS partition.

Related Commands [disk](#)
[\(config\) disk error-handling](#)

show tacacs

To display TACACS+ authentication protocol configuration information for a WAAS device, use the **show tacacs EXEC** command.

show tacacs

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Examples [Table 3-90](#) describes the fields shown in the **show tacacs** display.

Table 3-90 Field Descriptions for the show tacacs Command

Field	Description
Login Authentication for Console/Telnet Session	Indicates whether TACACS+ server is enabled for login authentication.
Configuration Authentication for Console/Telnet Session	Indicates whether TACACS+ server is enabled for authorization or configuration authentication.
TACACS+ Configuration	TACACS+ server parameters.
TACACS+ Authentication	Indicates whether TACACS+ authentication is enabled on the the WAAS device.
Key	Secret key that the WAE 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 WAAS device waits for a response from the specified TACACS+ authentication server before declaring a timeout.
Retransmit	Number of times that the WAAS device is to retransmit its connection to the TACACS+ if the TACACS+ timeout interval is exceeded.

Table 3-90 *Field Descriptions for the show tacacs Command (continued)*

Field	Description
Password type	Mechanism for password authentication. By default, the Password Authentication Protocol (PAP) is the mechanism for password authentication.
Server	Hostname or IP address of the TACACS+ server.
Status	Indicates whether server is the primary or secondary host.

Related Commands[clear](#)[show statistics tacacs](#)[show tacacs](#)[\(config\) tacacs](#)

show tcp

To display TCP configuration information for a WAAS device, use the **show tcp** EXEC command.

show tcp

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Examples [Table 3-91](#) describes the fields shown in the **show tcp** display. This command displays the settings configured with the **tcp** global configuration command.

Table 3-91 Field Descriptions for the show tcp Command

Field	Description
TCP Configuration	
TCP keepalive timeout XX sec	Length of time that the WAAS device is set to keep a connection open before disconnecting.
TCP keepalive probe count X	Number of times the WAAS device will retry a connection before the connection is considered unsuccessful.
TCP keepalive probe interval XX sec	Length of time (in seconds) that the WAAS device is set to keep an idle connection open.
TCP explicit congestion notification disabled	Configuration status of the TCP explicit congestion notification feature. Values are enabled or disabled.
TCP cwnd base value X	Value (in segments) of the send congestion window.
TCP initial slowstart threshold value X	Threshold (in segments) for slow start.
TCP increase (multiply) retransmit timer by X	Number of times set to increase the length of the retransmit timer base value.
TCP memory_limit	
Low water mark	Lower limit (in MB) of memory pressure mode, below which TCP enters into normal memory allocation mode.

Table 3-91 *Field Descriptions for the show tcp Command (continued)*

Field	Description
High water mark (pressure)	Upper limit (in MB) of normal memory allocation mode, beyond which TCP enters into memory pressure mode.
High water mark (absolute)	Absolute limit (in MB) on TCP memory usage.

Related Commands[clear](#)[show statistics tcp](#)[\(config\) tcp](#)

show tech-support

To view information necessary for Cisco's TAC to assist you, use the **show tech-support EXEC** command.

show tech-support [page]

Syntax Description	page (Optional) Displays output page by page.
Defaults	No default behavior or values
Command Modes	EXEC
Device Modes	application-accelerator replication-accelerator central-manager
Usage Guidelines	Use this command to view system information necessary for TAC to assist you with a WAAS device. We recommend that you log the output to a disk file. (See the “(config) logging” command.)
Examples	The following example displays technical support information:



Note

Because the **show tech-support** command output can be long, excerpts are shown in this example.

```
WAE# show tech-support
----- version and hardware -----

Cisco Wide Area Application Services Software (WAAS)
Copyright (c) 1999-2006 by Cisco Systems, Inc.
...
Version: ce510-4.0.0.180

Compiled 18:08:17 Feb 16 2006 by cnbuild

System was restarted on Fri Feb 17 23:09:53 2006.
The system has been up for 5 weeks, 3 days, 2 hours, 9 minutes, 49 seconds.

CPU 0 is GenuineIntel Intel(R) Celeron(R) CPU 2.40GHz (rev 2) running at 2401MHz
.
Total 1 CPU.
512 Mbytes of Physical memory.
...
BIOS Information:
Vendor                : IBM
Version               : -[PLEC52AUS-C.52]-
```

```

Rel. Date                : 05/19/03
...
List of all disk drives:
Physical disk information:

    disk00: Normal                (IDE disk)                76324MB( 74.5GB)
    disk01: Normal                (IDE disk)                76324MB( 74.5GB)

Mounted filesystems:

MOUNT POINT      TYPE      DEVICE                SIZE      INUSE      FREE      USE%
/                 root      /dev/root            31MB      26MB      5MB      83%
/sw              internal  /dev/md0             991MB     430MB     561MB    43%
/swstore         internal  /dev/md1             991MB     287MB     704MB    28%
/state          internal  /dev/md2             3967MB    61MB     3906MB   1%
/disk00-04      CONTENT  /dev/md4             62539MB   32MB     62507MB  0%
/local/local1   SYSFS    /dev/md5             3967MB    197MB    3770MB   4%
.../local1/spool PRINTSPOOL /dev/md6             991MB     16MB     975MB    1%

Software RAID devices:

DEVICE NAME      TYPE      STATUS                PHYSICAL DEVICES AND STATUS
/dev/md0         RAID-1   NORMAL OPERATION     disk00/00[GOOD] disk01/00[GOOD]
/dev/md1         RAID-1   NORMAL OPERATION     disk00/01[GOOD] disk01/01[GOOD]
/dev/md0         RAID-1   NORMAL OPERATION     disk00/00[GOOD] disk01/00[GOOD]
/dev/md1         RAID-1   NORMAL OPERATION     disk00/01[GOOD] disk01/01[GOOD]
/dev/md2         RAID-1   NORMAL OPERATION     disk00/02[GOOD] disk01/02[GOOD]
...
Currently content-fileSYSTEMS RAID level is not configured to change.

----- running configuration -----

! WAAS version 4.0.0
!
!
...
----- processes -----

CPU average usage since last reboot:
  cpu: 0.00% User,  1.79% System,  3.21% User(nice),  95.00% Idle
-----
PID  STATE  PRI  User  T   SYS  T   COMMAND
-----
   1   S     0   20138 21906 (init)
   2   S     0     0     0 (migration/0)
   3   S    19     0     0 (ksoftirqd/0)
   4   S   -10     0     0 (events/0)
   5   S   -10     0     0 (khelper)
  17   S   -10     0     0 (kacpid)
  93   S   -10     0     0 (kblockd/0)
...

```

Related Commands

[show version](#)
[show hardware](#)
[show disks details](#)
[show running-config](#)

show processes
show processes memory
show memory
show interface
show cdp entry
show cdp neighbors
show statistics weep
show alarms all
show statistics tfo
show statistics tfo application
show statistics tfo saving
show statistics tfo pass-through
show statistics tfo peer
show tfo auto-discovery
show tfo status
show tfo accelerators
show tfo bufpool accounting
show policy-engine status
show policy-engine application
show statistics dre
show statistics dre peer
show statistics tcp
show statistics ip
show statistics icmp
show standby
show statistics netstat
show disks SMART-info
show disks SMART-info details
show disks failed-sectors

show telnet

To display Telnet services configuration for a WAAS device, use the **show telnet** EXEC command.

show telnet

Syntax Description This command has no arguments or keywords.

Defaults Enabled

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Examples The following example displays whether or not Telnet is enabled on the WAAS device:

```
WAE# show telnet  
telnet service is enabled
```

Related Commands [telnet](#)
[\(config\) telnet enable](#)
[\(config\) exec-timeout](#)

show tfo accelerators

To display Traffic Flow Optimization (TFO) accelerators information for a WAE, use the **show tfo accelerators EXEC** command.

show tfo accelerators

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Device Modes application-accelerator

Examples The following example displays TFO accelerator information for the WAE:

```
WAE# show tfo accelerators
Name: TFO                State: Registered, Handling Level: 100%
  Keepalive timeout: 3.0 seconds, Session timeouts: 0, Total timeouts: 0
  Last keepalive received 00.5 Secs ago
  Last registration occurred 11:21:43:38.4 Days:Hours:Mins:Secs ago
Name: EPM                State: Registered, Handling Level: 100%
  Keepalive timeout: 5.0 seconds, Session timeouts: 0, Total timeouts: 0
  Last keepalive received 00.2 Secs ago
  Last registration occurred 11:21:43:36.7 Days:Hours:Mins:Secs ago
Name: CIFS               State: Not Registered, Handling Level: 0%
  Keepalive timeout: 0.0 seconds, Session timeouts: 0, Total timeouts: 0
  Last keepalive received -Never-
  Last Registration occurred -Never-
```

Related Commands [show tfo auto-discovery](#)

[show tfo bufpool](#)

[show tfo connection](#)

[show tfo filtering](#)

[show tfo status](#)

show tfo auto-discovery

To display Traffic Flow Optimization (TFO) auto-discovery statistics for a WAE, use the **show tfo auto-discovery EXEC** command.

```
show tfo auto-discovery [blacklist {entries [netmask netmask] [|] statistics [|] } [list] [|] {begin
regex [regex] | exclude regex [regex] | include regex [regex] }
```

Syntax Description		
blacklist	(Optional)	Displays the blacklist servers table.
entries		Displays all of the entries in the auto-discovery blacklist server table.
netmask		Displays the network mask to filter the table output.
<i>netmask</i>		Network mask (A.B.C.D/) for which you want to display the matching addresses.
statistics		Displays the auto-discovery blacklist server table management statistics.
list	(Optional)	Lists TCP flows that the WAE is currently optimizing or passing through.
 	(Optional)	Output modifier.
begin		Begins with the line that matches the regular expression.
<i>regex</i>		Regular expression to match. You can enter multiple expressions.
exclude		Excludes lines that match the regular expression.
include		Includes lines that match the regular expression.

Command Modes EXEC

Device Modes application-accelerator

Examples The following example displays TFO auto-discovery statistics for the WAE:

```
WAE# show tfo auto-discovery
Auto discovery structure:
  Allocation Failure:                0
  Allocation Success:                6615
  Deallocations:                    6615
  Timed Out:                         0
Auto discovery table:
  Bucket Overflows:                 0
  Table Overflows:                  0
  Entry Adds:                       6615
  Entry Drops:                      6615
  Entry Count:                      0
  Lookups:                          6624
Bind hash add failures:              0
Route Lookup:
  Failures:                         0
  Success:                           0
Socket:
  Allocation failures:               0
  Accept pair allocation failures:    0
```

```

        Unix allocation failures:                0
        Connect lookup failures:                0
Packets:
        Memory allocation failures:             0
        Total Sent:                             6624
        Total Received:                         13228
        Incorrect length or checksum received:  0
        Invalid filtering tuple received:       0
        Received for dead connection:           0
        Ack dropped in synack received state:   0
        Non Syn dropped in nostate state:       0
Auto discovery failure:
        No peer or asymmetric route:           6604
        Insufficient option space:              0
        Invalid connection state:              0
        Missing Ack conf:                      0
Auto discovery success TO:
        Internal server:                        0
        External server:                       0
Auto discovery success FOR:
        Internal client:                       0
        External client:                       0
Auto discovery success SYN retransmission:
        Zero retransmit:                       0
        One retransmit:                        0
        Two+ retransmit:                       0
Auto discovery Miscellaneous:
        Intermediate device:                   0
        RST received:                          0
        SYNs found with our device id:         0
        SYN retransmit count resets:           0

```

Related Commands

[show statistics tfo](#)
[show tfo accelerators](#)
[show tfo bufpool](#)
[show tfo connection](#)
[show tfo filtering](#)
[show tfo status](#)

show tfo bufpool

To display Traffic Flow Optimization (TFO) buffer pool information for a WAE, use the **show tfo bufpool EXEC** command.

```
show tfo bufpool { accounting | from-index index | owner-connection conn-id |
owner-module { RELib | tcpproxy } [from-index index | owner-connection conn-id |
state { free | in-use } [from-index index | owner-connection conn-id | to-index index] |
to-index index] | state { free | in-use } [from-index index | owner-connection conn-id |
to-index index] | to-index index}
```

Syntax Description		
accounting		Displays the buffer pool overall usage.
from-index		Displays the starting index of the buffer units to be displayed.
<i>index</i>		Index of a buffer unit (0–4294967295).
owner-connection		Displays the owner connection of the buffer units.
<i>conn-id</i>		Connection ID (0–4294967295).
owner-module		Displays the owner module of the buffer units.
RELlib		Shows the buffer units owned by the RE-library.
tcpproxy		Shows the buffer units owned by the TCP proxy.
state		Displays the state (free or used) of the buffer units.
free		Shows the free buffer units.
in-use		Shows the buffer units in use.
to-index		Displays the ending index of the buffer units to be displayed.

Command Modes EXEC

Device Modes application-accelerator

Examples The following example displays TFO buffer pool information for the WAE:

```
WAE# show tfo bufpool accounting
Total buffer pool size: 80740352 bytes
Free buffer: 80740352 bytes, in 78848 units (unit size: 1024 bytes)
Used buffer: 0 bytes, in 0 units
  Buffer usage by module:
    Tcpproxy: using 0 bytes, in 0 units
    RELib: using 0 bytes, in 0 units
    LZlib: using 0 bytes, in 0 units
  Buffer usage by connection:
```

Related Commands

- [show tfo accelerators](#)
- [show tfo auto-discovery](#)
- [show tfo connection](#)

[show tfo filtering](#)
[show tfo status](#)
[show statistics tfo](#)

show tfo connection

To display Traffic Flow Optimization (TFO) connection information for a WAE, use the **show tfo connection EXEC** command.

```
show tfo connection [[summary] | [client-ip host-address | client-port port | peer-id mac |
server-ip host-address | server-port port]]
```

Syntax Description		
summary	(Optional)	Displays a summary list of connections.
client-ip	(Optional)	Source IP address.
<i>host-address</i>		Hostname or IP address.
client-port	(Optional)	IP address of the source client.
<i>port</i>		Port number on the client or server.
peer-id	(Optional)	Displays the connection statistics for a specific peer.
<i>mac</i>		MAC address of a peer host.
server-ip	(Optional)	IP address of the destination server.
server-port	(Optional)	Destination port number.

Command Modes EXEC

Device Modes application-accelerator

Usage Guidelines Using this command without options displays detailed information about each of the TFO connections for a WAE. To display a summary list of the connections, use the **summary** option.

For the listed connections that have the F, D or L optimization policy, you can find additional information on DRE statistics by using the **show statistics dre connection** command with the **id** option to identify a specific connection id.

Examples The following example displays a summary of TFO optimized connections for the WAE:

```
WAE# show tfo connection summary
```

```
Optimized Connection List
Policy summary order: Our's, Peer's, Negotiated, Applied
F: Full optimization, D: DRE only, L: LZ Compression, T: TCP Optimization

Local-IP:Port      Remote-IP:Port      ConId  PeerId          Policy
10.77.156.99:59950 10.77.156.106:10005 21     00:11:25:ac:3e:04 F,F,F,F
10.77.156.99:59951 10.77.156.106:10007 22     00:11:25:ac:3e:04 F,F,F,F
10.77.156.99:59952 10.77.156.106:10008 23     00:11:25:ac:3e:04 F,F,F,F
10.77.156.99:59953 10.77.156.106:10009 24     00:11:25:ac:3e:04 F,F,F,F
10.77.156.99:59954 10.77.156.106:10010 25     00:11:25:ac:3e:04 F,F,F,F
```

Related Commands

- show statistics dre connection
- show statistics tfo
- show tfo accelerators
- show tfo auto-discovery
- show tfo bufpool
- show tfo filtering
- show tfo status

show tfo egress-methods connection

To display detailed egress method-related information about the connection segments for a WAE, use the **show tfo egress-methods connection EXEC** command.

```
show tfo egress-methods connection [local-ip ipaddress | local-port port | remote-ip ipaddress | remote-port port]
```

Syntax Description		
egress-methods		Shows detailed information on the egress methods.
connection		Shows the egress method-related statistics for the connection.
local-ip		(Optional) Local IP address for the connection tuple.
<i>ipaddress</i>		IP address.
local-port		(Optional) Local port number for the connection tuple.
<i>port</i>		Port number.
remote-ip		(Optional) Remote IP address for the connection tuple.
<i>ipaddress</i>		IP address.
remote-port		(Optional) Remote port number for the connection tuple.
<i>port</i>		Port number.

Command Modes EXEC

Device Modes application-accelerator

Usage Guidelines Using this command without options displays detailed information about each of the TFO connections for a WAE.

This command displays egress method-related information about connection segments in an environment where the data flow from start-point to end-point is being transparently intercepted by multiple devices. A connection tuple represents one segment of an end-to-end connection that is intercepted by a WAAS device (WAE) for processing.

For example, a single client-server connection may have three segments (see [Figure 3-1](#)):

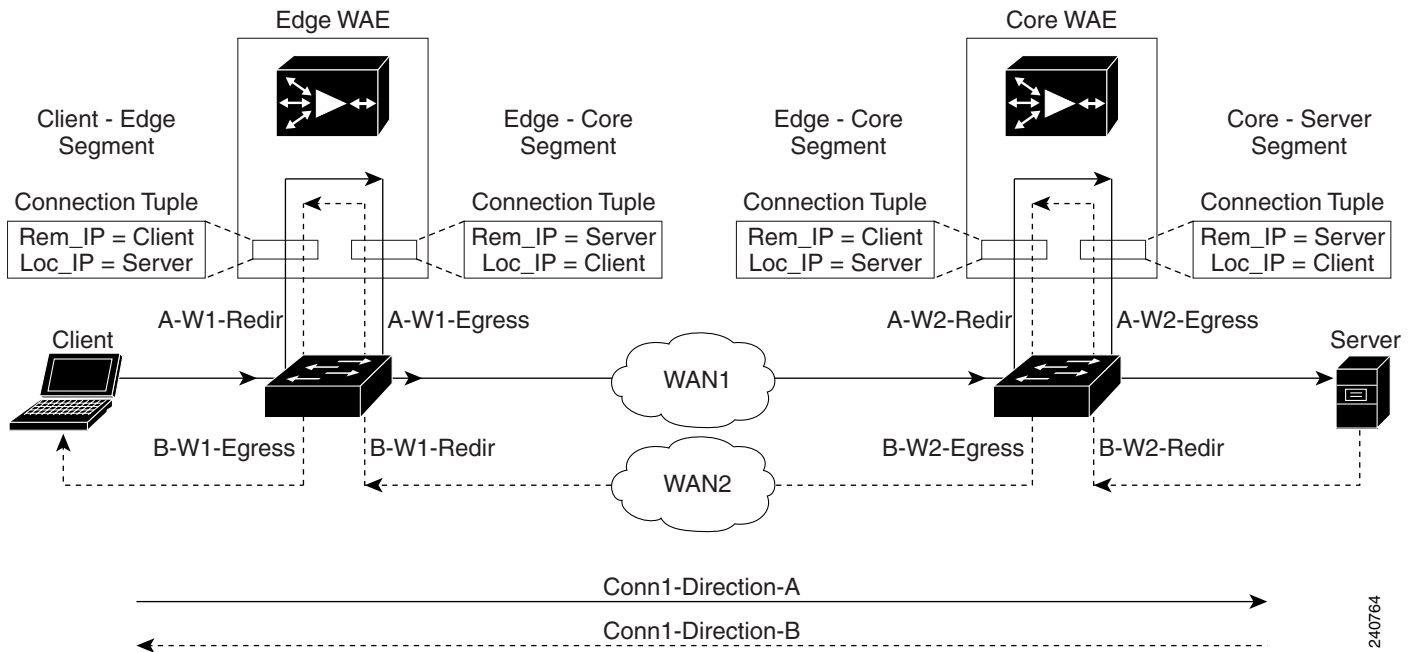
- Between the client and the Edge WAE
- Between the Edge WAE and the Core WAE
- Between the Core WAE and the server

In this example, the Edge WAE has two connection tuples for the two segments that it participates in:

- One connection tuple to represent the Client—Edge segment
- One connection tuple to represent the Edge—Core segment

In the show output, these two connection tuples appear as TUPLE and MATE. (See [Table 3-92](#).) The important information to view is the local and remote IP address of the connection tuple and not whether it is marked as TUPLE or MATE.

Figure 3-1 Topology with Three Segments and Corresponding Connection Tuples



Because the WAAS device is transparent to both the client-end of the connection and the server-end of the connection, the local IP address for a connection tuple depends on the segment in the end-to-end topology.

For example, when WAAS intercepts a packet from the client, this packet enters the connection tuple that represents the Client—Edge segment. On this tuple, the WAAS device appears to the client as though it were the server: the local IP address in this connection tuple is the IP address of the server, while the remote IP address in this connection tuple is that of the client. Similarly, when the Edge WAE sends data to the client, the packet egresses from this connection tuple as though it were coming from the server.

When WAAS sends a packet to the server, the packet egresses from the connection tuple that represents the Edge—Core segment. On this tuple, the WAAS device appears to the server as though it were the client: the local IP address in the connection tuple is the IP address of the client, while the remote IP address in this connection tuple is that of the server. Similarly, when the Edge WAE intercepts a packet from the Core WAE, the data in this connection tuple appears to be coming from the server.

Examples

Table 3-92 describes the fields shown in the `show tfo egress-methods connection` display.

Table 3-92 Field Descriptions for the `show tfo egress-methods connection` Command

Field	Description
TUPLE	
Local-IP:Port	IP address and port number of the local device in the connection tuple.
Remote-IP:Port	IP address and port number of the remote device in the connection tuple.

Table 3-92 *Field Descriptions for the show tfo egress-methods connection Command (continued)*

Field	Description
MATE	
Local-IP:Port	IP address and port number of the local device in the mate connection tuple.
Remote-IP:Port	IP address and port number of the remote device in the mate connection tuple.
Egress method	Egress method being used.
WCCP Service Bucket	WCCP service number and bucket number for the connection tuple and mate connection tuple.
Tuple Flags	Flags for intercept method and intercept mechanism. This field may contain the following values: WCCP or NON-WCCP as the intercept method; L2 or GRE as the intercept mechanism; or PROT showing whether this tuple is receiving packets through the flow protection mechanism.
Intercepting device (ID)	
ID IP address	IP address of the intercepting device.
ID MAC address	MAC address of the intercepting device.
ID IP address updates	Number of IP address changes for the intercepting device.
ID MAC address updates	Number of MAC address changes for the intercepting device.
Memory address	Memory address.

Each time a packet enters the connection tuple, the intercepting device IP address or MAC address is recorded. The updates field in the command output indicates whether the intercepting device IP address or intercepting device MAC address has been recorded. If, for example, the ID MAC address updates field is zero (0), the MAC address was not recorded, and the ID MAC address field will be blank. The recorded intercepting device information is used when a packet egresses from the WAE.

If the egress method for the connection tuple is IP forwarding, the updates fields are always zero (0) because the intercepting device information is neither required nor recorded for the IP forwarding egress method.

If the intercept method is WCCP GRE redirect and the egress method is WCCP GRE, only the IP address field is updated and recorded. The MAC address information is neither required nor recorded because the destination address in the GRE header only accepts an IP address.

If the intercept method is WCCP L2 redirect and the egress method is WCCP GRE, both the MAC address and the IP address fields are updated and recorded because incoming WCCP L2 packets contain only a MAC header. The MAC address is recorded and the intercepting device IP address is derived from a reverse ARP lookup and is then recorded, also. When packets egress the connection tuple in this scenario, they will have a GRE header with the destination IP address of the intercepting device that was recorded.

The updates count may be greater than 1 in certain topologies. For example, in a redundant router topology, where for the same direction of the same connection between two hosts, packets may be coming in from different intercepting routers. Each time a packet comes in, the intercepting device MAC or IP address is compared against the last recorded address. If the MAC or IP address has changed, the updates field is incremented and the new MAC or IP address is recorded.

Related Commands [show egress-methods](#)
 [show statistics tfo](#)

show tfo filtering

To display information about the incoming and outgoing TFO flows that the WAE currently has, use the **show tfo filtering** EXEC command.

```
show tfo filtering [list [l {begin regex [regex] | exclude regex [regex] | include regex [regex] }]] [l
{begin regex [regex] | exclude regex [regex] | include regex [regex]}]
```

Syntax Description		
list	(Optional) Lists TCP flows that the WAE is currently optimizing or passing through.	
l	(Optional) Output modifier.	
begin	Begins with the line that matches the regular expression.	
<i>regex</i>	Regular expression to match. You can enter multiple expressions.	
exclude	Excludes lines that match the regular expression.	
include	Includes lines that match the regular expression.	

Command Modes EXEC

Device Modes application-accelerator

Usage Guidelines This command lists TCP flows that the WAE is currently optimizing. It also includes TCP flows that are not being optimized but that are being passed through by the WAE. A “P” in the State column indicates a passed through flow.

Examples The following examples display TFO connection information for the WAE:

```
WAE# show tfo filtering
Number of filtering tuples:                2
Packets dropped due to ttl expiry:         0
Packets dropped due to bad route:          0
Syn packets dropped with our own id in the options: 0
Syn packets received and dropped on estab. conn: 0
Syn-Ack packets received and dropped on estab. conn: 0
Packets recvd on in progress conn. and not handled: 0
Packets dropped due to peer connection alive: 0
Packets dropped due to invalid TCP flags:  0
Packets dropped by FB packet input notifier: 0
Packets dropped by FB packet output notifier: 0
Number of errors by FB tuple create notifier: 0
Number of errors by FB tuple delete notifier: 0
Dropped WCCP GRE packets due to invalid WCCP service: 0
Dropped WCCP L2 packets due to invalid WCCP service: 0
```

```
WAE# show tfo filtering list
E: Established, S: Syn, A: Ack, F: Fin, R: Reset
s: sent, r: received, O: Options, P: Passthrough
B: Bypass, T: Timedout, C: Closed
```

Local-IP:Port	Remote-IP:Port	Tuple(Mate)	State
10.99.11.200:1398	10.99.22.200:80	0xcba709c0(0xcba70a00)	E
10.99.11.200:1425	10.99.22.200:80	0xcba70780(0xcba707c0)	E
10.99.11.200:1439	10.99.22.200:5222	0xcba703c0(0xcba70b40)	Sr
10.99.11.200:1440	10.99.22.200:5222	0xcba70400(0xcba70440)	Sr
10.99.22.200:1984	10.99.11.200:80	0xcba70600(0xcba70640)	E
10.99.22.200:1800	10.99.11.200:23	0xcba70480(0x0)	PE
10.99.11.200:1392	10.99.22.200:80	0xcba70f80(0x0)	E
10.99.22.200:20	10.99.11.200:1417	0xcba701c0(0xcba70180)	E
10.99.11.200:1417	10.99.22.200:20	0xcba70180(0x0)	E
10.99.22.200:1987	10.99.11.200:80	0xcba70240(0xcba70200)	E
10.99.11.200:1438	10.99.22.200:5222	0xcba70900(0xcba70580)	Sr
10.99.22.200:1990	10.99.11.200:80	0xcba70100(0xcba70140)	E
10.99.22.200:80	10.99.11.200:1426	0xcba70740(0xcba70700)	E
10.99.22.200:80	10.99.11.200:1425	0xcba707c0(0xcba70780)	E
10.99.22.200:1985	10.99.11.200:80	0xcba70a40(0xcba70a80)	E
10.99.22.200:80	10.99.11.200:1410	0xcba70500(0xcba70540)	E
10.99.22.200:80	10.99.11.200:1398	0xcba70a00(0xcba709c0)	E
10.99.22.200:80	10.99.11.200:1392	0xcba70f40(0xcba70f80)	E
10.0.19.5:54247	10.1.242.5:80	0xc9e5b400(0xc9e5b100)	ED

**Note**

Some state descriptions are missing from the legend. D = Done. The “ED” state occurs when one socket in the pair is closed (D), but the mate is still established (E).

Related Commands

[show tfo accelerators](#)
[show tfo auto-discovery](#)
[show tfo bufpool](#)
[show tfo connection](#)
[show tfo status](#)

show tfo status

To display global Traffic Flow Optimization (TFO) status information for a WAE, use the **show tfo status** EXEC command.

show tfo status

Command Modes EXEC

Device Modes application-accelerator

Examples The following example displays global TFO status information for the WAE:

```
WAE# show tfo status
Optimization Status:
  Configured: optimize full
  Current: optimize full
TFO is up since Sat Feb 25 13:18:51 2006
TFO is functioning normally.
Total number of optimized connections since start:      0
Number of active connections:                          0
Total number of peers:                                 0
```

Related Commands

- [show statistics tfo](#)
- [show tfo accelerators](#)
- [show tfo auto-discovery](#)
- [show tfo bufpool](#)
- [show tfo connection](#)
- [show tfo filtering](#)

show tfo synq

To display the cumulative statistics for the SynQ module, use the **show tfo synq** EXEC command.

```
show tfo synq [list [| {begin regex [regex] | exclude regex [regex] | include regex [regex] }]] [| {begin
regex [regex] | exclude regex [regex] | include regex [regex] }
```

Syntax Description		
list	(Optional)	Lists the connections tracked in the SynQ module.
	(Optional)	Output modifier.
begin		Begins with the line that matches the regular expression.
<i>regex</i>		Regular expression to match. You can enter multiple expressions.
exclude		Excludes lines that match the regular expression.
include		Includes lines that match the regular expression.

Command Modes EXEC

Device Modes application-accelerator

Usage Guidelines Use the **show tfo synq list** command to list connections that are currently being tracked in the SynQ module.

Examples The following example displays the output for the **show tfo synq** command:

```
WWAE# show tfo synq
Synq structures allocations success:          0
Synq structures allocations failure:         0
Synq structures deallocations:              0
Synq table entry adds:                      0
Synq table entry drops:                     0
Synq table entry lookups:                   0
Synq table overflows:                       0
Synq table entry count:                     0
Packets received by synq:                   0
Packets received with invalid filtering tuple: 0
Non-syn packets received:                   0
Locally originated/terminating syn packets received: 0
Retransmitted syn packets received while in Synq: 0
Synq user structure allocations success:     0
Synq user structure allocations failure:     0
Synq user structure deallocations:          0
```


show transaction-logging

To display the transaction log configuration settings and a list of archived transaction log files for a WAE, use the **show transaction-logging** EXEC command.

show transaction-logging

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator

Usage Guidelines Use the **show transaction-log** or **show transaction-logging** EXEC commands to display information about the current configuration of transaction logging on a WAE. Both of these EXEC commands display the same output. Transaction log file information is displayed for HTTP and WMT MMS caching proxy transactions and TFTP and ICAP transactions.

**Note**

For security reasons, passwords are never displayed in the output of the **show transaction-log** EXEC command.

Examples The following example displays information about the current configuration of transaction logging on a WAE:

```
WAAE# show transaction-logging
Transaction log configuration:
-----
TFO Logging is disabled.
TFO Archive interval: every-day every 1 hour
TFO Maximum size of archive file: 2000000 KB

TFO logging to remote syslog host is disabled.
TFO remote syslog host is not configured.
TFO facility is the default "*" which is "user".

Exporting files to ftp servers is disabled.
```

Related Commands [clear transaction-log \(config\) transaction-logs](#)

show user

To display user identification number and username information for a particular user of a WAAS device, use the **show user EXEC** command.

```
show user {uid number | username name}
```

Syntax Description

uid	Displays user information based on the identification number of the user.
<i>number</i>	Identification number (0–65535).
username	Displays user information based on the name of the user.
<i>name</i>	Name of user.

Command Default

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator
 replication-accelerator
 central-manager

Examples

[Table 3-93](#) describes the fields shown in the **show user** display.

Table 3-93 Field Descriptions for the show user Command

Field	Description
Uid	User ID number.
Username	Username.
Password	Login password. This field does not display the actual password.
Privilege	Privilege level of the user.
Configured in	Database in which the login authentication is configured.

Related Commands

clear
show users administrative
(config) username

show users administrative

To display users with administrative privileges or users that have been locked out, use the **show users administrative** EXEC command.

show users administrative {history | logged-in | locked-out}

Syntax Description	history	Displays a list of users that had previously logged in to the appliance CLI.
	logged-in	Displays a list of users that are currently logged in to the appliance CLI.
	locked-out	Displays a list of users that are locked out of the CLI.

Defaults No default behavior or values

Command Modes EXEC

Device Modes
 application-accelerator
 replication-accelerator
 central-manager

Examples The following example displays a list of users that had logged in to an appliance in the past:

```
WAE# show users administrative history
<username> <line> <ip address/host> <login details>
<username> <line> <ip address/host> <login details>
<username> <line> <ip address/host> <login details>
```

Table 3-94 describes the fields shown in the **show users administrative history** display.

Table 3-94 Field Descriptions for the show users administrative history Command

Field	Description
Username	Users that have logged in to this appliance CLI during the historical period.
Line	Type of terminal used to access this appliance.
IP address/Host	IP address or hostname of the user that logged in to this appliance.
Login details	Day of the week, month, date, time, and whether or not the user is still logged in.

The following example displays a list of users that are currently logged in to an appliance:

```
WAE# show users administrative logged-in
<username> <line> <ip address/host> <login details>
<username> <line> <ip address/host> <login details>
```

```
<username> <line> <ip address/host> <login details>
```

Table 3-95 describes the fields shown in the **show users administrative logged-in** display.

Table 3-95 Field Descriptions for the **show users administrative logged-in** Command

Field	Description
Username	Users currently logged in to the appliance CLI.
Line	Type of terminal used to access this appliance.
IP address/Host	IP address or hostname of the user that is logged in to this appliance.
Login details	Day of week, month, date, and time that each user logged in.

The following example displays a list of users that are locked out of the appliance:

```
WAE# show users administrative locked-out
<username>
<username>
```

You can use the username data with the **clear users locked-out username** *username* EXEC mode command. See “clear users”.

Related Commands

clear

clear users

(config) username

show version

To display version information about the WAAS software that is running on the WAAS device, use the **show version EXEC** command.

show version [last | pending]

Syntax Description

last	Displays the version information for the last saved image.
pending	Displays the version information for the pending upgraded image.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator
 replication-accelerator
 central-manager

Examples

[Table 3-96](#) describes the fields shown in the **show version** display.

Table 3-96 Field Descriptions for the show version Command

Field	Description
Cisco Wide Area Application Services Software (WAAS) Copyright (c) year by Cisco Systems, Inc. Cisco Wide Area Application Services Software Release XXX (build bXXX month day year)	Software application, copyright, release, and build information.
Version	Version number of the software that is running on the device.
Compiled hour:minute:second month day year by cnbuild	Complete information for the software build.
System was restarted on day of week month day hour:minute:second year	Date and time that the system was last restarted.
The system has been up for X hours, X minutes, X seconds	Length of time the system has been running since the last reboot.

show wccp

To display Web Cache Connection Protocol (WCCP) information for a WAE, use the **show wccp** EXEC command.

```

show wccp wide-area-engines

show wccp flows {tcp-promiscuous} [summary]

show wccp gre

show wccp masks {tcp-promiscuous} [summary]

show wccp routers

show wccp services [detail]

show wccp slowstart {tcp-promiscuous} [summary]

show wccp status

```

Syntax	Description
wide-area-engines	Displays which WAEs are seen by which routers.
flows	Displays WCCP packet flows.
tcp-promiscuous	Displays TCP-PROMISCUOUS caching service packet flows.
summary	(Optional) Displays summarized information about TCP-PROMISCUOUS caching service packet flows.
gre	Displays WCCP generic routing encapsulation packet-related information.
masks	Displays WCCP mask assignments for a given service.
routers	Displays routers seen and not seen by this WAE.
services	Displays WCCP services configured.
detail	(Optional) Displays details of services.
slowstart	Displays WCCP slow-start state for the selected service.
status	Displays version of WCCP that is enabled and running.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator

Examples The following example shows the output of the **show wccp services** command:

```

WAE# show wccp services
Services configured on this File Engine

```

```
TCP Promiscuous 61
TCP Promiscuous 62
```

The following example is partial output from the **show wccp services detail** command:

```
WAE# show wccp services detail
Service Details for TCP Promiscuous 61 Service
  Service Enabled           : Yes
  Service Priority          : 34
  Service Protocol          : 6
  Application               : Unknown
  Service Flags (in Hex)   : 501
  Service Ports             :      0      0      0      0
                           :      0      0      0      0

  Security Enabled for Service : No
  Multicast Enabled for Service : No
  Weight for this Web-CE       : 0
  Negotiated forwarding method : GRE
  Negotiated assignment method : HASH
  Negotiated return method    : GRE
  Received Values:
  Source IP mask (in Hex)     : 0
  Destination IP mask (in Hex) : 0
  Source Port mask (in Hex)   : 0
  Destination Port mask (in Hex) : 0
  Calculated Values:
  Source IP mask (in Hex)     : 0
  Destination IP mask (in Hex) : 1741
  Source Port mask (in Hex)   : 0
  Destination Port mask (in Hex) : 0

Service Details for TCP Promiscuous 62 Service
  Service Enabled           : Yes
  Service Priority          : 34
  Service Protocol          : 6
  Application               : Unknown
  Service Flags (in Hex)   : 502
  Service Ports             :      0      0      0      0
                           :      0      0      0      0

  Security Enabled for Service : No
  Multicast Enabled for Service : No
  Weight for this Web-CE       : 0
  Negotiated forwarding method : GRE
  Negotiated assignment method : HASH
  Negotiated return method    : GRE
  Received Values:
  Source IP mask (in Hex)     : 0
  Destination IP mask (in Hex) : 0
  Source Port mask (in Hex)   : 0
  Destination Port mask (in Hex) : 0
  Calculated Values:
  Source IP mask (in Hex)     : 0
  Destination IP mask (in Hex) : 1741
  Source Port mask (in Hex)   : 0
  Destination Port mask (in Hex) : 0
```

The following example is the output from the **show wccp routers** command:

```
WAE# show wccp routers
Router Information for Service: TCP Promiscuous 61
  Routers Configured and Seeing this File Engine(1)
    Router Id      Sent To      Recv ID
    0.0.0.0        10.10.20.1    00000000
  Routers not Seeing this File Engine
```

```

10.10.20.1
Routers Notified of but not Configured
-NONE-
Multicast Addresses Configured
-NONE-
Router Information for Service: TCP Promiscuous 62
Routers Configured and Seeing this File Engine(1)
  Router Id      Sent To      Recv ID
  0.0.0.0        10.10.20.1   00000000
Routers not Seeing this File Engine
10.10.20.1
Routers Notified of but not Configured
-NONE-
Multicast Addresses Configured
-NONE-

```

The following example is the output from the **show wccp status** command:

```

WAE# show wccp status
WCCP version 2 is enabled and currently active

```

[Table 3-97](#) describes the fields shown in the **show wccp gre** display.

Table 3-97 Field Descriptions for the **show wccp gre** Command

Field	Description
Transparent GRE packets received	Total number of GRE packets received by the WAE, regardless of whether or not they have been intercepted by WCCP. GRE is a Layer 3 technique that allows packets to reach the WAE, even if there are any number of routers in the path to the WAE.
Transparent non-GRE packets received	Number of non-GRE packets received by the WAE, either using the traffic interception and redirection functions of WCCP in the router hardware at Layer 2 or Layer 4 switching (a Content Switching Module [CSM]) that redirects requests transparently to the WAE.
Transparent non-GRE packets passed through	Number of non-GRE packets transparently intercepted by a Layer 4 switch and redirected to the WAE.
Total packets accepted	Total number of packets that are transparently intercepted and redirected to the WAE to serve client requests for content.
Invalid packets received	Number of packets that are dropped either because the redirected packet is a GRE packet and the WCCP GRE header has invalid data or the IP header of the redirected packet is invalid.
Packets received with invalid service	Number of WCCP version 2 GRE redirected packets that contain an invalid WCCP service number.
Packets received on a disabled service	Number of WCCP version 2 GRE redirected packets that specify the WCCP service number for a service that is not enabled on the WAE. For example, an HTTPS request redirected to the WAE when the HTTPS-caching service (service 70) is not enabled.
Packets received too small	Number of GRE packets redirected to the WAE that do not contain the minimum amount of data required for a WCCP GRE header.
Packets dropped due to zero TTL	Number of GRE packets that are dropped by the WAE because the redirected packet's IP header has a zero TTL.

Table 3-97 Field Descriptions for the show wccp gre Command (continued)

Field	Description
Packets dropped due to bad buckets	Number of packets that are dropped by the WAE because the WCCP flow redirection could not be performed due to a bad mask or hash bucket determination. Note A bucket is defined as a certain subsection of the allotted hash assigned to each WAE in a WAE cluster. If only one WAE exists in this environment, it has 256 buckets assigned to it.
Packets dropped due to no redirect address	Number of packets that are dropped because the flow redirection destination IP address could not be determined.
Packets dropped due to loopback redirect	Number of packets that are dropped by the WAE when the destination IP address is the same as the loopback address.
Pass-through pkts dropped on assignment update	Number of packets that were targeted for TFO pass-through, but were dropped instead because the bucket was not owned by the device.
Connections bypassed due to load	Number of connection flows that are bypassed when the WAE is overloaded. When the overload bypass option is enabled, the WAE bypasses a bucket and reroutes the overload traffic. If the load remains too high, another bucket is bypassed, and so on, until the WAE can handle the load.
Packets sent back to router	Number of requests that are passed back by the WAE to the WCCP-enabled router from which the request was received. The router then sends the flow toward the origin web server directly from the web browser, which bypasses the WAE.
Packets sent to another WAE	Number of packets that are redirected to another WAE in the WCCP service group. Service groups consist of up to 32 WAEs and 32 WCCP-enabled routers. In both packet-forwarding methods, the hash parameters specify how redirected traffic should be load balanced among the WAEs in the various WCCP service groups.
GRE fragments redirected	Number of GRE packets received by the WAE that are fragmented. These packets are redirected back to the router.
GRE encapsulated fragments received	Number of GRE encapsulated fragments received by the WAE. The tcp-promiscuous service does not inspect port information and therefore the router or switch may GRE encapsulate IP fragments and redirect them to the WAE. These fragments are then reassembled into packets before being processed.
Packets failed encapsulated reassembly	Number of reassembled GRE encapsulated packets that were dropped because they failed the reassembly sanity check. Reassembled GRE encapsulated packets are composed of two or more GRE encapsulated fragments. This field is related to the previous statistic.
Packets failed GRE encapsulation	Number of GRE packets that are dropped by the WAE because they could not be redirected due to problems while encapsulating the packet with a GRE header.

Table 3-97 *Field Descriptions for the show wccp gre Command (continued)*

Field	Description
Packets dropped due to invalid fwd method	Number of GRE packets that are dropped by the WAE because it was redirected using GRE but the WCCP service was configured for Layer 2 redirection.
Packets dropped due to insufficient memory	Number of GRE packets that are dropped by the WAE due to the failure to allocate additional memory resources required to handle the GRE packet.
Packets bypassed, no conn at all	Number of packets that failed to be associated with an existing flow because no TCP port was listening. WCCP can also handle asymmetric packet flows and always maintains a consistent mapping of web servers to caches regardless of the number of switches or routers used in a WCCP service group (up to 32 routers or switches communicating with up to 32 WAEs in a cluster).
Packets bypassed, no pending connection	Number of packets that failed to be associated with a pending connection because the initial handshake was not completed.
Packets due to clean wccp shutdown	Number of connection flows that are bypassed due to a clean WCCP shutdown. During a proper shutdown of WCCP, the WAE continues to service the flows it is handling but starts to bypass new flows. When the number of flows goes down to zero, the WAE takes itself out of the cluster by having its buckets reassigned to other WAEs by the lead WAE.
Packets bypassed due to bypass-list lookup	Number of connection flows that are bypassed due to a bypass list entry. When the WAE receives an error response from an origin server, it adds an entry for the server to its bypass list. When it receives subsequent requests for the content residing on the bypassed server, it redirects packets to the bypass gateway. If no bypass gateway is configured, then the packets are returned to the redirecting Layer 4 switch.
Packets received with client IP addresses	Number of packets that are associated to a connection flow that is being spoofed. By spoofing a client's IP address, the WAE can receive packets with the client IP (which is different from the WAE's own IP address) and send the packet to the correct application that is waiting for the packet.
Conditionally Accepted connections	Number of connection flows that are accepted by the WAE due to the conditional accept feature.
Conditionally Bypassed connections	Number of connection flows that are bypassed by the WAE due to the conditional accept feature.
Packets dropped due to received on loopback	Number of packets that were dropped by the WCCP L2 intercept layer because they were received on the loopback interface but were not destined to a local address of the device. There is no valid or usable route for the packet.
Packets w/WCCP GRE received too small	Number of packets transparently intercepted by the WCCP-enabled router at Layer 2 and sent to the WAE that need to be fragmented for the packets to be redirected using GRE. The WAE drops the packets since it cannot encapsulate the IP header.

Table 3-97 Field Descriptions for the *show wccp gre* Command (continued)

Field	Description
Packets dropped due to IP access-list deny	Number of packets that are dropped by the WAE when an IP access list that the WAE applies to WCCP GRE encapsulated packets denies access to WCCP applications (the wccp access-list command).
Packets fragmented for bypass	Number of GRE packets that do not contain enough data to hold an IP header.
Packet pullups needed	Number of times a packet had to be consolidated as part of its processing. Consolidation is required when a packet is received as fragments and the first fragment does not contain all the information needed to process it.
Packets dropped due to no route found	Number of packets that are dropped by the WAE because it cannot find the route.

Related Commands

- (config) **wccp access-list**
- (config) **wccp flow-redirect enable**
- (config) **wccp router-list**
- (config) **wccp shutdown**
- (config) **wccp tcp-promiscuous**
- (config) **wccp version**

show windows-domain

To display Windows domain configuration information for a WAAS device, use the **show windows-domain EXEC** command.

show windows-domain

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Examples [Table 3-98](#) describes the fields shown in the **show windows-domain** display.

Table 3-98 Field Descriptions for the show windows-domain Command

Field	Description
Login Authentication for Console/Telnet Session:	Status of the primary login authentication method for the session: enabled or disabled.
Configuration Authentication for Console/Telnet Session: enabled (secondary)	Status of the secondary login authentication method for the session: enabled or disabled.
Windows domain Configuration:	Shows the Windows domain configuration settings.
Workgroup	Workgroup identification string.
Comment	Comment line.
Net BIOS	Windows NetBIOS name for the WAE.
Realm	Kerberos Realm (similar to the Windows domain name, except for Kerberos).
WINS Server	IP address of the WINS server.
Password Server	Kerberos server DNS name.
Security	Type of authentication configured, either “Domain” for NTLM or “ADS” for Kerberos.
Administrative groups	
Super user group	Active Directory(AD) group name. Users in this group have administrative rights.
Normal user group	AD group name. Users in this group have the normal/default privilege level in the WAE.

Related Commands

[windows-domain](#)

[\(config\) windows-domain](#)

shutdown

To shut down the WAAS device use the **shutdown** EXEC command.

shutdown [poweroff]

Syntax Description	poweroff	(Optional) Turns off the power after closing all applications and operating system.
---------------------------	-----------------	-------------------------------------------------------------------------------------

Defaults	No default behavior or values
-----------------	-------------------------------

Command Modes	EXEC
----------------------	------

Device Modes	application-accelerator replication-accelerator central-manager
---------------------	-----------------------------------------------------------------------

Usage Guidelines A controlled shutdown refers to the process of properly shutting down a WAAS device without turning off the power on the device. With a controlled shutdown, all of the application activities and the operating system are properly stopped on a WAE, but the power remains on. Controlled shutdowns of a WAAS device can help you minimize the downtime when the WAAS device is being serviced.



Caution

If a controlled shutdown is not performed, the WAAS file system can be corrupted. Rebooting the WAAS device takes longer if it was not properly shut down.



Note

A WAAS device cannot be powered on again through the WAAS software after a software poweroff. You must press the power button once on a WAAS device to bring it back online.

The **shutdown** EXEC command facilitates a proper shutdown for WAAS device, and is supported on all WAE hardware models. The **shutdown poweroff** command is also supported by all of the WAE hardware models as they support the ACPI.

The **shutdown** command closes all applications and stops all system activities, but keeps the power on. The fans continue to run and the power LED is on, indicating that the device is still powered on. The device console displays the following menu after the shutdown process is completed:

```
===== SHUTDOWN SHELL =====
System has been shut down.
```

You can

0. Power down system by pressing and holding power button
1. Reload system by software
2. Power down system by software

[1-2]?

The **shutdown poweroff** command closes all applications and the operating system, stops all system activities, and turn 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 3-99 describes the shutdown-only operation and the shutdown poweroff operation for a WAAS device.

Table 3-99 Description of the shutdown Command Operations

Activity	Process
User performs a shutdown operation on the WAE	Shutdown poweroff WAE# shutdown poweroff
User intervention to bring WAE back online	After a shutdown poweroff, you must press the power button once to bring the WAAS device back online.
File system check	Is <i>not</i> performed after you turn the power on again and reboot the WAAS device.

You can enter the **shutdown EXEC** command from a console session or from a remote session (Telnet or SSH version 1 or SSH version 2) to perform shutdown on a WAAS device.

To perform a shutdown on a WAAS device, enter the **shutdown EXEC** command as follows:

```
WAE# shutdown
```

When you are asked if you want to save the system configuration, enter **yes**.

```
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.

```
Device can not be powered on again through software after shutdown.  
Proceed with shutdown?[confirm]
```

A message appears, reporting that all services are being shut down on this WAE.

```
Shutting down all services, will timeout in 15 minutes.  
shutdown in progress ..System halted.
```

After the system is shut down (the system has halted), a WAAS software shutdown shell displays the current state of the system (for example, “System has been shut down”) on the console. You are asked whether you want to perform a software power off (the **Power down system by software** option), or if you want to reload the system through the software.

```
===== SHUTDOWN SHELL =====  
System has been shut down.  
You can either  
    Power down system by pressing and holding power button  
or  
1. Reload system through software
```

2. Power down system through software

To power down the WAAS device, press and hold the power button on the WAAS device, 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 WAAS CLI, enter the **shutdown poweroff EXEC** command as follows:

```
WAE# shutdown poweroff
```

When you are asked if you want to save the system configuration, enter **yes**.

```
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:

```
WAE1# 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 WAAS device:

```
WAE2# 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 trigger

To configure thresholds for a user-selected MIB object for monitoring purposes on a WAAS device, use the **snmp trigger EXEC** command. Use the **no** form of this command to return the setting to the default value.

```
snmp trigger { create mibvar [wildcard] [wait-time [absent [LINE | mibvar1 mibvar1] [LINE | mibvar2 mibvar2] [LINE | mibvar3 mibvar3] [LINE] | equal [absolute value [[LINE | mibvar1 mibvar1] [LINE | mibvar2 mibvar2] [LINE | mibvar3 mibvar3] [LINE] | delta value [LINE | mibvar1 mibvar1] [LINE | mibvar2 mibvar2] [LINE | mibvar3 mibvar3] [LINE]] | falling [absolute value [LINE | mibvar1 mibvar1] [LINE | mibvar2 mibvar2] [LINE | mibvar3 mibvar3] [LINE] | delta value [LINE | mibvar1 mibvar1] [LINE | mibvar2 mibvar2] [LINE | mibvar3 mibvar3] [LINE]] | greater-than [absolute value [LINE | mibvar1 mibvar1] [LINE | mibvar2 mibvar2] [LINE | mibvar3 mibvar3] [LINE]] | delta value [LINE | mibvar1 mibvar1] [LINE | mibvar2 mibvar2] [LINE | mibvar3 mibvar3] [LINE]] | less-than [absolute value [LINE | mibvar1 mibvar1] [LINE | mibvar2 mibvar2] [LINE | mibvar3 mibvar3] [LINE] | delta value [LINE | mibvar1 mibvar1] [LINE | mibvar2 mibvar2] [LINE | mibvar3 mibvar3] [LINE]] | on-change [[LINE | mibvar1 mibvar1][LINE | mibvar2 mibvar2] [LINE | mibvar3 mibvar3] [LINE]] | present [LINE | mibvar1 mibvar1] [LINE | mibvar2 mibvar2] [LINE | mibvar3 mibvar3] [LINE] | rising [absolute value [LINE | mibvar1 mibvar1] [LINE | mibvar2 mibvar2] [LINE | mibvar3 mibvar3] [LINE] | delta value [LINE | mibvar1 mibvar1] [LINE | mibvar2 mibvar2] [LINE | mibvar3 mibvar3] [LINE]]] | delete mibvar }
```

Syntax Description

create	Configures a threshold for a MIB object.
<i>mibvar</i>	Name of the MIB object that you want to monitor or the MIB object for which you want to remove a monitoring threshold.
wildcard	(Optional) Treats the specified MIB variable name as having a wildcard.
<i>wait-time</i>	(Optional) Number of seconds, 60–600, to wait between trigger samples.
absent	(Optional) Applies the absent existence test.
<i>LINE</i>	(Optional) Description of the threshold being created.
mibvar1, mibvar2, mibvar3	(Optional) Adds a MIB object to the notification.
<i>mibvar1, mibvar2, mibvar3</i>	Name of the MIB object to add to the notification.
equal	Applies the equality threshold test.
absolute	(Optional) Uses an absolute sample type.
<i>value</i>	(Optional) Absolute or delta value for sample.
delta	Uses a delta sample type.
falling	Applies the falling threshold test.
greater-than	Applies the greater-than threshold test.
less-than	Applies the less-than threshold test.
on-change	Applies the changed existence test.
present	Applies the present test.
rising	Applies the rising threshold test.
delete	Removes a threshold for a MIB object.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines Using the **snmp trigger** global configuration command, you can define additional SNMP traps for other MIB objects of interest to your particular configuration. You can select any MIB object from any of the support MIBs for your trap. The trap can be triggered based on a variety of tests:

- absent—A specified MIB object that was present at the last sampling is no longer present as of the current sampling.
- equal—The value of the specified MIB object is equal to the specified threshold.
- falling—The value of the specified MIB object has fallen below the specified threshold value. After a trap is generated against this condition, another trap for this same condition is not generated until the sampled MIB object value rises above the threshold value and then falls below the falling threshold value again.
- greater-than—The value of the specified MIB object is greater than the specified threshold value.
- less-than—The value of the specified MIB object is less than the specified threshold value.
- on-change—The value of the specified MIB object has changed since the last sampling.
- present—A specified MIB object is present as of the current sampling that was not present at the previous sampling.
- rising—The value of the specified MIB object has risen above the specified threshold. After a trap is generated against this condition, another trap for this same condition is not generated until the sampled MIB object value falls below the threshold value and then rises above the rising threshold value again.

The threshold value can be based on an *absolute* sample type or on a *delta* sample type. An absolute sample type is one in which the test is evaluated against a fixed integer value between zero and 4294967295. A delta sample type is one in which the test is evaluated against the change in the MIB object value between the current sampling and the previous sampling.

After you configure SNMP traps, you must use the **snmp-server enable traps event** global configuration command for the event traps you just created to be generated. Also, to preserve SNMP trap configuration across a system reboot, you must configure event persistence using the **snmp mib persist event** global configuration command, and save the MIB data using the **write mib-data EXEC** command.

Examples The following example shows how to create a threshold for the MIB object *esConTabIsConnected* so that a trap is sent when the connection from the Edge WAE to the Core WAE is lost:

```
WAE# snmp trigger create esConTabIsConnected ?
    <60-600> The number of seconds to wait between trigger sample
    wildcard Option to treat the MIB variable as wildcarded
WAE# snmp trigger create esConTabIsConnected wildcard 600 ?
```

```

absent          Absent existence test
equal          Equality threshold test
falling        Falling threshold test
greater-than   Greater-than threshold test
less-than     Less-than threshold test
on-change     Changed existence test
present       Present present test
rising        Rising threshold test
WAE# snmp trigger create esConTabIsConnected wildcard 600 falling ?
absolute Absolute sample type
delta      Delta sample type
WAE# snmp trigger create esConTabIsConnected wildcard 600 falling absolute ?
<0-4294967295> Falling threshold value
WAE# snmp trigger create esConTabIsConnected wildcard 600 falling absolute 1 ?
LINE      Trigger-comment
mibvar1   Optional mib object to add to the notification
WAE# snmp trigger create esConTabIsConnected wildcard 600 falling absolute 1 "Lost the
connection with the core server."
WAE# configure
WAE(config)# snmp-server enable traps event

```

Once you have configured the WAE to send SNMP traps, you can view the results of these newly created traps using the **show snmp events EXEC** command.

You can also delete user-created SNMP traps. The following example shows how to delete the trap set for *esConTabIsConnected* that we created in the previous example.

```
WAE# snmp trigger delete esConTabIsConnected
```

Related Commands

- [\(config\) snmp-server community](#)
- [\(config\) snmp-server contact](#)
- [\(config\) snmp-server enable traps](#)
- [\(config\) snmp-server group](#)
- [\(config\) snmp-server host](#)
- [\(config\) snmp-server location](#)
- [\(config\) snmp-server mib persist event](#)
- [\(config\) snmp-server notify inform](#)
- [\(config\) snmp-server user](#)
- [\(config\) snmp-server view](#)

ssh

To allow secure encrypted communications between an untrusted client machine and a WAAS device over an insecure network, use the **ssh** EXEC command.

ssh *options*

Syntax Description

options

Options to use with the **ssh** EXEC command. For more information about the possible options, see Request for Comments (RFC 4254) at <http://www.rfc-archive.org/getrfc.php?rfc=4254>.

Defaults

By default, the Secure Shell (SSH) feature is disabled on a WAAS device.

Command Modes

EXEC

Device Modes

application-accelerator
 replication-accelerator
 central-manager

Usage Guidelines

SSH consists of a server and a client program. Like Telnet, you can use the client program to remotely log in 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.



Note

The Telnet daemon can still be used with the WAAS device. SSH does not replace Telnet.

Related Commands

(config) [sshd](#)
 (config) [ssh-key-generate](#)

tcpdump

To dump network traffic, use the **tcpdump** EXEC command.

tcpdump [*LINE*]

Syntax Description	<i>LINE</i> (Optional) Dump options.
Defaults	No default behavior or values
Command Modes	EXEC
Device Modes	application-accelerator replication-accelerator central-manager
Usage Guidelines	<p>TCPdump is a utility that allows a user to intercept and capture packets passing through a network interface, making it useful for troubleshooting network applications.</p> <p>During normal network operation, only the packets which are addressed to a network interface are intercepted and passed on to the upper layers of the TCP/IP protocol layer stack. Packets which are not addressed to the interface are ignored. In Promiscuous mode, the packets which are not intended to be received by the interface are also intercepted and passed on to the higher levels of the protocol stack. TCPdump works by putting the network interface into promiscuous mode. TCPdump uses the free libpcap (packet capture library).</p> <p>Use the <i>-h</i> option to view the options available, as shown in this example:</p> <pre>WAE# tcpdump -h tcpdump version 3.8.1 (jlemon) libpcap version 0.8 Usage: tcpdump [-aAdDeflLnNOpqRStuUvxxX] [-c count] [-C file_size] [-E algo:secret] [-F file] [-i interface] [-r file] [-s snaplen] [-T type] [-w file] [-y datalinktype] [expression]</pre>
Examples	<p>The following example starts a network traffic dump to a file named <i>tcpdump.txt</i>:</p> <pre>WAE# tcpdump -w tcpdump.txt</pre>
Related Commands	<p>less</p> <p>ping</p> <p>tethereal</p>

traceroute

telnet

To log in to a WAAS device using the Telnet client, use the **telnet** EXEC command.

```
telnet {hostname | ip-address} [portnum]
```

Syntax Description	hostname	Hostname of the network device.
	ip-address	IP address of the network device.
	portnum	(Optional) Port number (1–65535). Default port number is 23.

Defaults The default port number is 23.

Command Modes EXEC

Device Modes

- application-accelerator
- replication-accelerator
- central-manager

Usage Guidelines UNIX shell functions such as escape and the **suspend** command are not available in the Telnet client. Multiple Telnet sessions are also not supported. This Telnet client allows you to specify a destination port.

Examples The following example shows several ways that you can log in to a WAAS device using the Telnet client:

```
WAE# telnet cisco-wae
WAE# telnet 10.168.155.224
WAE# telnet cisco-wae 2048
WAE# telnet 10.168.155.224 2048
```

Related Commands (config) telnet enable

terminal

To set the number of lines displayed in the console window, or to display the current console **debug** command output, use the **terminal EXEC** command.

```
terminal {length length | monitor [disable]}
```

Syntax Description	length	Sets the length of the display on the terminal.
	<i>length</i>	Length of the display on the terminal (0–512). Setting the length to 0 means there is no pausing.
	monitor	Copies the debug output to the current terminal.
	disable	(Optional) Disables monitoring at this specified terminal.

Defaults The default is 24 lines.

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines When 0 is entered as the *length* parameter, the output to the screen does not pause. For all nonzero values of *length*, the -More- prompt is displayed when the number of output lines matches the specified *length* number. The -More- prompt is considered a line of output. To view the next screen, press the **Spacebar**. To view one line at a time, press the **Enter** key.

The **terminal monitor** command allows a Telnet session to display the output of the **debug** commands that appear on the console. Monitoring continues until the Telnet session is terminated.

Examples The following example sets the number of lines to display to 20:

```
WAE# terminal length 20
```

The following example configures the terminal for no pausing:

```
WAE# terminal length 0
```

Related Commands All **show** commands

tetherreal

To analyze network traffic from the command line, use the **tetherreal** EXEC command.

tetherreal [*LINE*]

Syntax Description	<i>LINE</i> (Optional) Options.
Defaults	No default behavior values
Command Modes	EXEC
Device Modes	application-accelerator replication-accelerator central-manager
Usage Guidelines	<p>Tetherreal is the command line version of the network traffic analyzer tool Ethereal. Like TCPdump, it also uses the packet capture library (libpcap). Aside from network traffic analysis, Tetherreal also provides facilities for decoding packets.</p> <p>The following example shows the options available with the WAAS tetherreal command:</p> <pre>WAE# tetherreal -h This is GNU tetherreal 0.10.6 (C) 1998-2004 Gerald Combs <gerald@ethereal.com> Compiled with GLib 1.2.9, with libpcap 0.6, with libz 1.1.3, without libpcrc, without UCD-SNMP or Net-SNMP, without ADNS. NOTE: this build does not support the "matches" operator for Ethereal filter syntax. Running with libpcap (version unknown) on Linux 2.4.16. tetherreal [-vh] [-DlNpqSVx] [-a <capture autostop condition>] ... [-b <number of ring buffer files>[:<duration>]] [-c <count>] [-d <layer_type>==<selector>,<decode_as_protocol>] ... [-f <capture filter>] [-F <output file type>] [-i <interface>] [-N <resolving>] [-o <preference setting>] ... [-r <infile>] [-R <read filter>] [-s <snaplen>] [-t <time stamp format>] [-T pdml ps psml text] [-w <savefile>] [-y <link type>] [-z <statistics string>] Valid file type arguments to the "-F" flag: libpcap - libpcap (tcpdump, Ethereal, etc.) rh6_1libpcap - RedHat Linux 6.1 libpcap (tcpdump) suse6_3libpcap - SuSE Linux 6.3 libpcap (tcpdump) modlibpcap - modified libpcap (tcpdump) nokialibpcap - Nokia libpcap (tcpdump) lanalyzer - Novell LANalyzer ngsniffer - Network Associates Sniffer (DOS-based) snoop - Sun snoop netmon1 - Microsoft Network Monitor 1.x netmon2 - Microsoft Network Monitor 2.x</pre>

```
ngwsniffer_1_1 - Network Associates Sniffer (Windows-based) 1.1
ngwsniffer_2_0 - Network Associates Sniffer (Windows-based) 2.00x
visual - Visual Networks traffic capture
5views - Accellent 5Views capture
niobserverv9 - Network Instruments Observer version 9
default is libpcap
```

Related Commands [tcpdump](#)

traceroute

To trace the route between a WAAS device to a remote host, use the **traceroute** EXEC command.

```
traceroute {hostname | ip-address}
```

Syntax Description	hostname	Name of remote host.
	ip-address	IP address of remote host.

Defaults No default behavior values

Command Modes EXEC

Device Modes application-accelerator
 replication-accelerator
 central-manager

Usage Guidelines Traceroute is a widely available utility on most operating systems. Much like ping, it is a valuable tool for determining connectivity in a network. Ping allows the user to find out if there is a connection between two end systems. Traceroute does this as well, but also lists the intermediate routers between the two systems. Users can therefore see the possible routes packets can take from one system to another. Use **traceroute** to find the route to a remote host, when either the hostname or the IP address is known.

Examples The following example traces the route between the WAAS device and a device with an IP address of 10.0.0.0:

```
WAE# traceroute 10.0.0.0
traceroute to 10.0.0.0 (10.0.0.0), 30 hops max, 38 byte packets
 1 sblab2-rtr.abc.com (192.168.10.1)  0.959 ms  0.678 ms  0.531 ms
 2 192.168.1.1 (192.168.1.1)  0.665 ms  0.576 ms  0.492 ms
 3 172.24.115.66 (172.24.115.66)  0.757 ms  0.734 ms  0.833 ms
 4 sjc20-sbb5-gw2.abc.com (192.168.180.93)  0.683 ms  0.644 ms  0.544 ms
 5 sjc20-rbb-gw5.abc.com (192.168.180.9)  0.588 ms  0.611 ms  0.569 ms
 6 sjce-rbb-gw1.abc.com (172.16.7.249)  0.746 ms  0.743 ms  0.737 ms
 7 sj-wall-2.abc.com (172.16.7.178)  1.505 ms  1.101 ms  0.802 ms
 8 * * *
 9 * * *
 .
 .
 .
29 * * *
30 * * *
```

Related Commands [ping](#)

transaction-log

To force the exporting or the archiving of the transaction log, use the **transaction-log EXEC** command.

transaction-log {export | tfo force archive}

Syntax Description

export	Forces the archiving of a WAE's transaction file.
tfo force archive	Forces the archiving of the Traffic Flow Optimization (TFO) transaction log file.

Command Modes

EXEC

Device Modes

application-accelerator

Examples

The following example forces the archiving of the transaction file on the WAE:

```
WAE# transaction-log export
```

The following example forces the archiving of a WAE's TFO transaction log file:

```
WAE# transaction-log tfo force archive
```

Related Commands

[\(config\) transaction-logs](#)
[show transaction-logging](#)

type

To display a file, use the **type** EXEC command.

type *filename*

Syntax Description	<i>filename</i> Name of file.
Defaults	No default behavior or values
Command Modes	EXEC
Device Modes	application-accelerator replication-accelerator central-manager
Usage Guidelines	Use this EXEC command to display the contents of a file within any file directory on a WAAS device. 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 contents of the <i>syslog.txt</i> file: WAE# type /local1/syslog.txt
Related Commands	cpfile dir lls ls pwd rename

type-tail

To view a specified number of lines of the end of a log file, to view the end of the file continuously as new lines are added to the file, to start at a particular line in the file, or to include or exclude specific lines in the file, use the **type-tail** command in EXEC mode.

```
type-tail filename [line | follow | { begin LINE | exclude LINE | include LINE }]
```

Syntax Description

<i>filename</i>	File to be examined.
<i>line</i>	(Optional) Number of lines from the end of the file to be displayed (1–65535).
follow	(Optional) Displays the end of the file continuously as new lines are added to the file.
	(Optional) Displays contents of the file according to the begin , exclude , and include output modifiers.
begin	Identifies the line at which to begin file display.
<i>LINE</i>	Regular expression to match in the file where you want to begin display, or that is to be included or excluded from display.
exclude	Indicates lines that are to be excluded from the file display.
include	Indicates lines that are to be included in the file display.

Defaults

Last ten lines are shown.

Command Modes

EXEC

Device Modes

application-accelerator
 replication-accelerator
 central-manager

Usage Guidelines

This EXEC 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 as with the **follow** option, use the key sequence **Ctrl-C**.

You can further indicate the type of information to display using the output modifiers. These allow you to include or exclude specific lines or to indicate where to begin displaying the file.

Examples

The following example looks for a list of log files in the */local1* directory and then displays the last ten lines of the *syslog.txt* file. In this example, the number of lines to display is not specified, so the default of ten lines is used:

```
WAE# ls /local1
actona
core_dir
```

```

crash
dbupgrade.log
downgrade
errorlog
logs
lost+found
sa
service_logs
spool
syslog.txt
syslog.txt.1
syslog.txt.2
syslog.txt.3
syslog.txt.4
var
wdd.sh.signed

```

```

WAE# type-tail /local1/syslog.txt
Apr 17 00:21:09 edge-wae-11 java: %CE-CMS-4-700001: unable to get https
equest throughput stats(error 4)
Apr 17 00:21:09 edge-wae-11 java: %CE-CMS-4-700001: ds_getStruct got err
r : 4 for key stat/cache/ftp connection 5
Apr 17 00:21:09 edge-wae-11 java: %CE-CMS-4-700001: ds_getStruct: unable
to get `stat/cache/ftp' from dataserver
Apr 17 00:21:09 edge-wae-11 java: %CE-CMS-4-700001: unable to get ftp-ov
er-http request throughput stats(error 4)
Apr 17 00:21:09 edge-wae-11 java: %CE-CMS-4-700001: setValues getMethod
all ...
Apr 17 00:21:09 edge-wae-11 java: %CE-CMS-4-700001: setValues found...
Apr 17 00:21:48 edge-wae-11 java: %CE-CMS-4-700001: ds_getStruct got err
r : 4 for key stat/cache/http/perf/throughput/requests/sum connection 5
Apr 17 00:21:48 edge-wae-11java: %CE-CMS-4-700001: ds_getStruct: unable
to get `stat/cache/http/perf/throughput/requests/sum' from dataserver
Apr 17 00:21:48 edge-wae-11 java: %CE-CMS-4-700001: unable to get http r
quest throughput stats(error 4)
Apr 17 00:23:20 edge-wae-11 java: %CE-TBD-3-100000: WCCP_COND_ACCEPT: TU
LE DELETE conditional accept tuple {Source IP [port] = 0.0.0.0 [0] Destinati
o
IP [port] = 32.60.43.2 [53775] }returned error: -1 errno 9

```

The following example follows the *syslog.txt* file as it grows:

```

WAE# type-tail /local1/syslog.txt follow

```

undebug

To disable debugging functions, use the **undebug** EXEC command. (See also the **no** form of the **debug** EXEC command.)

In the application-accelerator device mode, the **undebug** commands are as follows:

undebug aaa accounting

undebug all

undebug authentication {content-request | user | windows-domain}

undebug buf {all | dmbuf | dmsg}

undebug cdp {adjacency | events | ip | packets}

undebug cli {all | bin | parser}

undebug cms

undebug dataserver {all | clientlib | server}

undebug dhcp

undebug dre {aggregation | all | cache | connection {aggregation [acl] | cache [acl] | core [acl] | message [acl] | misc [acl] | acl} | core | lz | message | misc}

undebug epm

undebug flow monitor tcpstat-v1

undebug logging all]

undebug ntp

undebug print-spooler {all | brief | errors | warnings}

undebug rbcg

undebug snmp {all | cli | main | mib | traps}

undebug tfo {buffer-mgr | connection [auto-discovery [acl] | comp-mgr [acl] | conn-mgr [acl] | egress-method [acl] | filtering [acl] | netio-engine [acl] | policy-engine [acl] | synq [acl] | acl] | stat-mgr | translog}

undebug translog export

undebug wafs {{all | core-fe | edge-fe | manager | utilities} {debug | error | info | warn}}

undebug wccp {all | detail | error | events | keepalive | packets | slowstart}



Note

The **dre**, **epm**, **flow**, **print-spooler**, **rbcg**, **tfo**, **translog**, **wafs**, and **wccp** command options are supported in the application-accelerator device mode only.

In the central manager device mode, the **undebug** commands are as follows:

```
undebug aaa accounting
undebug all
undebug authentication {content-request | user | windows-domain}
undebug buf {all | dmbuf | dmsg}
undebug cdp {adjacency | events | ip | packets}
undebug cli {all | bin | parser}
undebug cms
undebug dataserver {all | clientlib | server}
undebug dhcp
undebug emdb [level [levelnum]]
undebug logging all
undebug ntp
undebug rpc {detail | trace}
undebug snmp {all | cli | main | mib | traps}
```



Note

The **emdb**, **key-manager**, and **rpc** command options are supported in the central manager device mode only.

Syntax Description

aaa accounting	(Optional) Disables AAA accounting actions.
all	(Optional) Disables all debugging options.
authentication	(Optional) Disables authentication debugging.
content-request	Disables content request authentication debugging.
user	Disables debugging of the user login against the system authentication.
windows-domain	Disables Windows domain authentication debugging.
buf	(Optional) Disables buffer manager debugging.
all	Disables all buffer manager debugging.
dmbuf	Disables only dmbuf debugging.
dmsg	Disables only dmsg debugging.
cdp	(Optional) Disables CDP debugging.
adjacency	Disables CDP neighbor information debugging.
events	Disables CDP events debugging.
ip	Disables CDP IP debugging.

packets	Disables packet-related CDP debugging.
cli	(Optional) Disables CLI debugging.
all	Disables all CLI debugging.
bin	Disables CLI command binary program debugging.
parser	Disables CLI command parser debugging.
cms	(Optional) Disables CMS debugging.
dataserver	(Optional) Disables data server debugging.
all	Disables all data server debugging.
clientlib	Disables data server client library module debugging.
server	Disables data server module debugging.
dhcp	(Optional) Disables DHCP debugging.
dre	(Optional) Disables DRE debugging.
aggregation	Disables DRE chunk-aggregation debugging.
all	Disables the debugging of all DRE commands.
cache	Disables DRE cache debugging.
connection	Disables DRE connection debugging.
aggregation [acl]	Disables DRE chunk-aggregation debugging for a specified connection.
cache [acl]	Disables DRE cache debugging for a specified connection.
core [acl]	Disables DRE core debugging for a specified connection.
message [acl]	Disables DRE message debugging for a specified connection.
misc [acl]	Disables DRE other debugging for a specified connection.
<i>acl</i>	ACL to limit connections traced.
core	Disables DRE core debugging.
message	Disables DRE message debugging.
misc	Disables DRE other debugging.
epm	(Optional) Disables the DCE-RPC EPM debugging.
flow	(Optional) Enables network traffic flow debugging.
monitor	Enables monitor flow performance debugging commands.
tcpstat-v1	Enables tcpstat-v1 debugging.
logging	(Optional) Disables logging debugging.
all	Disables all logging debugging.
ntp	(Optional) Disables NTP debugging.
print-spooler	(Optional) Disables print spooler debugging.
all	Disables print spooler debugging using all debug features.
brief	Disables print spooler debugging using only brief debug messages.
errors	Disables print spooler debugging using only the error conditions.
warnings	Disables print spooler debugging using only the warning conditions.
rbcp	(Optional) Disables RBCP debugging.
snmp	(Optional) Disables SNMP debug commands.

all	Disables all SNMP debug commands.
cli	Disables SNMP CLI debugging.
main	Disables SNMP main debugging.
mib	Disables SNMP MIB debugging.
traps	Disables SNMP trap debugging.
tfo	(Optional) Disables TFO debugging.
buffer-mgr	Disables TFO buffer manager debugging.
connection	Disables TFO connection debugging.
auto-discovery [<i>acl</i>]	(Optional) Disables TFO connection debugging for the auto-discovery module.
comp-mgr [<i>acl</i>]	(Optional) Disables TFO connection debugging for the compression module.
conn-mgr [<i>acl</i>]	(Optional) Disables TFO connection debugging for the connection manager.
egress-method [<i>acl</i>]	(Optional) Disables TFO connection debugging for the egress-method.
filtering [<i>acl</i>]	(Optional) Disables TFO connection debugging for filtering module.
netio-engine [<i>acl</i>]	(Optional) Disables TFO connection debugging for network input/output module.
policy-engine [<i>acl</i>]	(Optional) Disables TFO connection debugging of application policies.
synq [<i>acl</i>]	(Optional) Disables TFO connection debugging for the SynQ module.
<i>acl</i>	(Optional) ACL to limit TFO connections.
stat-mgr	Disables TFO statistics manager debugging.
translog	Disables TFO transaction log debugging.
translog	(Optional) Disables transaction logging debug commands.
export	Disables transaction log FTP export debugging.
wafs	(Optional) Unsets the notification level (debug, info, warn, error) at which messages from the WAAS software component and utilities are logged.
all	Unsets the logging level for all software components and utilities at once.
core-fe	Unsets the logging level for WAEs acting as a core File Engine.
edge-fe	Unsets the logging level for WAEs acting as an edge File Engine.
manager	Unsets the logging level for the Device Manager.
utilities	Unsets the logging level for WAAS utilities.
wccp	(Optional) Disables the WCCP information debugging.
all	Disables all WCCP debugging functions.
detail	Disables the WCCP detail debugging.
error	Disables the WCCP error debugging.
events	Disables the WCCP events debugging.

keepalive	Disables the debugging for WCCP keepalives that are sent to the applications.
packets	Disables the WCCP packet-related information debugging.
slowstart	Disables the WCCP slow-start debugging.

The following syntax table describes the options that are available in the central manager device mode:

emdb	(Optional) Disables embedded database debugging.
level	(Optional) Disables the specified debug level for EMDb service.
<i>levelnum</i>	(Optional) Debug level to disable. (Level 0 disables debugging.)
key-manager	(Optional) Disables the Central Manager key manager debugging.
rpc	(Optional) Disables the remote procedure calls (RPC) logs.
detail	Disables the RPC logs of priority “detail” level or higher.
trace	Disables the RPC logs of priority “trace” level or higher.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines We recommend that the **debug** and **undebg** commands be used only at the direction of Cisco Systems technical support personnel.

Related Commands [debug](#)
[show debugging](#)

wafs

To back up, restore, or create a system report about the Wide Area File Services (WAFS)-related network configuration, plus the configurations of file servers, printers, users, and so forth, on a WAE, use the **wafs EXEC** command.

```
wafs { backup-config filename | restore-config filename |
      sysreport [filename | date-range from_date end_date filename]}
```



Note

Executing the **wafs sysreport** command can temporarily impact the performance of your WAE.

Syntax Description

backup-config	Copies current WAFS-related configuration information to a file.
<i>filename</i>	Name of the file, in <i>xxxx.tar.gz</i> format, where you want to save the WAFS configuration. This file is saved to the <i>/local/local1</i> directory.
restore-config	Loads saved WAFS-related configuration information from a file.
<i>filename</i>	(Optional) Name of the file, in <i>xxxx.tar.gz</i> format, where the desired WAFS configuration information has been stored. This file should be in the <i>/local/local1</i> directory.
sysreport	Deprecated; use copy sysreport .
date-range	(Optional) Displays the range of time that the system report is to cover.
<i>from_date</i>	Start date of information in the generated system report.
<i>to_date</i>	End date of information in the generated system report.
<i>filename</i>	Name of the file, in <i>xxxx.tar.gz</i> format, in which the system information is to be stored.

Defaults

No default behavior or values

Command Modes

EXEC

Device Modes

application-accelerator

Usage Guidelines

The **wafs backup-config EXEC** command is used when back up of basic network configuration is not sufficient (performed using the **copy running-config** command), for example, when you want to back up system configurations before making any changes using the WAAS CLI global configuration mode and you want to protect the current configuration from loss of data by erroneous operations.

The **wafs restore-config** automatically performs a reload function. We strongly recommend that you re-register your WAE on completion of this command.

This **wafs** command is also useful when backup and system restoration, or generation of a system report, are not available from the WAAS Central Manager GUI.

Examples

The following example creates a backup file of the WAFS configuration information:

```
WAE# wafs ?
  backup-config  backup system configurations to a file.
  restore-config restore system configurations from a file. WARNING: After
                  restoring configuration, the system needs to be restarted and
                  re-registered.
  sysreport      system report to a file
```

```
WAE# wafs backup-config backup.tar.gz
      system configuration is stored in file /local/local1/backup.tar.gz
```

The following example restores a system with previously saved WAAS configuration information:

```
WAE# wafs restore-config backup.tar.gz
Restoring configurations ...
After upload is completed the File Engine will be reloaded. We strongly recommend you
re-register after the engine is reloaded.
```

Related Commands

[copy running-config](#)

whoami

To display the username of the current user, use the **whoami** EXEC command.

whoami

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines Use this EXEC command to display the username of the current user.

Examples The following example displays your username:

```
WAE# whoami  
admin
```

Related Commands [pwd](#)

windows-domain

To access the Windows domain utilities on a WAAS device, use the **windows-domain EXEC** command.

windows-domain diagnostics { **findsmb** | **getent** | **net** | **nmblookup** | **smbclient** | **smbstatus** | **smbtree** | **tddbbackup** | **tdbdump** | **testparm** | **wbinfo** }

Syntax	Description
diagnostics	Enables selection of Windows domain diagnostic utilities.
findsmb	Displays the utility for troubleshooting NetBIOS name resolution and browsing.
getent	Displays the utility to get unified list of both local and PDC users and groups.
net	Displays the utility for administration of remote CIFS servers.
nmblookup	Displays the utility for troubleshooting NetBIOS name resolution and browsing.
smbclient	Displays the utility for troubleshooting the Windows environment and integration.
smbstatus	Displays the utility for inspecting the Samba server status, connected clients, etc.
smbtree	Displays the utility for inspecting the Windows network neighborhood structure and content.
tddbbackup	Displays the utility for backing up, verifying and restoring Samba database files.
tdbdump	Displays the utility for inspecting the Samba database files.
testparm	Displays the utility to validate <i>smb.conf</i> file correctness.
wbinfo	Displays the utility for Winbind and domain integration troubleshooting.

Defaults No default behavior or values

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines Use this command to activate the selected Windows domain diagnostic utility.

Examples The following example shows the options available for the Get Entity utility:

```
WAE# windows-domain diagnostics getent --help
```



```
Usage: getent [OPTION...] database [key ...]
getent - get entries from administrative database.
```

```
-s, --service=CONFIG      Service configuration to be used
-?, --help                Give this help list
--usage                  Give a short usage message
-V, --version             Print program version
```

Mandatory or optional arguments to long options are also mandatory or optional for any corresponding short options.

Supported databases:

```
aliases ethers group hosts netgroup networks passwd protocols rpc
services shadow
```

The following example shows the options available for the NMB Lookup Utility for troubleshooting NetBIOS name resolution and browsing:

```
WAE# windows-domain diagnostics nmblookup -h
Usage: [-?TV] [--usage] [-B BROADCAST-ADDRESS] [-f VAL] [-U STRING] [-M VAL]
       [-R VAL] [-S VAL] [-r VAL] [-A VAL] [-d DEBUGLEVEL] [-s CONFIGFILE]
       [-l LOGFILEBASE] [-O SOCKETOPTIONS] [-n NETBIOSNAME] [-W WORKGROUP]
       [-i SCOPE] <NODE> ...
```

The following example shows the options available for the Samba Client Utility for troubleshooting the Windows environment and integration:

```
WAE# windows-domain diagnostics smbclient -h
Usage: [-?EgVNkP] [--usage] [-R NAME-RESOLVE-ORDER] [-M HOST] [-I IP] [-L HOST]
       [-t CODE] [-m LEVEL] [-T <c|x>IXFqgbNan] [-D DIR] [-c STRING] [-b BYTES]
       [-p PORT] [-d DEBUGLEVEL] [-s CONFIGFILE] [-l LOGFILEBASE]
       [-O SOCKETOPTIONS] [-n NETBIOSNAME] [-W WORKGROUP] [-i SCOPE]
       [-U USERNAME] [-A FILE] [-S on|off|required] service <password>
```

The following example shows the options available for the TDB Backup Utility:

```
WAE# windows-domain diagnostics tdbbackup -h
Usage: tdbbackup [options] <fname...>

-h          this help message
-s suffix   set the backup suffix
-v          verify mode (restore if corrupt)
```

The following example shows the use of the -u option of the WinBind Utility to view the information about a user registered in a Windows domain:

```
WAE# windows-domain diagnostics wbinfo -u
administrator
guest
user98
tuser1

WAE# show user username user98
Uid          : 70012
Username     : user98
Password    : *****
Privilege    : super user
Configured in : Windows Domain database

WAE# show user uid 70012
Uid          : 70012
Username     : user98
Password    : *****
Privilege    : super user
```

Configured in : Windows Domain database

The following example shows how to register a Windows domain:

```
WAE# windows-domain diagnostics  
      net join -S<domain server> -U<domain admin username>%<domain admin password>
```

Related Commands [\(config\) windows-domain](#)

write

To save startup configurations on a WAAS device, use the **write EXEC** command.

write [**erase** | **memory** | **mib-data** | **terminal**]

Syntax Description		
erase	(Optional)	Erases startup configuration from NVRAM.
memory	(Optional)	Writes the configuration to NVRAM. This is the default location for saving startup information.
mib-data	(Optional)	Saves MIB persistent configuration data to disk.
terminal	(Optional)	Writes the configuration to a terminal session.

Defaults The configuration is written to NVRAM by default.

Command Modes EXEC

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines Use this command to either save running configurations to NVRAM or to 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 WAAS device.

Use the **write terminal** command to display the current running configuration in the terminal session window. The equivalent command is **show running-config**.

Examples The following example saves the current startup configuration to memory:

```
WAE# write memory
```

Related Commands [copy running-config](#)
[copy startup-config](#)
[show running-config](#)
[show startup-config](#)

Configuration Mode Commands

Use global configuration mode for setting, viewing, and testing configuration of WAAS software features for the entire device. To enter this mode, enter the **configure** command from privileged EXEC mode. The prompt for global configuration mode consists of the hostname of the WAE followed by (config) and the pound sign (#). You must be in global configuration mode to enter global configuration commands.

```
WAE# configure  
WAE(config)#
```

Commands entered in global configuration mode update the running configuration file as soon as they are entered. These changes are not saved into the startup configuration file until you enter the **copy running-config startup-config** EXEC mode command. Once the configuration is saved, it is maintained across WAE reboots.

You also can use global configuration mode to enter specific configuration modes. From global configuration mode you can enter the interface configuration mode, standard ACL configuration mode, or the extended ACL configuration mode.

To exit global configuration mode and return to privileged-level EXEC mode, use either the **exit** or **end** global configuration command:

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

(config) aaa accounting

To configure AAA accounting on a WAAS device, use the **aaa accounting** command in global configuration mode.

```
aaa accounting {commands {0 | 15} default {start-stop | stop-only | wait-start} tacacs | exec
               default {start-stop | stop-only | wait-start} tacacs | system default {start-stop | stop-only}
               tacacs}
```

Syntax Description		
commands		Configures accounting for all commands at the specified privilege level.
0		User privilege level for a normal user.
15		User privilege level for an administrative user.
default		Sets AAA accounting to use the default accounting list.
start-stop		Sends a start accounting notice at the beginning of a process and a stop accounting notice at the end of a process. The start accounting record is sent in the background. The requested user process begins regardless of whether the start accounting notice was received by the accounting server.
stop-only		Sends a stop accounting notice at the end of the process requested by the user.
wait-start		Sends both a start and a stop accounting notice to the accounting server. However, the requested user service does not begin until the start accounting notice is acknowledged. The user cannot execute a CLI command or login until the user is on record. A stop accounting notice is also sent but does not need acknowledgement.
tacacs		Enables use of TACACS+ for accounting.
exec		Enables accounting for user EXEC processes (user shells). When enabled, the EXEC shell accounting reports EXEC terminal session (user shell) events and login and logout by an administrator to the EXEC shell.
system		Enables accounting for all system-level events not associated with users, such as reloads.

Defaults AAA accounting is disabled by default.

Command Modes global configuration

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines

The AAA accounting feature enables you to track the activities of an administrative user, services that users access, and the amount of network resources they consume (for example, connection time or the bytes transferred). You can use the AAA accounting feature to track user activity for billing, auditing, reporting, or security purposes. WAAS uses TACACS+ to implement AAA accounting; RADIUS is not currently supported. When AAA accounting is enabled, the WAAS device reports user activity to the TACACS+ security server in the form of accounting records. This data can then be analyzed for network management, client billing, and auditing.

You can activate accounting for the following types of events:

- **EXEC**—EXEC shell accounting is used to report the events of an administrator logging in and out of the EXEC shell through Telnet, FTP, or SSH (SSH Version 1 or Version 2). This type of accounting records information about user EXEC terminal sessions (user shells) on the WAAS device, including username, date, start and stop times for each session, time zone, and IP address of the system used to access the WAAS device. The EXEC shell accounting information can be accessed through the accounting log file on the TACACS+ server. This log file uses the following report format for this type of accounting information:

```
WeekDay#Month#Day#Time#Year#CEaddress#username#terminal#RemoteHost#Event#
EventTime#TaskId#Timezone#Service
```

- **Command**—The WAAS device records information about the CLI commands that were executed on the WAAS device. Each command accounting record includes the executed command syntax, username of the user who executed the command, the privilege level of the user, and the date and time that each command was executed. The WAAS device supports two privilege levels, 0 and 15, representing normal users and administrative users, respectively. The command accounting information can be accessed through the accounting log file on the TACACS+ server. This log file uses the following report format for this type of accounting information:

```
WeekDay#Month#Day#Time#Year#CEaddress#username#terminal#RemoteHost#Event#
EventTime#TaskId#Timezone#Service#PrivilegeLevel#CLICommand
```

- **System**—The WAAS device records information about all system-level events (for example, when the system reboots). You can access the system accounting information through the accounting log file on the TACACS+ server. This log file uses the following report format for this type of accounting information:

```
WeekDay#Month#Day#Time#Year#CEaddress#username#terminal#RemoteHost#Event#
EventTime#TaskId#Timezone#SystemService#SystemAccountingEvent#EventReason
```

The WAAS software supports only the default accounting list.

**Caution**

Before using the **wait-start** option, make sure that the WAAS device is configured with the TACACS+ server and is able to successfully contact the server. If the WAAS device cannot contact a configured TACACS+ server, it might become unresponsive.

The WAAS software displays the following warning message if the **wait-start** option is configured:

```
Warning: The device may become non-responsive if it cannot contact a configured TACACS+
server.
```

The administrator is asked to confirm the configuration in an indefinite loop until the administrator enters “yes” to the following prompt:

```
Are you sure you want to proceed? [yes]
```

Examples

The following example configures TACACS+ on the WAAS device and also specifies that a start accounting notice should be sent at the beginning of the process and a stop accounting notice at the end of the process, and the requested user process should begin regardless of whether the start accounting notice was received by the accounting server:

```
WAE(config)# tacacs key abc
WAE(config)# tacacs server 192.168.50.1 primary
WAE(config)# aaa accounting system default start-stop tacacs
WAE# show aaa accounting
Accounting Type      Record event(s)  Protocol
-----
Exec shell           unknown          unknown
Command level 0     unknown          unknown
Command level 15    unknown          unknown
System               start-stop       TACACS+
```

The following example shows that the WAAS device is set to record all user EXEC sessions. The command also specifies that a stop accounting notice should be sent to the TACACS+ server at the end of the session.

```
WAE(config)# aaa accounting exec default stop-only tacacs
```

The following example shows that the WAAS device is set to record all CLI commands executed by a normal user. The command also specifies that a stop accounting notice should be sent to the TACACS+ server at the end of each CLI command executed by a normal user.

```
WAE(config)# aaa accounting commands 0 default stop-only tacacs
```

The following example shows that the WAAS device is set to record all CLI commands executed by an administrative user. The command also specifies that a start accounting notice should be sent to the TACACS+ server at the beginning of the process and a stop accounting notice at the end of the process. The CLI command executed by the administrative user does not proceed until the start accounting notice has been acknowledged.

```
WAE(config)# aaa accounting commands 15 default wait-start tacacs
```

The following examples show the EXEC shell accounting report that is available on the TACACS+ server:

```
Wed Apr 14 11:19:19 2004 172.16.0.0 super10 pts/0 172.31.0.0 start
start_time=1081919558 task_id=3028 timezone=PST service=shell
Wed Apr 14 11:19:23 2004 172.16.0.0 super10 pts/0 172.31.0.0
stop stop_time=1081919562 task_id=3028 timezone=PST service=shell
Wed Apr 14 11:22:13 2004 172.16.0.0 normal20 pts/0 via5.abc.com start
start_time=1081919732 task_id=3048 timezone=PST service=shell
Wed Apr 14 11:22:16 2004 172.16.0.0 normal20 pts/0 via5.abc.com stop
stop_time=1081919735 task_id=3048 timezone=PST service=shell
Wed Apr 14 11:25:29 2004 172.16.0.0 admin ftp via5.abc.com start start_time=1081919928
task_id=3069 timezone=PST service=shell
Wed Apr 14 11:25:33 2004 172.16.0.0 admin ftp via5.abc.com stop stop_time=1081919931
task_id=3069 timezone=PST service=shell
```

The following examples show the system accounting report that is available on the TACACS+ server:

```
Wed Apr 14 08:37:14 2004 172.16.0.0 unknown unknown 0.0.0.0 start start_time=1081909831
task_id=2725 timezone=PST service=system event=sys_acct reason=reload
Wed Apr 14 10:19:18 2004 172.16.0.0 admin ttyS0 0.0.0.0 stop stop_time=1081915955
task_id=5358 timezone=PST service=system event=sys_acct reason=shutdown
```

The following examples show the command accounting report that is available on the TACACS+ server:

```
Wed Apr 14 12:35:38 2004 172.16.0.0 admin ttyS0 0.0.0.0 start start_time=1081924137
task_id=3511 timezone=PST service=shell -lvl=0 cmd=logging console enable
```

```
Wed Apr 14 12:35:39 2004 172.16.0.0 admin ttyS0 0.0.0.0 stop stop_time=1081924137
task_id=3511    timezone=PST service=shell priv-lvl=0 cmd=logging console enable
```

In addition to command accounting, the WAAS device records any executed CLI command in the system log (*syslog.txt*). The message format is as follows:

```
ce_syslog(LOG_INFO, CESH_PARSER, PARSER_ALL, CESH_350232,
"CLI_LOG %s: %s \n", __FUNCTION__, pd->command_line);
```

Related Commands[debug](#)[show aaa accounting](#)

(config) adapter

To enable the EndPoint Mapper (EPM) service, use the **adapter** global configuration command. To disable the EPM service, use the **no** form of the command.

adapter epm enable

Syntax Description

epm	Specifies the Microsoft PortMapper adapter.
enable	Enables the EPM service.

Defaults

The EPM service is enabled by default when you upgrade to WAAS software release 4.0.3 and later releases. The EPM service is disabled by default on new WAE appliances or when you restore the factory default settings.

Command Modes

global configuration

Device Modes

application-accelerator
 replication-accelerator
 central-manager

Usage Guidelines

Use the **adapter epm enable** command to enable EPM service when the Microsoft PortMapper adapter is installed.

Examples

The following example enables the EPM service:

```
WAE(config)# adapter epm enable
```

Related Commands

[show adapter](#)
[show statistics epm](#)

(config) alarm overload-detect

To detect alarm overload situations, use the **alarm overload-detect** global configuration command.

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

Syntax	Description
clear	Specifies the threshold at which the alarm overload state on the WAAS device is cleared. When the alarm drops below this threshold, the alarm is cleared and the SNMP traps and alarm notifications are again sent to your NMS. Note The alarm overload-detect clear value must be less than the alarm overload-detect raise value.
<i>1-999</i>	Number of alarms per second that ends an alarm overload condition.
raise	(Optional) Specifies the threshold at which the WAAS device enters an alarm overload state and SNMP traps and alarm notifications to your network management station (NMS) are suspended.
enable	Enables the detection of alarm overload situations.
<i>10-1000</i>	Number of alarms per second that triggers an alarm overload.

Defaults

clear: 1 alarm per second

raise: 10 alarms per second

Command Modes

global configuration

Device Modes

application-accelerator

replication-accelerator

central-manager

Usage Guidelines

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

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

- An alarm overload notification is sent to SNMP and the NMS. The **clear** and **raise** values are also communicated to SNMP and the NMS.
- SNMP traps and NMS notifications for subsequent alarm raise and clear operations are suspended.
- Alarm overload clear notification is sent.

- The WAAS device remains in the alarm overload state until the rate of incoming alarms decreases to the **clear** value.



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

Examples

The following example enables detection of alarm overload:

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

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

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

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

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

Related Commands

[show alarms](#)

(config) asset

To set the tag name for the asset tag string, use the **asset** global configuration command. To remove the asset tag name, use the **no** form of this command.

asset tag *name*

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

Defaults No default behaviors or values

Command Modes global configuration

Device Modes application-accelerator
 replication-accelerator
 central-manager

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

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

(config) authentication

To specify administrative login authentication and authorization methods for a WAAS device, use the **authentication** global configuration mode command. To selectively disable options, use the **no** form of this command.

```
authentication { configuration { local | radius | tacacs | windows-domain } enable [primary | secondary | tertiary | quaternary] | fail-over server-unreachable | login { local | radius | tacacs | windows-domain } enable [primary | secondary | tertiary | quaternary] | content-request windows-domain disconnected-mode enable }
```

Syntax	Description
configuration	Sets the administrative login authorization (configuration) parameters for the WAAS device.
local	Selects the local database method as a login authorization (configuration) method for the WAAS device.
radius	Selects the RADIUS method as a login authorization (configuration) method for the WAAS device.
tacacs	Selects the TACACS+ method as a login authorization (configuration) method for the WAAS device.
windows-domain	Selects the Windows domain controller method as a login authorization (configuration) method for the WAAS device.
enable	Enables the specified administrative login authorization methods for the WAAS device.
primary	(Optional) Specifies the first method the WAAS device should use for administrative login authorization.
secondary	(Optional) Specifies the second method the WAAS device should use for administrative login authorization if the primary method fails.
tertiary	(Optional) Specifies the third method the WAAS device should use for administrative login authorization if the primary and secondary methods fail.
quaternary	(Optional) Specifies the fourth method the WAAS device should use for administrative login authorization if the primary, secondary, and tertiary methods all fail.
fail-over server-unreachable	Specifies that the WAAS device is to query the secondary authentication database if the primary authentication server is unreachable.
login	Sets the administrative login authentication parameters for the WAAS device.
local	Selects the local database method as an administrative login authentication method for the WAAS device.
radius	Selects the RADIUS method as an administrative login authentication method for the WAAS device.
tacacs	Selects the TACACS+ method as an administrative login authentication method for the WAAS device.
windows-domain	Selects the Windows domain controller method as an administrative login authentication method for the WAAS device.

enable	Enables the selected administrative login authentication methods for the WAAS device.
primary	(Optional) Specifies the first method the WAAS device should use for administrative login authentication.
secondary	(Optional) Specifies the second method the WAAS device should use for administrative login authentication if the primary method fails.
tertiary	(Optional) Specifies the second method the WAAS device should use for administrative login authentication if the primary method fails.
quaternary	(Optional) Specifies the fourth method the WAAS device should use for administrative login authentication if the primary, secondary, and tertiary methods all fail.
content-request	Authenticates a request for content. Note This option is available in the application-accelerator device mode only.
windows-domain	Selects a Windows domain controller for domain server authentication.
disconnected-mode	Authenticates in the disconnected mode.
enable	Enables authentication in the disconnected mode.

Defaults

The local authentication method is enabled by default.

Command Modes

global configuration

Device Modes

application-accelerator
 replication-accelerator
 central-manager

Usage Guidelines

The **authentication** command configures both the authentication and authorization methods that govern login and configuration access to the WAAS device.

**Note**

We strongly recommend that you use the WAAS Central Manager GUI instead of the WAAS CLI to configure administrative login authentication and authorization for your WAAS devices, if possible. For information about how to use the WAAS Central Manager GUI to centrally configure administrative login authentication and authorization on a single WAE or group of WAEs, which are registered with a WAAS Central Manager, see the *Cisco Wide Area Application Services Configuration Guide*.

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

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

The **authentication login tacacs** and **authentication configuration tacacs** commands use a remote TACACS+ server to determine the level of user access. WAAS software supports only TACACS+ and not TACACS or Extended TACACS.

To configure TACACS+, use the **authentication** and **tacacs** commands. To enable TACACS+, use the **tacacs enable** command. For more information on TACACS+ authentication, see the “(config) tacacs” command.

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

By default, the local method is enabled, with TACACS+ and RADIUS both disabled for login and configuration. Whenever TACACS+ and RADIUS are disabled, local is automatically enabled. TACACS+, RADIUS, and local methods can be enabled at the same time.

The **primary** option specifies the first method to attempt for both login and configuration; the **secondary** option specifies the method to use if the primary method fails. The **tertiary** option specifies the method to use if both primary and secondary methods fail. The **quaternary** option specifies the method to use if the primary, secondary, and tertiary methods fail. If all methods of an **authentication login** or **authentication configuration** command are configured as primary, or all as secondary or tertiary, local is attempted first, then TACACS+, and then RADIUS.

Enforcing Authentication with the Primary Method

The **authentication fail-over server-unreachable** global configuration command allows you to specify that failover to the secondary authentication method should occur only if the primary authentication server is unreachable. This feature ensures that users gain access to the WAAS device using the local database only when remote authentication servers (TACACS+ or RADIUS) are unreachable. For example, when a TACACS+ server is enabled for authentication with user authentication failover configured and the user tries to log in to the WAAS device using an account defined in the local database, login fails. Login succeeds only when the TACACS+ server is unreachable.

Login Authentication and Authorization Through the Local Database

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

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

Specifying RADIUS Authentication and Authorization Settings

To configure RADIUS authentication on a WAAS device, you must first configure a set of RADIUS authentication server settings on the WAAS device by using the **radius-server** global configuration command. (See the “(config) radius-server” command.)

Use the **authentication login radius** global configuration command to enable RADIUS authentication for normal login mode.

Use the **authentication configuration radius** global configuration command to enable RADIUS authorization.

To disable RADIUS authentication and authorization on a WAAS device, use the **no** form of the **authentication** global configuration command (for example, use the **no authentication login radius enable** command to disable RADIUS authentication).

Specifying TACACS+ Authentication and Authorization Settings

To configure TACACS+ authentication on WAAS devices, you must configure a set of TACACS+ authentication settings on the WAAS device by using the **tacacs** global configuration command. (See the “(config) **tacacs**” command.)

Server Redundancy

Authentication servers can be specified with the **tacacs host** or **radius-server host** global configuration commands. In the case of TACACS+ servers, the **tacacs host hostname** command can be used to configure additional servers. These additional servers provide authentication redundancy and improved throughput, especially when WAAS device load-balancing schemes distribute the requests evenly between the servers. If the WAAS device cannot connect to any of the authentication servers, no authentication takes place and users who have not been previously authenticated are denied access.

Specifying Windows Domain Login Authentication

You can enable Windows domain as an administrative login authentication and authorization method for a device or device group. Before you enable Windows authentication, you must first configure the Windows domain controller by using the using the **windows-domain wins-server** global configuration command. (See the “(config) **windows-domain**” command.)

We recommend that you use the WAAS Central Manager GUI instead of the WAAS CLI to configure Windows domain controller settings. See Chapter 6 of the *Cisco Wide Area Application Services Configuration Guide*.

Examples

The following example shows how to query the secondary authentication database if the primary authentication server is unreachable, enter the following command. This feature is referred to as the fail-over server-unreachable feature.

```
WAE(config)# authentication fail-over server-unreachable
```

If you enable the fail-over server-unreachable feature on the WAAS device, only two login authentication scheme (a primary and secondary scheme) can be configured on the WAAS device. The WAAS device fails over from the primary authentication scheme to the secondary authentication scheme only if the specified authentication server is unreachable.

To enable authentication privileges using the local, TACACS+, RADIUS, or Windows databases, and to specify the order of the administrative login authentication use the **authentication login** global configuration command. The following example shows that RADIUS is specified as the primary method, TACACS+ is specified as the secondary method, Windows as the third method, and the local database as the fourth method. In this example, four login authentication methods are specified because the fail-over server-unreachable feature is not enabled on the WAAS device.

```
WAE(config)# authentication login radius enable primary
WAE(config)# authentication login tacacs enable secondary
WAE(config)# authentication login windows-domain enable tertiary
WAE(config)# authentication login local enable quaternary
```



Note

If you have enabled the failover server unreachable feature on the WAAS device, make sure that you specify either **TACACS+** or **RADIUS** as the primary scheme for authentication, and specify local as the secondary scheme for authentication.

To enable authorization privileges using the local, TACACS+, RADIUS, or Windows databases, and to specify the order of the administrative login authorization (configuration), use the **authentication configuration** global configuration command.



Note Authorization privileges apply to console and Telnet connection attempts, secure FTP (SFTP) sessions, and Secure Shell (SSH, Version 1 and Version 2) sessions.

We strongly recommend that you set the administrative login authentication and authorization methods in the same order. For example, configure the WAAS device to use RADIUS as the primary login method, TACACS+ as the secondary login method, Windows as the tertiary method, and the local method as the quaternary method for both administrative login authentication and authorization.

The following example shows that RADIUS is specified as the primary method, TACACS+ as the secondary method, Windows as the third method, and the local database as the fourth method. In this example, four login authorization (configuration) methods are specified because the fail-over server-unreachable feature is not enabled on the WAAS device.

```
WAE(config)# authentication configuration radius enable primary
WAE(config)# authentication configuration tacacs enable secondary
WAE(config)# authentication configuration windows-domain enable tertiary
WAE(config)# authentication configuration local enable quaternary
```



Note If you have enabled the failover server unreachable feature on the WAAS device, make sure that you specify either **TACACS+** or **RADIUS** as the primary scheme for authorization (configuration), and specify local as the secondary scheme for authorization (configuration).

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

```
WAE# show authentication user

Login Authentication:      Console/Telnet/Ftp/SSH Session
-----
local                    enabled (primary)
Windows domain           enabled
Radius                   disabled
Tacacs+                  disabled

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

Related Commands

(config) radius-server
 show authentication
 show statistics radius
 show statistics tacacs
 (config) tacacs
 windows-domain
 (config) windows-domain

(config) authentication strict-password-policy

To activate strong password policy on a WAAS device, use the **authentication strict-password-policy** global configuration command. To deactivate strong password policy and use standard password policy on a WAAS device, use the **no** form of this command.

authentication strict-password-policy

Syntax Description

This command has no arguments or keywords.

Defaults

Strong password policy is enabled on the WAAS device.

Command Modes

global configuration

Device Modes

application-accelerator
 replication-accelerator
 central-manager

Usage Guidelines

When strong password policy is enabled, user passwords must meet the following requirements:

- The password must be at least 11 characters long.
- The password can include both uppercase and lowercase letters (A–Z and a–z), numbers (0–9), and special characters including ~`!@#%&*()_+=[\] ; : , < / > .
- The password cannot contain all the same characters (for example, **99999**).
- The password cannot contain consecutive characters (for example, **12345**).
- The password cannot be the same as the username.
- User passwords expire within 90 days. Each new password must be different from the previous 12 passwords.
- The password cannot contain the characters ` ` | (apostrophe, double quote, or pipe) or any control characters.

When strong password policy is disabled, user passwords must meet the following requirements:

- The password must be 1 to 34 characters long.
- The password can include both uppercase and lowercase letters (A–Z and a–z), and numbers (0–9).
- The password cannot contain the characters ` ` | (apostrophe, double quote, or pipe) or any control characters.



Note

When strong password policy is enabled, existing standard-policy passwords will still work. However, these passwords are subject to expiration under the strong password policy.

Examples

The following example enables strong password policy:

```
WAE(config)# authentication strict-password-policy
```

The following example disables strong password policy:

```
WAE(config)# no authentication strict-password-policy
```

Related Commands

[clear users](#)

[\(config\) authentication](#)

(config) auto-register

To enable discovery of a Fast Ethernet or Gigabit Ethernet WAE and its automatic registration with the WAAS Central Manager through Dynamic Host Configuration Protocol (DHCP), use the **auto-register** global configuration command. To disable the autoregistration feature on a WAE, use the **no** form of this command.

auto-register enable [**FastEthernet** *slot/port* | **GigabitEthernet** *slot/port*]

Syntax	Description
enable	Enables the automatic registration of devices using DHCP with the WAAS Central Manager.
FastEthernet	(Optional) Selects a Fast Ethernet interface for automatic registration using DHCP.
<i>slot/port</i>	Fast Ethernet slot (0–3) and port number.
GigabitEthernet	(Optional) Selects a Gigabit Ethernet interface for automatic registration using DHCP.
<i>slot/port</i>	Gigabit Ethernet slot (1–2) and port number.

Defaults Automatic registration using DHCP is enabled on a WAE by default.

Command Modes global configuration

Device Modes application-accelerator

Usage Guidelines Autoregistration automatically configures network settings and registers WAEs with the WAAS Central Manager. On bootup, devices running WAAS software (with the exception of the WAAS Central Manager itself) automatically discover the WAAS Central Manager and register with it. The administrator does not have to do any manual configuration on the device. Once the WAE is registered, the administrator approves the device and configures it remotely using the WAAS Central Manager GUI.

The **auto-register enable** command allows a Fast Ethernet or Gigabit Ethernet WAE to discover the hostname of the WAAS Central Manager through DHCP and to automatically register the device with the WAAS Central Manager. Discovery and registration occur at bootup.

To assign a static IP address using the **interface GigabitEthernet slot/port** command, the automatic registration of devices through DHCP must be disabled by using the **no auto-register enable** command, because automatic registration through DHCP is enabled by default.

For autoregistration to work, you must have a DHCP server that is configured with the hostname of the WAAS Central Manager and that is capable of handling vendor class option 43.



Note

The form of DHCP used for autoregistration is *not* the same as the interface-level DHCP that is configurable through the **ip address dhcp** interface configuration command.

The DHCP server needs to send the vendor class option (option 43) information to the WAAS device in the format for encapsulated vendor-specific options as provided in RFC 2132. The relevant section of RFC 2132, Section 8.4, is reproduced here as follows:

You should encode the encapsulated vendor-specific options field as a sequence of code/length/value fields of syntax identical to that of the DHCP options field with the following exceptions:

1. There should not be a “magic cookie” field in the encapsulated vendor-specific extensions field.
2. Codes other than 0 or 255 may be redefined by the vendor within the encapsulated vendor-specific extensions field but should conform to the tag-length-value syntax defined in section 2.
3. Code 255 (END), if present, signifies the end of the encapsulated vendor extensions, not the end of the vendor extensions field. If no code 255 is present, then the end of the enclosing vendor-specific information field is taken as the end of the encapsulated vendor-specific extensions field.

In accordance with the RFC standard, the DHCP server needs to send the WAAS Central Manager hostname information in code/length/value format. (Code and length are single octets.) The code for the WAAS Central Manager hostname is 0x01. DHCP server management and configuration are not within the scope of the autoregistration feature.

The WAAS device sends CISCOCDN as the vendor class identifier in option 60 to facilitate device groupings by customers.

Autoregistration DHCP also requires that the following options be present in the DHCP server’s offer to be considered valid:

- Subnet-mask (option 1)
- Routers (option 3)
- Domain-name (option 15)
- Domain-name-servers (option 6)
- Host-name (option 12)

Interface-level DHCP requires only subnet-mask (option 1) and routers (option 3) for an offer to be considered valid; domain-name (option 15), domain-name-servers (option 6), and host-name (option 12) are optional. All of the above options, with the exception of domain-name-servers (option 6), replace the existing configuration on the system. The domain-name-servers option is added to the existing list of name servers with the restriction of a maximum of eight name servers.

Autoregistration is enabled by default on the first interface of the device. The first interface depends on the WAE model as follows:

- For the WAE-511, WAE-512, WAE-611, WAE-612, and WAE-7320, use GigabitEthernet 1/0.

If you do not have a DHCP server, the device is unable to complete autoregistration and eventually times out. You can disable autoregistration at any time after the device has booted and proceed with manual setup and registration.

Examples

The following example enables autoregistration on GigabitEthernet port 2/0:

```
WAE(config)# auto-register enable GigabitEthernet 2/0
```

The following example disables autoregistration on all configured interfaces on the WAE:

```
WAE(config)# no auto-register enable
```

Related Commands

[show auto-register](#)

show running-config

show startup-config

(config) banner

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

```
banner enable | { exec | login | motd } [message text]
```

Syntax Description

enable	Enables banner support on the WAE.
exec	Configures an EXEC banner.
message	(Optional) Specifies a message to be displayed when an EXEC process is created.
<i>text</i>	Message text on a single line. The WAE translates the \n portion of the message to a new line when the banner is displayed to the user.
login	Configures a login banner.
motd	Configures an MOTD banner.

Defaults

Banner support is disabled by default

Command Modes

global configuration

Usage Guidelines

You can configure the following three types of banners in any device mode:

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



Note

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

The **message** keyword is optional. If you enter a carriage return without specifying the **message** keyword, you will be prompted to enter your message text. For message text on one or more lines, press the **Return** key or enter delimiting characters (\n) to specify a message to appear on a new line. You can enter up to a maximum of 980 characters, including new-line characters (\n). Enter a period (.) at the beginning of a new line to save the message and return to the prompt for the global configuration mode.



Note

The EXEC banner content is obtained from the command-line input that the user enters after being prompted for the input.

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

**Note**

When you run an SSH version 1 client and log in to the WAE, 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 WAE.

Examples

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

```
WAE(config)# banner motd message This is a WAAS 4.0.7 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 WAE translates the \n portion of the message to a new line when the MOTD message is displayed to the user.

```
WAE(config)# banner motd message "This is the motd message.
\nThis is a WAAS 4.0.7 device\n"
```

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

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

The following example shows how to enable banner support:

```
WAE(config)# banner enable
```

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

```
WAE(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 WAAS username and password to log in to this WAE.\n
.
Message has 99 characters.
WAE(config)#
```

Assume that a WAE 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 WAE, the user will see a login session that includes a MOTD banner and a login banner that asks the user to enter a login password as follows:

```
This is the motd banner.
This is a WAAS 4.0.7 device
This is login banner.
Use your password to login.

Cisco Wide Area Application Services Engine

admin@wae's password:
```

After the user enters a valid login password, the EXEC banner is displayed, and the user is asked to enter the WAAS 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 WAAS username and password to log in to this WAE.

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

```
WAE#
```

Related Commands [show banner](#)

(config) bypass

To configure static bypass lists on a WAE, use the **bypass** global configuration command. To disable the bypass feature (clear the static bypass lists), use the **no** form of this command.

```
bypass static { clientip | any-client } { serverip | any-server }
```

Syntax Description	static	Adds a static entry to the bypass list.
	<i>clientip</i>	Requests from this IP address bypass the WAE.
	any-client	Bypasses the traffic from any client destined to a particular server.
	<i>serverip</i>	Requests from this IP address bypass the WAE.
	any-server	Requests from a specified client to any server bypass the WAE.

Defaults No default behaviors or values

Command Modes global configuration

Device Modes application-accelerator

Usage Guidelines Using a static bypass allows traffic flows between a configurable set of clients and file servers to bypass handling by the WAE. By configuring static bypass entries on the Edge WAE, you can control traffic interception without modifying the router configuration. Separately, if so desired, IP access lists may be configured on the router to bypass traffic without first redirecting it to the Edge WAE. Typically, the WCCP accept list defines the group of file servers that are cached (and the file servers that are not). Static bypass can be used in rare cases when you want to prevent WAAS from caching a connection from a certain client to a certain file server (or from a certain client to all file servers).

The **bypass static** command permits traffic from specified sources to bypass the WAE. Wildcards in either the client or server IP addresses are not supported.



Note

We recommend that you use IP access lists on the WCCP-enabled router, rather than using the static bypass feature, because access lists are more efficient.

Examples The following example forces traffic from a specified client to a specified server to bypass the WAE:

```
WAE(config)# bypass static 10.1.17.1 172.16.7.52
```

The following example forces all traffic destined to a specified server to bypass the WAE:

```
WAE(config)# bypass static any-client 172.16.7.52
```

The following example forces all traffic from a specified client to any file server to bypass the WAE:

```
WAE(config)# bypass static 10.1.17.1 any-server
```

A static list of source and destination addresses helps to isolate instances of problem-causing clients and servers. To display static configuration list items, use the **show bypass list** command as follows:

```
WAE# show bypass list
Client          Server          Entry type
-----
10.1.17.1:0     172.16.7.52:0  static-config
any-client:0    172.16.7.52:0  static-config
10.1.17.2:0     any-server:0    static-config
```

Related Commands [show bypass](#)

(config) cdp

To configure the Cisco Discovery Protocol (CDP) options globally on all WAAS device interfaces, use the **cdp** command in global configuration mode.

cdp { **enable** | **holdtime** *seconds* | **timer** *seconds* }

Syntax	Description
enable	Enables CDP globally.
holdtime	Sets the length of time in seconds that a receiver keeps CDP packets before they are discarded. The default is 180 seconds.
<i>seconds</i>	Length of time that a receiver keeps the CDP packet in seconds (10–255).
timer	Interval between the CDP advertisements in seconds. The default is 60 seconds.
<i>seconds</i>	Interval in seconds (5–254).

Defaults

holdtime: 180 seconds

timer: 60 seconds

Command Modes

global configuration

Device Modes

application-accelerator

replication-accelerator

central-manager

Usage Guidelines

When enabled with the **cdp enable** command, CDP obtains protocol addresses of neighboring devices and discovers the platform of those devices. It also shows information about the interfaces used by your device. CDP is media- and protocol-independent and runs on Cisco-manufactured equipment.

Use of SNMP with the CDP MIB allows network management applications to learn the device type and the SNMP agent address of neighboring devices and to send SNMP queries to those devices. Cisco Discovery Protocol uses the CISCO-CDP-MIB.

Each device configured for CDP sends periodic messages, known as advertisements, to a multicast address. The **cdp timer** *seconds* command specifies the rate at which CDP packets are sent. Each device advertises at least one address at which it can receive SNMP messages. The advertisements also contain Time-To-Live or hold-time information. To set the hold time, use the **cdp holdtime** *seconds* command to specify the period of time in seconds that a receiver is to keep CDP packets. Each device also listens to the periodic CDP messages sent by others to learn about neighboring devices.

Examples

The following example shows that CDP is first enabled, the hold time is set to 10 seconds for keeping CDP packets, and then the rate at which CDP packets are sent (15 seconds) is set:

```
WAE(config)# cdp enable
WAE(config)# cdp holdtime 10
WAE(config)# cdp timer 15
```

Related Commands

[\(config-if\) cdp](#)

[clear](#)

[show cdp](#)

(config) central-manager

To specify the WAAS Central Manager's role and port number, use the **central-manager** global configuration command in central-manager device mode. To specify the IP address or hostname of the WAAS Central Manager with which a WAE is to register, use the **central-manager** global configuration command in application-accelerator device mode. To negate these actions, use the **no** form of this command.

```
central-manager {address {hostname | ip-address} | role {primary | standby} | ui port port-num}
```

Syntax Description

address	Specifies the hostname or IP address of the WAAS Central Manager with which the WAE should register.
<i>hostname</i>	Hostname of the WAAS Central Manager with which the WAE should register.
<i>ip-address</i>	IP address of the WAAS Central Manager with which the WAE should register.
role	Configures the WAAS Central Manager role to either primary or standby.
primary	Configures the WAAS Central Manager to be the primary WAAS Central Manager for the WAEs that are registered with it.
standby	Configures the WAAS Central Manager to be the standby WAAS Central Manager for the WAEs that are registered with it.
ui	Configures the WAAS Central Manager GUI port address.
port	Configures the WAAS Central Manager GUI port. The default is port 8443.
<i>port-num</i>	Port number (1–65535).



Note

The **address** option works in the application-accelerator device mode only. The **role** and **ui port** options work in the central-manager device mode only.

Defaults

The WAAS Central Manager GUI is preconfigured to use port 8443.

Command Modes

global configuration

Device Modes

application-accelerator

replication-accelerator

central-manager

Usage Guidelines

The **central-manager address** global configuration command associates a WAE device with the WAAS Central Manager so that the device can be approved as a part of the WAAS network. After the device is configured with the WAAS Central Manager 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 WAAS Central Manager.

If you change the WAAS Central Manager GUI port number, the Centralized Management System (CMS) service is automatically restarted on the WAAS Central Manager if the **cms enable** global configuration command on the WAAS Central Manager.

Configuring Devices Inside a NAT

In a WAAS network, there are two methods for a WAAS device that is registered with the WAAS Central Manager (WAEs or a standby WAAS Central Manager) to obtain configuration information from the primary WAAS Central Manager. The primary method is for the device to periodically poll the primary WAAS Central Manager on port 443 to request a configuration update. You cannot configure this port number. The backup method is when the WAAS Central Manager 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. WAAS networks do not work reliably if devices registered with the WAAS Central Manager are unable to poll the WAAS Central Manager for configuration updates.

All of the above methods become complex in the presence of Network Address Translation (NAT) firewalls. When a WAAS device (WAEs at the edge of the network and the primary or standby WAAS Central Managers) 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 WAAS Central Manager. 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 WAAS Central Manager 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 WAAS Central Manager's inside local IP address on its NAT, and using this address, rather than the WAAS Central Manager's inside local IP address, in the **central-manager address ip-address** global configuration command when you register the device to the WAAS Central Manager. If a WAAS device is inside a NAT and the WAAS Central Manager is outside the NAT, you can allow the WAAS device to poll for getUpdate requests by configuring a static translation (inside global IP address) for the WAAS device'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 WAAS Central Managers

The Cisco WAAS software implements a standby WAAS Central Manager. This process allows you to maintain a copy of the WAAS network configuration. If the primary WAAS Central Manager fails, the standby can be used to replace the primary.

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

**Note**

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

Switching a WAAS Central Manager from Warm Standby to Primary

If your primary WAAS Central Manager becomes inoperable, you can manually reconfigure one of your warm standby WAAS Central Managers to be the primary WAAS Central Manager. Configure the new role by using the global configuration **central-manager role primary** command as follows:

```
WAE# configure
WAE(config)# central-manager role primary
```

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

**Caution**

If you switch a warm standby WAAS Central Manager to primary while your primary WAAS Central Manager is still online and active, both WAAS Central Managers detect each other, automatically shut themselves down, and disable management services. The WAAS Central Managers are switched to halted, which is automatically saved in flash memory. For information about how to return halted WAAS Central Managers to an online status, see the *Cisco Wide Area Application Services Configuration Guide*.

**Caution**

When you switch a WAAS Central Manager from primary to standby, the configuration on the Central Manager is erased. The Central Manager, after becoming a standby, will begin replicating its configuration information from whichever Central Manager is now the primary. If standby and primary units are not synchronized before switching roles, important configuration information can be lost. Before you use this command, see the *Cisco Wide Area Application Services Configuration Guide*.

Examples

The following example specifies that the WAAS device named waas-cm is to function as the primary WAAS Central Manager for the WAAS network:

```
waas-cm(config)# central-manager role primary
```

The following example specifies the WAE should register with the WAAS Central Manager that has an IP address of 10.1.1.1. This command associates the WAE with the primary WAAS Central Manager so that the WAE can be approved as a part of the WAAS network.

```
WAE(config)# central-manager address 10.1.1.1
```

The following example configures a new GUI port to access the WAAS Central Manager GUI:

```
WAE(config)# central-manager ui port 8550
```

The following example configures the WAAS Central Manager as the standby WAAS Central Manager:


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

(config) clock

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

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

Syntax Description

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

Defaults No default behavior or values

Command Modes global configuration

Device Modes application-accelerator
 replication-accelerator
 central-manager

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

Use the **clock timezone offset** command to specify a time zone, where *timezone* is the desired time zone entry listed in the table below and *0 0* is the offset (ahead or behind) UTC is in hours and minutes. (UTC was formerly known as Greenwich mean time [GMT]).

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



Note

The time zone entry is case sensitive and must be specified in the exact notation listed in [Table 3-100](#). When you use a time zone entry from the time zone table, the system is automatically adjusted for daylight saving time.

Table 3-100 Time Zone—Offsets from UTC

Time Zone	Offset from UTC
Africa/Algiers	+1
Africa/Cairo	+2
Africa/Casablanca	0
Africa/Harare	+2
Africa/Johannesburg	+2
Africa/Nairobi	+3
America/Buenos_Aires	-3
America/Caracas	-4
America/Mexico_City	-6
America/Lima	-5
America/Santiago	-4
Atlantic/Azores	-1
Atlantic/Cape_Verde	-1
Asia/Almaty	+6
Asia/Baghdad	+3

Table 3-100 Time Zone—Offsets from UTC (continued)

Time Zone	Offset from UTC
Asia/Baku	+4
Asia/Bangkok	+7
Asia/Colombo	+6
Asia/Dacca	+6
Asia/Hong_Kong	+8
Asia/Irkutsk	+8
Asia/Jerusalem	+2
Asia/Kabul	+4.30
Asia/Karachi	+5
Asia/Katmandu	+5.45
Asia/Krasnoyarsk	+7
Asia/Magadan	+11
Asia/Muscat	+4
Asia/New Delhi	+5.30
Asia/Rangoon	+6.30
Asia/Riyadh	+3
Asia/Seoul	+9
Asia/Singapore	+8
Asia/Taipei	+8
Asia/Tehran	+3.30
Asia/Vladivostok	+10
Asia/Yekaterinburg	+5
Asia/Yakutsk	+9
Australia/Adelaide	+9.30
Australia/Brisbane	+10
Australia/Darwin	+9.30
Australia/Hobart	+10
Australia/Perth	+8
Australia/Sydney	+10
Canada/Atlantic	-4
Canada/Newfoundland	-3.30
Canada/Saskatchewan	-6
Europe/Athens	+2
Europe/Berlin	+1
Europe/Bucharest	+2
Europe/Helsinki	+2

Table 3-100 Time Zone—Offsets from UTC (continued)

Time Zone	Offset from UTC
Europe/London	0
Europe/Moscow	+3
Europe/Paris	+1
Europe/Prague	+1
Europe/Warsaw	+1
Japan	+9
Pacific/Auckland	+12
Pacific/Fiji	+12
Pacific/Guam	+10
Pacific/Kwajalein	-12
Pacific/Samoa	-11
US/Alaska	-9
US/Central	-6
US/Eastern	-5
US/East-Indiana	-5
US/Hawaii	-10
US/Mountain	-7
US/Pacific	-8

Examples

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

```
WAE(config)# clock timezone US/Pacific -8 0
```

The following example negates the time zone setting on the WAAS device:

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

The following example configures daylight saving time:

```
WAE(config)# clock summertime US/Pacific date 10 October 2005 23:59 29 April 2006 23:59 60
```

Related Commands

[clock](#)

[show clock](#)

(config) cms

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

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

Syntax Description

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

Defaults

database maintenance regular: enabled
database maintenance full: enabled
connection: 30 seconds for WAAS Central Manager; 180 seconds for a WAE
incoming wait: 30 seconds
transfer: 300 seconds

Command Modes

global configuration

Device Modes

application-accelerator
 replication-accelerator
 central-manager

Usage Guidelines

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

The **cms enable** global configuration command automatically registers the node in the database management tables and enables the CMS process. The **no cms enable** global configuration command only stops the management services on the WAAS device. Use the **cms deregister EXEC** command to de-register (remove) a WAAS device from the WAAS network.

Examples

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

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

The following example shows how to enable the CMS process on a WAAS device:

```
WAE(config)# cms enable
Generating new RPC certificate/key pair
Restarting RPC services

Creating database backup file emerg-debug-db-01-25-2006-15-31.dump
Registering Wide Area Central Manager...
Registration complete.
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 Wide Area Central Manager UI.
management services enabled
```

Related Commands

[cms](#)
[show cms](#)

(config) device mode

To configure the device mode for the WAAS device, use the **device mode** global configuration command. To reset the mode of operation on your WAAS device, use the **no** form of this command.

device mode { **application-accelerator** | **replication accelerator** | **central-manager** }

Syntax Description

application-accelerator	Configures the WAAS device to function as a WAAS Accelerator. All of your Edge WAEs and Core WAEs should be operating in this mode or replication-accelerator mode.
replication-accelerator	Configures the WAAS device to function as a WAAS Accelerator for data center replication applications. All Core WAEs participating in the replication must be in replication-accelerator mode.
central-manager	Configures the WAAS device to function as a WAAS Central Manager.

Defaults

The default device operation mode is application-accelerator.

Command Modes

global configuration

Device Modes

application-accelerator
replication-accelerator
central-manager

Usage Guidelines

You must deploy the WAAS Central Manager on a dedicated appliance. In the WAAS 4.0 software release, the device mode feature was added, which allows you to deploy a WAAS device as either a WAAS Central Manager or a WAE. A WAAS device can operate in one device mode only. The set of WAAS CLI commands that are available vary based on the device mode of the WAAS device.



Note

A WAAS Central Manager is the device management station of a WAAS network. It allows you to centrally configure, manage, and monitor your WAEs.

By default, a WAAS device uses the application-accelerator mode, which makes it operate as a Wide Area Application Engine (WAE). Before you configure network settings for your WAAS Central Managers using the WAAS CLI, you must change the device mode to central-manager.

After you have changed the device mode to central-manager, use the **cms enable** global configuration command to enable WAAS network-related applications and services. Use the **no** form of this command to disable the WAAS network.

You cannot configure the WAE network module (any of the NME-WAE family of devices) as a Central Manger.

You can configure an inline WAE as a Central Manager, but the functionality of the inline feature will not be available.

Examples

The following example shows how to specify central manager as the device mode of a WAAS device:

```
WAE(config)# device mode central-manager
```

The following example shows how to specify application accelerator as the device mode of a WAAS device:

```
WAE(config)# device mode application-accelerator
```

The following example shows how to specify replication accelerator as the device mode of a WAAS device:

```
WAE(config)# device mode replication-accelerator
```

The following example shows how to change the device mode from central-manager to application-accelerator or replication-accelerator:

**Note**

You must first use the **cms deregister force** command in EXEC mode to disable the Centralized Management System on the Central Manager, and then use the **device mode** command in global configuration mode.

```
WAE# cms deregister force
WAE(config)# device mode application-accelerator
WAE# copy running-config startup-config
```

Related Commands

[show device-mode](#)

(config) disk disk-name

To disable the disk for online removal, use the **disk disk-name** global configuration command. To reenablen the disk, use the **no** form of this command.

disk disk-name diskxx shutdown [force]

Syntax Description		
<i>diskxx</i>		Name of the disk (disk00-disk05).
shutdown		Disables the disk for maintenance.
force		(Optional) When used with the no form of this command, forces a disk to be reenabled.
		This option is not available on RAID-5 systems.

Defaults Disks enabled

Command Modes global configuration

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines This command replaces the **disk mark EXEC** mode command.

This command is not available on the WAE-7341 and WAE-7371 models. Instead, use the **disk disk-name diskxx replace EXEC** mode command.

Logical Disk Handling with RAID-1

RAID-1 is implemented in WAAS as a software feature. A RAID-1 WAAS device can use two disk drives to increase reliability. RAID-1 provides disk mirroring (data is written redundantly to two or more drives). The goal is higher reliability through redundancy. With RAID-1, file system write performance may be affected because each disk write must be executed against two disk drives. RAID-1 (mirroring) is used for all file systems on the RAID-1 device. This setup ensures reliable execution of the software in all cases.



Note

The WAAS software uses the CONTENT file system for both the Wide Area File Services (WAFS) file system and the data redundancy elimination (DRE) cache.

Hot Swap for WAE-612, WAE-7326, WAE-7341, and WAE-7371 Disk Drives

This release of WAAS supports hot swap functionality for both failed disk replacement and scheduled disk maintenance. On the WAE-612 and WAE-7326, use the **disk disk-name diskxx shutdown** global configuration command to manually shut down a disk for scheduled disk maintenance. On the

WAE-7341 and WAE-7371, use the **disk disk-name diskxx replace** EXEC command to manually shut down a disk for scheduled disk maintenance. (For the schedule disk maintenance procedure, see the *Cisco Wide Area Application Services Configuration Guide*, Chapter 14.)

You must wait for the disk to be completely shut down before you physically remove the disk from the WAE. When the RAID removal process is complete, WAAS generates a disk failure alarm and trap. In addition, a syslog ERROR message is logged.

If the software removes a failed disk during the RAID rebuild process, a RAID rebuild failure alarm is generated. If you administratively shut down the disk during the RAID rebuild process, a RAID rebuild abort alarm is generated instead.

If the removal event occurs while the RAID is in the rebuild process, the RAID removal process may take up to one minute before it is successful. The exact duration of this process depends on the size of the disk.

Automatic Failed Disk Handling for RAID-1

The disk hot swap functionality automatically disables a failed disk if the system detects one critical disk alarm. The software will remove the failed disk automatically regardless of the setting for **disk error-handling**.

Replacing a Failed Disk

To administratively disable disks for removal, use the **disk disk-name** command in global configuration mode. To administratively reenable disks after replacement, use the **no** form of this command.

When a disk is manually shutdown, it remains shutdown until you enter the **no disk disk-name diskxx shutdown** command.

For RAID-1 devices, you may replace a disk that was previously identified as a bad disk by using the **disk disk-name diskxx shutdown force** command in global configuration mode to manually override the bad status.

Disk Information

To identify which disks have been identified as failed or bad, use the **show disks failed-disk-id** EXEC command. Do not reinsert any disk with a serial number shown in this list.



Note

The **show disks failed-disk-id** EXEC command is not available on WAE-7341 and WAE-7371 models.

Related Commands

[\(config\) disk error-handling](#)
[\(config\) disk logical shutdown](#)
[disk](#)
[show disks](#)

(config) disk encrypt enable

To enable disk encryption, use the **disk encrypt enable** global configuration command. To disable disk encryption, use the **no** form of this command.

disk encrypt enable

Syntax Description

There are no keywords or arguments for this command.

Defaults

Disk encryption is disabled by default.

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

The disk encryption feature addresses the need to securely protect sensitive information that flows through deployed ACE service module systems and that is stored in ACE service module persistent storage. Disk encryption includes two aspects: the actual data encryption on the WAE disk and the encryption key storage and management.

When you enable disk encryption, all data in ACE service module persistent storage will be encrypted. The encryption key for unlocking the encrypted data is stored on the Central Manager, and key management is handled by the Central Manager. When you reboot the WAE after configuring disk encryption, the WAE retrieves the key from the Central Manager, allowing normal access to the data that is stored in ACE service module persistent storage.

Disk encryption requirements are as follows:

- You must have a Central Manager configured for use in your network.
- Your WAE devices must be registered with the Central Manager.
- Your WAE devices must be online (have an active connection) with the Central Manager. This requirement applies only if you are enabling disk encryption.
- You must reboot your WAE for the disk encryption configuration to take effect.

After you reboot your WAE, the encryption partitions are created using the new key, and any previously existing data is removed from the partition.

Any change to the disk encryption configuration, whether to enable or disable encryption, causes the disk to clear its cache. This feature protects sensitive customer data from being decrypted and accessed should the WAE ever be stolen.

If you enable disk encryption and then downgrade to a software version that does not support this feature, you cannot use the disk partitions. In such cases, you must delete the disk partitions after you downgrade.

To enable or disable disk encryption, use the **disk encrypt** global configuration command. When you enable or disable disk encryption, the file system is reinitialized during the first subsequent reboot. Reinitialization may take from ten minutes to several hours, depending on the size of the disk partitions. During this time, the WAE is accessible, but it does not provide any services.

If you change the Central Manager IP address, or if you relocate the Central Manager, or replace one Central Manager with another Central Manager that has not copied over all the information from the original Central Manager, and you reload the WAE when disk encryption is enabled, the WAE file system cannot complete the reinitialization process or obtain the encryption key from the Central Manager.

If the WAE fails to obtain the encryption key, disable disk encryption by using the **disk encrypt disable** global configuration command from the CLI, and reload the WAE. Ensure connectivity to the Central Manager before you enable disk encryption and reload the WAE. This process clears the disk cache.

To view the encryption status details, use the **show disks details** EXEC command. While the file system is initializing, **show disks details** displays the following message: “System initialization is not finished, please wait...” You may also view the disk encryption status, whether it is enabled or disabled, in the Central Manager GUI, Device Home window.

Related Commands[disk](#)[show disks](#)

(config) disk error-handling

To configure how disk errors are handled and to define a disk error-handling threshold on a WAAS device, use the **disk error-handling** global configuration command. Use the **no** form of this command to return to the default error-handling threshold.

disk error-handling { **reload** | **remap** | **threshold** *number* }

Syntax Description		
reload		Reloads the disk if the system file system (SYSFS) on disk00 has problems.
remap		Sets the disk to attempt to remap disk errors automatically.
threshold		Sets the number of disk errors allowed before the disk is marked as bad.
<i>number</i>		Number of disk errors allowed before the disk is marked as bad (0–100). The default is 10. A value of zero indicates that the disk should never be marked bad.

Defaults **error-handling threshold** *number*: 10

Command Modes global configuration

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines If you have a two-drive system, the RAID software protects the SYSFS from single-drive failures and prevents applications from seeing I/O errors. With this configuration, error handling need not be specified. For all other configurations, error handling should be specified.

To operate properly, the WAAS device must have a disk drive named disk00. The WAAS device must also contain a disk drive that contains the first SYSFS (system file system) partition. The SYSFS partition is used to store log files, including system logs and internal debugging logs. It may also be used to store image files and configuration files on a WAAS device. Disk00 always contains the SYSFS partition. When software RAID is applied, the SYSFS partitions are contained on both disk00 and disk01. In either case, the disk00 disk and the disk that contains the first SYSFS partition are called *critical drives* and are required for proper operation of the WAAS device.

When a WAE is booted and a critical disk drive is not detected at system startup time, the WAAS device runs at a degraded state. If one of the critical disk drives becomes inoperable at run time, the WAAS device can exhibit symptoms such as the applications malfunctioning or failing, or the WAAS device can stop responding. You must monitor the critical disk drives on a WAAS device and report any disk drive errors to Cisco TAC.

With a WAAS device, a disk device error is defined as any of the following events:

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

The disk status is recorded in Flash memory (nonvolatile storage). When an error occurs on the disk drive of a WAAS device, 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 WAAS device.

Specifying the Disk Error-Handling Threshold

You can define a disk device error-handling threshold on the WAAS device. If the number of disk device errors reaches the specified threshold, the corresponding disk device is automatically marked as bad. By default, this threshold is set to 10. The device does not stop using the bad disk device immediately; it stops using the bad disk drive after the next reboot.

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

If the specified threshold is exceeded, the WAAS device either records this event or reboots. If the bad disk drive is a critical disk drive, and the automatic reload feature (**disk error-handling reload** command) is enabled, then the WAAS software marks the disk drive as bad, and the WAAS device is automatically reloaded. After the WAAS device is reloaded, a syslog message and an SNMP trap are generated.

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

Examples

The following example shows how to configure five disk drive errors for a particular disk drive (for example, disk00) as the maximum number of errors allowed before the disk drive is automatically marked as bad:

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

Related Commands

[disk](#)

[show disks](#)

(config) disk logical shutdown

To shutdown the RAID-5 logical disk drive, use the **disk logical shutdown** global configuration command. To reenble the RAID-5 logical disk drive, use the **no** form of this command.

disk logical shutdown

Syntax Description

There are no keywords or arguments for this command.

Defaults

The RAID-5 array is enabled by default.

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

This command is supported on WAE-7341 and WAE-7371 models only.

Use this command to operate the WAE-7341 or WAE-7371 in diskless mode. In diskless mode, the partitions and disks are not mounted and cannot be used.

You must reload the device for this command to take effect.

(config) egress-method

To configure the egress method for intercepted connections, use the **egress-method** global configuration command.

```
egress-method {ip-forwarding | negotiated-return} intercept-method wccp
```

Syntax Description		
ip-forwarding		Configures the IP forwarding egress method.
negotiated-return		Configures the WCCP negotiated return egress method.
intercept-method		Chooses for which interception method the egress method is being configured.
wccp		Configures the egress method for WCCP interception.

Defaults The default egress method is IP forwarding.

Command Modes global configuration

Device Modes application-accelerator

Usage Guidelines WCCP interception mode supports two egress configuration options: IP forwarding and negotiated return. Negotiated return supports WCCP GRE as the WCCP egress method.

WCCP GRE packet return allows you to place WAEs on the same VLAN or subnet as clients and servers, a topology that is not allowed when using the IP forwarding egress method. For optimized flows, WCCP GRE packet return also provides “best effort” support for redundant routers and router load balancing.

When you configure WCCP GRE as the egress method, WAAS makes a best effort to maintain the original router selection when router load balancing is used in the network. WAAS applies the following logic in its router selection for WCCP GRE:

- When WAAS applies DRE and compression to a TCP flow, the number of packets sent out may be fewer, such that a single packet carrying optimized data may represent original data that was received in multiple packets redirected from different routers. That optimized data-carrying packet egresses from the WAE to the router that last redirected a packet to the WAE for that flow direction.
- When the WAE receives optimized data, the data may arrive in multiple packets from different routers. WAAS expands the optimized data back to the original data, which is sent out as several packets. Those original data-carrying packets egress from the WAE to the router that last redirected a packet to the WAE for that flow direction.

Negotiated return supports WCCP GRE as the only WCCP egress method. When WCCP negotiates WCCP L2 return, the WAE defaults to using IP forwarding as the egress method. You do not receive any notification if the negotiated egress method defaults to IP forwarding; however, a syslog message is generated if such a case occurs.

The default egress method is IP forwarding. If you do not configure the **negotiated-return** option, IP forwarding is used.

WCCP bypass flows, however, use the WCCP negotiated return method and not IP forwarding, regardless of the CLI configuration.

**Note**

The WCCP GRE egress method does not apply to the inline mode of operation.

Examples

To configure the egress method for WCCP interception mode from the Central Manager GUI, choose **Devices > Devices > Interception > Egress Methods**.

The following example shows how to configure the interception and egress method for WCCP GRE packet return from the CLI:

```
WAE(config)# egress-method negotiated-return intercept-method wccp
```

The following example shows how to configure the interception and egress method for IP forwarding from the CLI:

```
WAE(config)# egress-method ip-forwarding intercept-method wccp
```

To view the egress method that is configured and that is being used on a particular WAE, use the **show egress-methods EXEC** command or the **show tfo egress-methods connection EXEC** command.

Related Commands

[show egress-methods](#)

[show tfo egress-methods connection](#)

[\(config\) wccp tcp-promiscuous](#)

(config) end

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

end

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes global configuration

Device Modes application-accelerator
replication-accelerator
central-manager

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.
The **Ctrl-Z** command also exits global configuration mode.

Examples The following example shows how to exit global configuration mode on a WAAS device:

```
WAE(config)# end
WAE#
```

Related Commands [\(config\) exit](#)

(config) exec-timeout

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

exec-timeout *timeout*

Syntax Description	<i>timeout</i>	Timeout in minutes (0–44640).
--------------------	----------------	-------------------------------

Defaults	The default is 15 minutes.
----------	----------------------------

Command Modes	global configuration
---------------	----------------------

Device Modes	application-accelerator replication-accelerator central-manager
--------------	-----------------------------------------------------------------------

Usage Guidelines	A Telnet session or Secure Shell (SSH) session with the WAAS device can remain open and inactive for the interval of time specified by the exec-timeout command. When the exec-timeout interval elapses, the WAAS device automatically closes the Telnet or SSH session.
------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Examples	The following example configures a timeout of 100 minutes:
----------	------------------------------------------------------------

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

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

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

Related Commands	(config) telnet enable
------------------	----------------------------------------

(config) exit

To terminate global configuration mode and return to the privileged-level EXEC mode, use the **exit** command.

exit

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes All modes

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines This command is equivalent to the **Ctrl-Z** or the **end** command.

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

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

Related Commands [\(config\) end](#)

(config) external-ip

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

external-ip *ip-addresses*

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

Defaults	No default behavior or values	
-----------------	-------------------------------	--

Command Modes	global configuration	
----------------------	----------------------	--

Device Modes	application-accelerator	
---------------------	-------------------------	--

Usage Guidelines	Use this command to configure up to eight NAT IP addresses on a WAE 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.	
-------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

In a WAAS network, there are two methods for a WAE that is registered with a WAAS Central Manager to obtain configuration information from the primary WAAS Central Manager. The primary method is for the device to periodically poll the primary WAAS Central Manager on port 443 to request a configuration update. You cannot configure this port number. The backup method is when the WAAS Central Manager 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 more timely manner. You cannot configure this port number even when the backup method is being used. WAAS networks do not work reliably if devices registered with the WAAS Central Manager are unable to poll the WAAS Central Manager for configuration updates.

When a WAAS device (WAEs at the edge of the network and the primary or standby WAAS Central Managers) 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 WAAS Central Manager. All other devices inside the NAT use the inside local IP address to contact the centrally managed device that resides inside the NAT. A device that is not inside the same NAT as the centrally managed device cannot contact it without a special configuration.

If the primary WAAS Central Manager is inside a NAT, you can allow a WAAS 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 WAAS Central Manager's inside local IP address on its NAT, and using this address, rather than the WAAS Central Manager's inside local IP address in the **central manager address ip-address** global configuration command when you register the WAAS device to the WAAS Central Manager. If a WAAS device is inside a NAT and the WAAS Central Manager is outside the NAT, you can allow the WAAS device to poll for getUpdate requests by configuring a static translation (NAT IP address or inside global IP address) for the WAE inside local address on its NAT.

**Note**

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

Examples

The following example configures four external NAT IP addresses on a WAAS device:

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

Related Commands

(config) interface

(config) ip

(config-if) ip

(config) flow monitor

To enable network traffic flow monitoring and to register the WAE with the tcpstat-v1 collector for traffic analysis, use the **flow monitor** global configuration command. To disable the network traffic flow configuration, use the **no** form of this command.

```
flow monitor tcpstat-v1 {enable | host ip_address}
```

Syntax Description	monitor	Monitors the flow performance.
	tcpstat-v1	Sets the tcpstat-v1 collector configuration.
	enable	Enables flow monitoring.
	host	Specifies the collection control agent.
	ip_address	IP address of the collection control agent.

Defaults The default configuration has no host address configured and the feature is disabled.

Command Modes global configuration

Device Modes application-accelerator

Usage Guidelines For procedures to configure flow monitoring on the WAE, see the *Cisco Wide Area Application Services Configuration Guide*, Chapter 15.

For information about using the NetQoS SuperAgent console and configuring NetQoS SuperAgent entities, go to the following website: <http://www.netqos.com>

(config) help

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

help

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC and global configuration

Device Modes application-accelerator
replication-accelerator
central-manager

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

Two styles of help are provided:

- Full help is available when you are ready to enter a command argument (for example, **show ?**) and 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** global configuration command:

```
WAE# configure
WAE(config)# 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.
2. Partial help is provided when an abbreviated argument is entered.

The following example shows how to use full help to see what WCCP command arguments are available:

```
WAE# configure
WAE(config)# wccp ?
  access-list      Configure an IP access-list for inbound WCCP encapsulate
                  traffic
  flow-redirect    Redirect moved flows
  router-list      Router List for use in WCCP services
  shutdown         Wccp Shutdown parameters
  slow-start       accept load in slow-start mode
```

```
tcp-promiscuous  TCP promiscuous mode service
version          WCCP Version Number
```

The following example shows how to use partial help to determine the syntax of a WCCP argument:

```
WAE(config)# wccp tcp ?
mask          Specify mask used for CE assignment
router-list-num Router list number
```

(config) hostname

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

hostname *name*

Syntax Description

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

Defaults

The default hostname is the model number of the WAAS device (for example WAE-511, WAE-611, or WAE-7326).

Command Modes

global configuration

Device Modes

application-accelerator
 replication-accelerator
 central-manager

Usage Guidelines

Use this command to configure the hostname for the WAAS device. The hostname is used for the command prompts and default configuration filenames. This name is also used for routing, so it conforms to the following rules:

- It can use only alphanumeric characters and hyphens (-).
- The maximum length is 30 characters.
- The following characters are considered illegal and cannot be used when naming a device: @, #, \$, %, ^, &, *, (), |, \"/>, <>.

Examples

The following example changes the hostname of the WAAS device to *sandbox*:

```
WAE-511 (config) # hostname sandbox
Sandbox (config) #
```

The following example removes the hostname:

```
Sandbox (config) # no hostname
WAE-511 (config) #
```

Related Commands

[dnslookup](#)
[\(config\) ip](#)
[\(config-if\) ip](#)

■ (config) hostname

show hosts

(config) inetd enable

To enable FTP and RCP services on a WAAS device, use the **inetd enable** global configuration command. To disable these same services, use the **no** form of this command.

```
inetd enable {ftp | rcp}
```

Syntax Description

ftp	Enables FTP services.
rcp	Enables RCP services.

Defaults

FTP is enabled; RCP is disabled.

Command Modes

global configuration

Device Modes

application-accelerator
 replication-accelerator
 central-manager

Usage Guidelines

Inetd (an Internet daemon pronounced eye net dee) is a program that listens for connection requests or messages for certain ports and starts server programs to perform the services associated with those ports. Use the **inetd enable** command with the **ftp** and **rcp** keywords to enable and disable services on the WAAS device. To disable the service, enter the **no** form of the **inetd enable** command. Use the **show inetd EXEC** command to see whether current **inetd** sessions are enabled or disabled.

Examples

The following example enables an FTP service session on the WAAS device:

```
WAE(config)# inetd enable ftp
```

The following example disables FTP services:

```
WAE(config)# no inetd enable ftp
```

Related Commands

[show inetd](#)

(config) interface

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

```
interface GigabitEthernet slot/port [autosense | bandwidth {10 | 100 | 1000} | cdp enable | channel-group {1} | description text | full-duplex | half-duplex | ip {access-group {acl-num | acl_name} {in | out} | address {ip_address netmask [secondary] | dhcp [client-id id hostname name | hostname name client-id id}} | mtu mtusize | shutdown | standby grpnumber [priority priority]]
```

```
interface InlineGroup slot/grpnumber [autosense | bandwidth {10 | 100 | 1000} | failover timeout {1 | 3 | 5} | full-duplex | half-duplex | inline [vlan {all | native | vlan_list}] | shutdown]
```

```
interface PortChannel {1} [description text | ip {access-group {acl-num | acl_name} {in | out} | address ip-address netmask} | shutdown]
```

```
interface Standby grpnumber {description text | errors max-error-number | ip ip_address | no {description text | errors max-error-number | ip ip_address | shutdown} | shutdown}
```

Syntax Description

GigabitEthernet	Selects a Gigabit Ethernet interface to configure.
<i>slot/port</i>	Slot and port number for the selected interface. The slot range is 0–2; the port range is 0–3. The slot number and port number are separated with a forward slash character (/).
autosense	(Optional) Sets the GigabitEthernet interface to automatically sense the interface speed.
bandwidth	(Optional) Sets the bandwidth of the specified interface.
10	Sets the bandwidth of the interface to 10 megabits per second (Mbps).
100	Sets the bandwidth of the interface to 100 Mbps.
1000	Sets the bandwidth of the interface to 1000 Mbps. This option is not available on all ports and is the same as autosense.
cdp enable	(Optional) Enables Cisco Discovery Protocol (CDP) on the specified interface.
channel-group	(Optional) Configures the EtherChannel group.
1	Assigns the interface EtherChannel to group 1.
description	Enters a description of the interface.
<i>text</i>	Text describing this interface.
full-duplex	(Optional) Sets the interface to full-duplex operation.
half-duplex	(Optional) Sets the interface to half-duplex operation.
	Note We strongly recommend that you do not use half-duplex connections on the WAE or on routers, switches, or other devices.
ip	(Optional) Enables IP configuration commands for the interface.
access-group	Configures access control for IP packets on this interface using access control list (ACL).

<i>acl_num</i>	Numeric identifier that identifies the ACL to apply to the current interface. For standard ACLs, the valid range is 1–99; for extended ACLs, the valid range is 100–199.
<i>acl_name</i>	Alphanumeric identifier of up to 30 characters, beginning with a letter that identifies the ACL to apply to the current interface.
in	Applies the specified ACL to inbound packets on the current interface.
out	Applies the specified ACL to outbound packets on the current interface.
address	Sets the interface IP address.
<i>ip-address</i>	IP address of this interface.
<i>netmask</i>	Netmask of this interface.
secondary	(Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.
dhcp	(Optional) Sets the IP address to that negotiated over Dynamic Host Configuration Protocol (DHCP).
client-id	(Optional) Specifies the client identifier.
<i>id</i>	Client identifier.
hostname	(Optional) Specifies the hostname.
<i>name</i>	Hostname.
mtu	(Optional) Sets the interface Maximum Transmission Unit (MTU) size.
<i>mtusize</i>	MTU size in bytes (88–1500).
shutdown	(Optional) Shuts down this interface.
standby	(Optional) Sets standby interface configuration commands.
<i>grpnumber</i>	Standby group number (1–4).
priority	(Optional) Sets the priority of an interface for the standby group.
<i>priority</i>	Interface priority for the standby group (0–4294967295).
InlineGroup	Sets the InlineGroup of interfaces to configure.
<i>slotgrpnumber</i>	Slot and inline group number for the selected interface. The group number for the inline feature is either 0 or 1 (each adapter has 2 grouped pairs).
failover	(Optional) Modifies failover parameters.
timeout	Sets the maximum time for the inline group of interfaces to transfer traffic to another port in the group after a failover event.
1	Number of seconds before failover occurs.
3	Number of seconds before failover occurs.
5	Number of seconds before failover occurs.
inline	(Optional) Enables inline interception for an InlineGroup of interfaces.
vlan	(Optional) Modifies the VLAN list parameters.
all	Applies the command to all tagged and untagged packets.
native	Specifies untagged packets.
<i>vlan_list</i>	Comma-separated list of VLAN IDs. Restricts the inline feature to the specified set of VLANs.
PortChannel	Selects the EtherChannel of interfaces to configure.
1	Sets the port-channel interface number to 1.

errors	Specifies the maximum error number.
<i>max-error-number</i>	Maximum number of errors.
ip	Specifies the IP address of the interface.
<i>ip_address</i>	IP address of the interface.

Defaults

No default behavior or values

Command Modes

global configuration

Device Modes

application-accelerator

replication-accelerator

central-manager

Usage Guidelines

The **interface** command contains an option for **FibreChannel**; however, the FibreChannel interface is not supported for WAAS devices. The **interface FibreChannel** command is not documented in this Command Reference.

To configure an interface bandwidth on a WAAS device, use the **bandwidth** interface configuration command. The bandwidth is specified in megabits per second (Mbps). The **1000** Mbps option is not available on all ports. Using this option automatically enables autosense on the interface. You cannot change the interface speed on a WAE-7320 model that has an optical Gigabit Ethernet interface. Gigabit Ethernet interfaces only run at 1000 Mbps for a WAE-7320. For newer models of the WAAS device (for example, the WAE-611 or WAE-7326) that have a Gigabit Ethernet interface over copper, this restriction does not apply; you can configure these Gigabit Ethernet interfaces to run at 10, 100, or 1000 Mbps. On newer WAAS models, the 1000-Mbps setting implies autosense. For example, you cannot configure the Gigabit Ethernet interface to run at 1000 Mbps and half duplex.

Using the **cdp enable** command in global configuration mode enables CDP globally on all the interfaces. If you want to control CDP behavior per interface, then use the **cdp enable** command in interface configuration mode. The interface level control overrides the global control.

To display the interface identifiers (for example, interface GigabitEthernet 1/0), use the **show running-config** or **show startup-config** commands. The **autosense**, **bandwidth**, **full-duplex**, **half-duplex**, **ip**, and **shutdown** commands are listed separately in this command reference.

Configuring Multiple Secondary IP Addresses on a Single Physical Interface

Use the **interface secondary** global configuration command to configure more than one IP address on the same interface. By configuring multiple IP addresses on a single interface, the WAAS device can be present in more than one subnet. This configuration allows you to optimize the response time because the content goes directly from the WAAS device to the requesting client without being redirected through a router. The WAAS device becomes visible to the client because both are configured on the same subnet.

Up to four secondary addresses can be assigned to an interface. These addresses become active only after the primary address is configured. No two interfaces can have the same IP address in the same subnetwork. To set these secondary IP addresses, use the **ip address** command.

If a WAAS device has one physical interface that has multiple secondary IP addresses assigned to it, the egress traffic uses the source IP address that is chosen by IP routing. If the secondary IP addresses of a WAAS device in the same subnet as the primary IP address, then the egress traffic uses the primary IP address only. In contrast, if the secondary IP addresses are in a different subnet than the primary IP address, then the destination IP address determines which IP address on the WAAS device is used for the egress traffic.

Configuring Interfaces for DHCP

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

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

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



Note

You must disable autoregistration before you can manually configure an interface for DHCP. Autoregistration is enabled by default on the first interface of the device.

Defining Interface Descriptions

You can specify a one-line description for a specific interface on a WAAS device. Use the **description text** interface configuration command to enter the description for the specific interface. The maximum length of the description text is 240 characters. This feature is supported for the Gigabit Ethernet, port-channel, and Standby interfaces.



Note

This feature is not currently supported for the SCSI or IDE interfaces.

After you define the description for an interface, use the **show EXEC** commands to display the defined interface descriptions. Enter the **show interface interface type slot/port EXEC** command to display the defined description for a specific interface on the WAE.

Port-Channel (EtherChannel) Interface

EtherChannel for the WAAS software supports the grouping of two same-speed network interfaces into one virtual interface. This configuration allows you to set or remove a virtual interface that consists of the two integrated Gigabit Ethernet interfaces. EtherChannel also provides interoperability with Cisco routers, switches, and other networking devices or hosts supporting EtherChannel, load balancing, and automatic failure detection and recovery based on each interface's current link status.



Note

You cannot use the inline Ethernet interfaces that are located on the WAE inline network adapter to form an EtherChannel.

InlineGroup Interface

An InlineGroup interface is a logical grouping of a pair of Ethernet ports that are physically contained in the optional 4-port inline network adapter card. The inline network adapter is supported on all WAAS appliance platforms beginning with the WAAS 4.0.7 release. You can have up to two InlineGroup interfaces, which allows for two bypass-enabled paths for traffic to pass through the WAE appliance, making multiple-router deployments possible. The InlineGroup interfaces provide failover capability and can be assigned to any desired set of VLANs. (For examples of InlineGroup interface configurations, see the “(config-if) inline” command.)

You can configure the InlineGroup interface for link speed (**bandwidth** or **autosense**) and mode of operation (**half-duplex** or **full-duplex**).



Note

We strongly recommend that you do not use half-duplex connections on the WAE or on routers, switches, or other devices. Use of half-duplex impedes the system’s ability to improve performance and should not be used. Double-check each Cisco WAE interface as well as the port configuration on the adjacent device (router, switch, firewall, WAE) to verify that full-duplex is configured.

Examples

The following example configures an attribute of an interface with a single CLI command:

```
WAE(config)# interface GigabitEthernet 1/0 full-duplex
```

The following example shows that an interface can be configured in a sequence of CLI commands:

```
WAE(config)# interface GigabitEthernet 1/0
WAE(config-if)# full-duplex
WAE(config-if)# exit
WAE(config)#
```

The following example enables a shutdown interface:

```
WAE(config)# no interface GigabitEthernet 1/0 shutdown
```

The following example creates an EtherChannel. The port channel is port channel 1 and is assigned an IP address of 10.10.10.10 and a netmask of 255.0.0.0:

```
WAE# configure
WAE(config)# interface PortChannel 1
WAE(config-if)# ip address 10.10.10.10 255.0.0.0
WAE(config-if)# exit
```

The following example removes an EtherChannel:

```
WAE(config)# interface PortChannel 1
WAE(config-if)# no ip address 10.10.10.10 255.0.0.0
WAE(config-if)# exit
WAE(config)# no interface PortChannel 1
```

The following example adds an interface to a channel group:

```
WAE# configure
WAE(config)# interface GigabitEthernet 1/0
WAE(config-if)# channel-group 1
WAE(config-if)# exit
```

The following example removes an interface from a channel group:

```
WAE(config)# interface GigabitEthernet 1/0
WAE(config-if)# no channel-group 1
WAE(config-if)# exit
```

The following example assigns a secondary IP address on a Gigabit Ethernet interface on a WAAS device using the **ip address** configuration interface command:

```
WAE# configure
WAE(config)# interface GigabitEthernet 1/0
WAE(config-if)# ip address 10.10.10.10 255.0.0.0 secondary
```

The following example configures a description for a Gigabit Ethernet interface:

```
WAE(config)# interface GigabitEthernet 1/0
WAE(config-if)# description This is a GigabitEthernet interface.
```

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

```
WAE# show running-config
.
.
.
interface GigabitEthernet 1/0
  description This is an interface to the WAN
  ip address dhcp
  ip address 192.168.1.200 255.255.255.0
  no autosense
  bandwidth 100
  full-duplex
  exit
.
.
.
```

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

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

Related Commands

[show interface](#)

[show running-config](#)

[show startup-config](#)

(config) ip

To change initial network device configuration settings, use the **ip** global configuration command. To delete or disable these settings, use the **no** form of this command.

ip default-gateway *ip-address*

ip domain-name *name1 name2 name3*

ip name-server *ip-addresses*

ip path-mtu-discovery **enable**

ip route *dest_addrs net_addrs gateway_addrs*

Syntax	Description
default-gateway	Specifies the default gateway (if not routing IP).
<i>ip-address</i>	IP address of the default gateway.
domain-name	Specifies domain names.
<i>name1</i> through <i>name3</i>	Domain name (up to three can be specified).
name-server	Specifies the address of the name server.
<i>ip-addresses</i>	IP addresses of the name servers (up to a maximum of eight).
path-mtu-discovery	Configures RFC 1191 Path Maximum Transmission Unit (MTU) discovery.
enable	Enables Path MTU discovery.
route	Specifies the net route.
<i>dest_addrs</i>	Destination route address.
<i>net_addrs</i>	Netmask address.
<i>gateway_addrs</i>	Gateway address.

Defaults No default behavior or values

Command Modes global configuration

Device Modes application-accelerator
replication-accelerator
central-manager

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 WAAS device 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 WAAS device 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 WAAS device 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 WAAS device uses DNS servers. Use the **ip name-server** command to point the WAAS device to a specific DNS server. You can configure up to eight servers.

Path MTU auto discovery 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 WAAS software supports IP Path MTU Discovery, as defined in RFC 1191. When enabled, Path MTU Discovery discovers the largest IP packet size allowable between the various links along the forwarding path and automatically sets the correct value for the packet size. By using the largest MTU that the links will bear, the sending device can minimize the number of packets that it must send.



Note

IP Path MTU Discovery is useful when a link in a network goes down, forcing the use of another, different MTU-sized link. IP Path MTU Discovery is also useful when a connection is first being established and the sender has no information at all about the intervening links.

IP Path MTU Discovery is initiated by the sending device. If a server does not support IP Path MTU Discovery, the receiving device will have no mechanism available to avoid fragmenting datagrams generated by the server.

Use the **ip route** command to add a specific static route for a network or host. Any IP packet designated for the specified destination uses the configured route.

To configure static IP routing, use the **ip route** command. To remove the route, use the **no** form of this command. Do not use the **ip route 0.0.0.0 0.0.0.0** command to configure the default gateway; use the **ip default-gateway** command instead.

Examples

The following example configures a default gateway for the WAAS device:

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

The following example disables the default gateway:

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

The following example configures a static IP route for the WAAS device:

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

The following example negates the static IP route:

```
WAE(config)# no ip route 172.16.227.128 255.255.255.0 172.16.227.250
```

The following example configures a default domain name for the WAAS device:

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

The following example negates the default domain name for the WAAS device:

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

The following example configures a name server for the WAAS device:

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

The following example disables the name server for the WAAS device:

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

Related Commands [show ip routes](#)

(config) ip access-list

To create and modify access lists on a WAAS device for controlling access to interfaces or applications, use the **ip access-list** global configuration commands. To disable an access list, use the **no** form of the command.

```
ip access-list {standard | extended} {acl-name | acl-num}
```

Syntax Description		
standard	Enables standard ACL configuration mode. The CLI enters the standard ACL configuration mode in which all subsequent commands apply to the current standard access list. The (config-std-nacl) prompt appears: WAE(config-std-nacl)# See the “ Standard ACL Configuration Mode Commands ” section for details about working with entries in a standard access list and the commands available from the standard ACL configuration mode (config-std-nacl)#.	
extended	Enables extended ACL configuration mode. The CLI enters the extended ACL configuration mode in which all subsequent commands apply to the current extended access list. The (config-ext-nacl) prompt appears: WAE(config-ext-nacl)# See the “ Extended ACL Configuration Mode Commands ” section for details about working with entries in an extended access list and the commands available from the extended ACL configuration mode (config-ext-nacl)#.	
<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.	
<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.	

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

Command Modes global configuration

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines

Use access lists to control access to specific applications or interfaces on a WAAS device. An access control list consists of one or more condition entries that specify the kind of packets that the WAAS device will drop or accept for further processing. The WAAS device 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.

**Note**

IP ACLs that are defined on a router take precedence over the IP ACLs that are defined on the WAE. IP ACLs that are defined on a WAE take precedence over the WAAS application definition policies that are defined on the WAE.

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 will be 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 WAAS device 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. Therefore, you must include at least one **permit** entry to create a valid access list.

After creating an access list, you can include the access list in an access group using the **access-group** command, which determines how the access list is applied. You can also apply the access list to a specific application using the appropriate command. A reference to an access list that does not exist is the equivalent of a **permit any** condition statement.

To work with access lists, enter either the **ip access-list standard** or **ip access-list extended** global configuration command. Identify the new or existing access list with a name up to 30 characters long beginning with a letter, or with a number. If you use a number to identify a standard access list, it must be between 1 and 99; for an extended access list, use a number from 100 to 199. You must use a standard access list for providing access to the SNMP server or to the TFTP gateway/server. However, you can use either a standard access list or an extended access list for providing access to the WCCP application.

After you identify the access list, the CLI enters the appropriate configuration mode and all subsequent commands apply to the specified access list. The prompt for each configuration mode is shown in the following examples.

```
WAE(config)# ip access-list standard test
WAE(config-std-nacl)# exit
WAE(config)# ip access-list extended test2
WAE(config-ext-nacl)#
```

Examples

The following example shows how to create an access list on the WAAS device. You create this access list to allow the WAAS device to accept all web traffic that is redirected to it, but limits host administrative access using SSH:

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

The following example activates the access list for an interface:

```
WAE(config)# interface gigabitethernet 1/0
WAE(config-if)# ip access-group example in
WAE(config-if)# exit
```


The following example shows how this configuration appears when you enter the **show running-configuration** command:

```
...
!  
interface GigabitEthernet 1/0  
 ip address 10.1.1.50 255.255.0.0  
 ip access-group example in  
 exit  
...  
ip access-list extended example  
 permit tcp any any eq www  
 permit tcp host 10.1.1.5 any eq ssh  
 exit  
...  
...
```

Related Commands

[clear](#)

[\(config-if\) ip access-group](#)

[show ip access-list](#)

(config) kerberos

To authenticate a user that is defined in the Kerberos database, use the **kerberos** global configuration command. To disable authentication, use the **no** form of the command.

```
kerberos {local-realm kerberos-realm | realm {dns-domain | host} kerberos-realm | server
kerberos-realm {hostname | ip-address} [port-number]}
```



Note

Your Windows domain server must have a Reverse DNS Zone configured for this command to execute successfully.

Syntax Description

local-realm	Displays the default realm for WAAS. Configures a switch to authenticate users defined in the Kerberos database.
<i>kerberos-realm</i>	IP address or name (in UPPERCASE letters) of the Kerberos realm. Default value is a NULL string.
realm	Maps a host name or DNS domain name to a Kerberos realm.
<i>dns-domain</i>	DNS domain name to map to Kerberos realm. Note The name must begin with a leading dot (.).
<i>host</i>	Host IP address or name to map to Kerberos host realm.
server	Specifies the Key Distribution Center (KDC) to use in a given Kerberos realm and, optionally, the port number the KDC is monitoring.
<i>hostname</i>	Name of the host running the KDC.
<i>ip-address</i>	IP address of the host running the KDC.
<i>port-number</i>	(Optional) Number of the port on the KDC server.

Defaults

kerberos-realm: NULL string
port-number: 88

Command Modes

global configuration

Device Modes

application-accelerator
replication-accelerator
central-manager

Usage Guidelines

All Windows 2000 domains are also Kerberos realms. Because the Windows 2000 domain name is also a DNS domain name, the Kerberos realm name for the Windows 2000 domain name is always in uppercase letters. This capitalization follows the recommendation for using DNS names as realm names in the Kerberos Version 5 protocol document (RFC-1510) and affects only interoperability with other Kerberos-based environments.

The KDC server and all hosts with Kerberos authentication configured must interact within a 5-minute window or authentication will fail. All hosts, especially the KDC, should be running NTP. For information about configuring NTP, see the “(config) ntp” command.

The KDC server and Admin server must have the same IP address. The default port number for both servers is port 88.

The **kerberos** command modifies the krb5.conf file.

Examples

The following example shows how to configure the WAAS device to authenticate with a specified KDC in a specified Kerberos realm. The configuration is then verified.

```
WAE(config)# kerberos ?
  local-realm  Set local realm name
  realm        Add domain to realm mapping
  server       Add realm to host mapping
WAE(config)# kerberos local-realm WAE.ABC.COM
WAE(config)# kerberos realm wae.abc.com WAE.ABC.COM
WAE(config)# kerberos server wae.abc.com 10.10.192.50
WAE(config)# exit
WAE# show kerberos
Kerberos Configuration:
-----
Local Realm: WAE.ABC.COM
DNS suffix: wae.abc.com
Realm for DNS suffix: WAE.ABC.COM
Name of host running KDC for realm:
Master KDC: 10.10.192.50
Port: 88
```

Related Commands [show kerberos](#)

(config) kernel kdb

To enable access to the kernel debugger (kdb), use the **kernel kdb** global configuration command. Once enabled, kdb is automatically activated if kernel problems occur, or you can manually activate it from the local console for the WAAS device by pressing the required key sequence. To disable access to the kernel debugger, use the **no** form of the command.

kernel kdb

Syntax Description This command has no arguments or keywords.

Defaults The kernel debugger is disabled by default.

Command Modes global configuration

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines Once enabled, kdb is automatically activated when kernel problems occur. Once activated, all normal functioning of the WAAS device is suspended until kdb is manually deactivated. The kdb prompt looks like this:

```
[0]kdb>
```

To deactivate kdb, enter **go** at the kdb prompt. If kdb was automatically activated because of kernel problems, the system generates a core dump and restarts. 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.

kdb is disabled by default and you must enter the **kernel kdb** command in global configuration mode to enable it. If kdb has been previously enabled, you can enter the **no kernel kdb** global configuration command to disable it. When kdb is enabled, you can activate it manually from the local console by pressing **Ctrl-_** followed by **Ctrl-B**.

The rationale for disabling the kernel debugger is as follows: the WAAS device is often unattended at many sites, and it is desirable for the WAAS device to automatically reboot after generating a core dump instead of requiring user intervention. Disabling the kernel debugger allows automatic recovery.

Examples The following example shows to enable, and then disable, access to the kernel debugger:

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

(config) line

To specify terminal line settings, use the **line** global configuration command. To configure the WAAS device to not check for the carrier detect signal, use the **no** form of the command.

line console carrier-detect

Syntax Description	console	carrier-detect
	Configures the console terminal line settings.	Sets the device to check the carrier detect signal before writing to the console.

Defaults No default behavior or values

Command Modes global configuration

Device Modes application-accelerator
replication-accelerator
central-manager

Examples The following example sets the WAAS device to check for the carrier detect signal:
WAE(config)# **line console carrier-detect**

(config) logging

To configure system logging, use the **logging** global configuration command. To disable logging functions, use the **no** form of this command.

```
logging { console { enable | priority loglevel } | disk { enable | filename filename | priority loglevel | recycle size } | facility facility | host { hostname | ip-address } [port port_num | priority loglevel | rate-limit message_rate ] }
```

Syntax Description

console	Sets system logging to a console.
enable	Enables system logging to a console.
priority	Sets which priority level messages to send to syslog file.
<i>loglevel</i>	Use one of the following keywords: <ul style="list-style-type: none"> • alert—Immediate action needed. Priority 1. • critical—Immediate action needed. Priority 2. • debug—Debugging messages. Priority 7. • emergency—System is unusable. Priority 0. • error—Error conditions. Priority 3. • information—Informational messages. Priority 6. • notice—Normal but significant conditions. Priority 5. • warning—Warning conditions. Priority 4.
disk	Sets system logging to a disk file.
enable	Enables system logging to a disk file.
filename	Sets the name of the syslog file.
<i>filename</i>	Name of the syslog file.
recycle	Overwrites <i>syslog.txt</i> when it surpasses the recycle size.
<i>size</i>	Size of syslog file in bytes (1000000–50000000).
facility	Sets facility parameter for syslog messages.

<i>facility</i>	Use one of the following keywords: <ul style="list-style-type: none"> • auth—Authorization system • daemon—System daemons • kernel—Kernel • local0—Local use • local1—Local use • local2—Local use • local3—Local use • local4—Local use • local5—Local use • local6—Local use • local7—Local use • mail—Mail system • news—USENET news • syslog—Syslog itself • user—User process • uucp—UUCP system
host	Sets system logging to a remote host.
<i>hostname</i>	Hostname of the remote syslog host. Specify up to four remote syslog hosts. Note To specify more than one syslog host, use multiple command lines; specify one host per command.
<i>ip-address</i>	IP address of the remote syslog host. Specify up to four remote syslog hosts. Note To specify more than one syslog host, use multiple command lines; specify one host per command.
port	(Optional) Specifies the port to be used when logging to a host.
<i>port_num</i>	Port to be used when logging to a host. The default port is 514.
priority	(Optional) Sets the priority level for messages when logging messages to a host. The default priority is warning.
<i>loglevel</i>	Use one of the following keywords: <ul style="list-style-type: none"> • alert—Immediate action needed. Priority 1. • critical—Immediate action needed. Priority 2. • debug—Debugging messages. Priority 7. • emergency—System is unusable. Priority 0. • error—Error conditions. Priority 3. • information—Informational messages. Priority 6. • notice—Normal but significant conditions. Priority 5. • warning—Warning conditions. Priority 4.

rate-limit	(Optional) Sets the rate limit (in messages per second) for sending messages to a host.
<i>message_rate</i>	Rate limit (in messages per second) for sending messages to the host. (0–10000). Setting the rate limit to 0 disables rate limiting.

Defaults

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

Command Modes

global configuration

Device Modes

application-accelerator
 replication-accelerator
 central-manager

Usage Guidelines

Use the **logging** command to set specific parameters of the system log file. System logging is always enabled internally. By default, system logging is enabled on a WAAS device. The system log file is located on the SYSFS partition at /local1/syslog.txt. This file contains authentication entries, privilege levels, and administrative details.

WAAS supports filtering multiple syslog messages for a single failed section on SCSI disks and SATA disks.

To configure the WAAS device to send varying levels of event messages to an external syslog host, use the **logging host** option. Logging can be configured to send various levels of messages to the console using the **logging console priority** option.

The **no logging disk recycle size** command sets the file size to the default value. Whenever the current log file size surpasses the recycle size, the log file is rotated. The log file cycles through at most five rotations, and they are saved as [*log file name*].[1-5] under the same directory as the original log. The rotated log file is the one configured using the **logging disk filename** command.

Configuring System Logging to Remote Syslog Hosts

You can configure a WAAS device to send varying levels of messages to up to four remote syslog hosts. Use the **logging host hostname** global configuration command as follows:

```
WAE(config)# [no] logging host hostname [priority priority-code | port port | rate-limit limit]
```

where

- *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 is capable of receiving a different level of event messages.

**Note**

You can achieve syslog host redundancy by configuring multiple syslog hosts on the WAAS device 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 WAAS device 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, the specified remote syslog host drops the messages. There is no default rate limit, and by default all syslog messages are sent to all of the configured syslog hosts. If the rate limit is exceeded, a “message of the day” (motd) will be printed for any CLI EXEC shell login.

Examples

The following example shows how the WAAS device is configured to send messages that have a priority code of “error” (level 3) to the console:

```
WAE(config)# logging console priority error
```

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

```
WAE(config)# no logging console error
```

The following example shows how the WAAS device 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:

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

Related Commands

[clear](#)

[show logging](#)

(config) no

To undo a global configuration command or set its defaults, use the **no** form of a global configuration command.

no *command*

Syntax Description

aaa	Unconfigures AAA.
alarm	Unconfigures alarm parameters.
authentication	Unconfigures login authentication and authorization.
bypass	Unconfigures bypass.
cdp	Unconfigures CDP.
clock	Unconfigures the time-of-day clock.
disk	Unconfigures disk-related parameters.
exec-timeout	Unconfigures the exec timeout.
help	Unconfigures assistance for the command-line interface.
hostname	Unconfigures the system's network name.
inetd	Unconfigures FTP, rcp, and TFTP services.
interface	Not supported.
	Note Although the CLI contains the no interface option, the no command cannot be applied to an interface. The software displays the following error message: Removing of physical interface is not permitted.
ip	Unconfigures IP parameters.
ip access-list	Unconfigures IP access lists.
kerberos	Unconfigures kerberos security options.
kernel	Disables access to the kernel debugger.
line	Unconfigures terminal line settings.
logging	Unconfigures system logging (syslog).
ntp	Unconfigures NTP.
port-channel	Unconfigures port channel global options.
print-services	Unconfigures the parameters for the WAAS print services.
radius-server	Unconfigures RADIUS server parameters.
smb-conf	Unconfigures the Windows domain <i>smb.conf</i> file.
sshd	Unconfigures the parameters for the Secure Shell (SSH) service.
ssh-key-generate	Unconfigures the SSH host key.
tacacs	Unconfigures the TACACS+ parameters.
tcp	Unconfigures the global TCP parameters.
telnet enable	Disables the Telnet service.
username	Unconfigures username authentication.
wccp	Disables WCCP.
windows-domain	Unconfigures Windows domain server parameters.

Defaults No default behavior or values

Command Modes global configuration

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines Use the **no** command to disable functions or negate a command. If you need to negate a specific argument in a 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**.

Examples The following example shows how the Telnet service is disabled on the WAAS device:

```
WAE(config)# no telnet enable
```

(config) ntp

To configure the NTP server and to allow the system clock to be synchronized by a time server, use the **ntp** global configuration command. To disable this function, use the **no** form of this command.

```
ntp [authenticate | authentication-key authentication-key [md5 encryption-type] | server
  {ip-address | hostname} [ip-addresses | hostnames] | server-with-authentication {ip-address |
  hostname} key authentication-key]
```

Syntax Description	
authenticate	Authenticate the NTP server.
authentication-key	Sets the NTP authentication key.
<i>authentication-key</i>	The NTP authentication key value. Must be from 0 to 4294967295.
md5	Sets MD5 cryptographic hash function.
<i>encryption-type</i>	The MD5 encryption type must be set to 0.
server	Sets the NTP server IP address for the WAAS device.
<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 4).
<i>hostnames</i>	(Optional) Hostname of the time server providing the clock synchronization (maximum of 4).
server-with-authentication	Sets the authentication NTP server IP address for the WAAS device.
<i>ip-address</i>	NTP server IP address.
<i>hostname</i>	NTP server hostname.
key	Sets the NTP authentication key value.
<i>authentication-key</i>	The NTP authentication key value. Must be from 0 to 4294967295.

Defaults The default NTP version number is 3.

Command Modes global configuration

Device Modes application-accelerator
 replication-accelerator
 central-manager

Usage Guidelines Use this command to synchronize the clock on the WAAS device with the specified NTP server. The **ntp** command enables NTP servers for timekeeping purposes and is the only way to synchronize the system clock with a time server in WAAS software.

Examples

The following example specifies the NTP server IP address as the time source for a WAAS device. It also removes this configuration.

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

Related Commands

[clock](#)
[\(config\) clock](#)
[ntpdate](#)
[show clock](#)
[show ntp](#)

(config) policy-engine application classifier

To create or edit an existing application classifier on a WAE, use the **policy-engine application classifier** global configuration command. You can use this command to add or modify rules, also known as match conditions, to identify specific types of traffic. You can also use this command to list the classifier's match conditions.

To delete an application classifier or a condition, use the **no** form of this command.

```
policy-engine application classifier classifier-name [list |
  match {all | dst {host hostname | ip ip_address | port {eq port | range port1 port2}} |
  src {host hostname | ip ip_address | port {eq port | range port1 port2}}}]
```

Syntax Description		
	<i>classifier-name</i>	Classifier name (up to 30 characters). The name must start with a letter representing the application class.
	list	(Optional) Lists the conditions contained in the specified classifier.
	match	(Optional) Specifies the criteria for matching traffic.
	all	Matches any type of traffic.
	dst	Specifies the criteria for identifying the destination host.
	host <i>hostname</i>	Specifies the hostname of the system that is the source or destination of the traffic.
	ip <i>ip_address</i>	Specifies the IP address of the system that is the source or destination of the traffic.
	port	Specifies the criteria for identifying the port or ports used by the source or destination hosts.
	eq <i>port</i>	Specifies the source or destination port number.
	range <i>port1 port2</i>	Specifies a range of source or destination port numbers.
	src	Specifies the criteria for identifying the source host.

Command Modes global configuration

Device Modes application-accelerator

Usage Guidelines Deleting a classifier fails if there are policies using it. When creating a new application classifier or adding an existing application classifier, the WAAS CLI enters into an appropriate submode allowing you to specify one or more conditions. However, if the condition specified matches an already existing condition in the classifier's conditions list, no action is taken. A condition can be deleted by using the **no** form of this command. When creating a new classifier, you must add at least one condition.



Note

You cannot have more than 512 different application classifiers.

The WAAS software comes with over 150 default application policies that help your WAAS system classify and optimize some of the most common traffic on your network. Before you create a new application policy, we recommend that you review the default policies and modify them as appropriate. It is usually easier to modify an existing policy than to create a new one. For a list of the default applications and classifiers that WAAS will either optimize or pass through based on the policies that come bundled with the system, see the *Cisco Wide Area Application Services Configuration Guide*.

**Note**

We strongly recommend that you use the WAAS Central Manager GUI to centrally configure application policies for your WAEs. For more information, see the *Cisco Wide Area Application Services Configuration Guide*.

Related Commands

(config) policy-engine application map adaptor EPM
(config) policy-engine application map adaptor WAFS transport
(config) policy-engine application map basic delete
(config) policy-engine application map basic disable
(config) policy-engine application map basic insert
(config) policy-engine application map basic list
(config) policy-engine application map basic move
(config) policy-engine application map basic name
(config) policy-engine application map other optimize DRE
(config) policy-engine application map other optimize full
(config) policy-engine application map other pass-through
(config) policy-engine application name

(config) policy-engine application map adaptor EPM

To configure the application policy with advanced policy map lists of the EndPoint Mapper (EPM) service on a WAE, use the **policy-engine application map adaptor EPM** global configuration command. To disable the EPM service in the application policy configuration, use the **no** form of this command.

```

policy-engine application map adaptor EPM epm-map {

    delete line-number |

    disable line-number |

    insert { first | last | pos line-number } name app-name { All | classifier classifier-name }
    [disable] action { optimize { DRE { yes | no } compression { LZ | none } | full } |
    pass-through } |

    list [from line-number [to line-number] | to line-number [from line-number]] |

    move from line-number to line-number |

    name app-name { All | classifier classifier-name } [disable] action { optimize { DRE { yes | no }
    compression { LZ | none } | full } | pass-through } }

```

Syntax Description

<i>epm-map</i>	Messaging Application Programming Interface (MAPI) or Universal Unique ID (UUID).
delete	Deletes the application policy map specified by the line number.
<i>line-number</i>	Line number or position of an application policy map in the list.
disable	Disables the application policy map specified by the line number.
insert	Inserts or adds a new policy map at the specified position.
first	Inserts the new application policy map at the beginning of the list.
last	Inserts the new application policy map at the end of the list.
pos	Inserts the new application policy map at the specified line number.
name	Specifies the name of the application.
<i>app-name</i>	Name of the application.
All	Specifies all traffic.
classifier	Specifies the name of the application traffic classifier.
<i>classifier-name</i>	Name of the application traffic classifier.
disable	Disables optimization or pass-through.
action	Specifies whether to optimize the traffic or let it pass through.
optimize	Applies general optimization.
DRE	Enables or disables DRE optimization.
yes	Enables DRE optimization.
no	Disables DRE optimization.
compression	Applies Lempel-Ziv (LZ) compression or no compression.

LZ	Applies LZ compression.
none	Applies no compression.
full	Applies full generic optimization.
pass-through	Allows traffic to pass through without any optimization.
list	Lists the specified application policy maps.
from	(Optional) Specifies the line number of the first application policy map to list.
to	(Optional) Specifies the line number of the last application policy map to list.
move	Moves the specified application policy map from one line to another.

Command Modes global configuration

Device Modes application-accelerator

Usage Guidelines EndPoint Mapper (EPM) is a service that dynamically allocates server ports to certain applications. Unlike most applications that always use the same port, applications that rely on the EPM service can be assigned a different port at every request.



Note

We strongly recommend that you use the WAAS Central Manager GUI to centrally configure application policies for your WAEs. For more information, see the *Cisco Wide Area Application Services Configuration Guide*.

Related Commands

- (config) policy-engine application classifier
- (config) policy-engine application map adaptor WAFS transport
- (config) policy-engine application map basic delete
- (config) policy-engine application map basic disable
- (config) policy-engine application map basic insert
- (config) policy-engine application map basic list
- (config) policy-engine application map basic move
- (config) policy-engine application map basic name
- (config) policy-engine application map other optimize DRE
- (config) policy-engine application map other optimize full

(config) policy-engine application map adaptor WAFS transport

To configure application policies with the Wide Area File Services (WAFS) transport option, use the **policy-engine application map adaptor WAFS transport** global configuration command. To disable the WAFS transport policy map in the application policy configuration, use the **no** form of this command.

policy-engine application map adaptor WAFS transport {

delete *line-number* |

disable *line-number* |

insert {**first** | **last** | **pos** *line-number*} **name** *app-name* {**All** | **classifier** *classifier-name*}
[**disable**] **action** {**optimize** {**DRE** {**yes** | **no**} **compression** {**LZ** | **none**} | **full**} |
pass-through} |

list [**from** *line-number* [**to** *line-number*] | **to** *line-number* [**from** *line-number*]] |

move from *line-number* **to** *line-number* |

name *app-name* {**All** | **classifier** *classifier-name*} [**disable**] **action** {**optimize** {**DRE** {**yes** | **no**}
compression {**LZ** | **none**} | **full**} | **pass-through**}}

Syntax Description

delete	Deletes the application policy map specified by the line number.
<i>line-number</i>	Line number or position of an application policy map in the list.
disable	Disables the application policy map specified by the line number.
insert	Inserts or adds a new policy map at the specified position.
first	Inserts the new application policy map at the beginning of the list.
last	Inserts the new application policy map at the end of the list.
pos	Inserts the new application policy map at the specified line number.
name	Specifies the name of the application.
<i>app-name</i>	Name of the application.
All	Specifies all traffic.
classifier	Specifies the name of the application traffic classifier.
<i>classifier-name</i>	Name of the application traffic classifier.
disable	Disables optimization or pass-through.
action	Specifies whether to optimize the traffic or let it pass through.
optimize	Applies general optimization.
DRE	Enables or disables DRE optimization.
yes	Enables DRE optimization.
no	Disables DRE optimization.
compression	Applies Lempel-Ziv (LZ) compression or no compression.
LZ	Applies LZ compression.
none	Applies no compression.
full	Applies full generic optimization.

pass-through	Allows traffic to pass through without any optimization.
list	Lists the specified application policy maps.
from	(Optional) Specifies the line number of the first application policy map to list.
to	(Optional) Specifies the line number of the last application policy map to list.
move	Moves the specified application policy map from one line to another.

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

By default, when you enable WAFS, all CIFS traffic going between an Edge WAE and a core cluster is accelerated. Use this command to specify another action (such as **optimize**) for CIFS traffic traveling between edge and core devices.

**Note**

We strongly recommend that you use the WAAS Central Manager GUI to centrally configure application policies for your WAEs. For more information, see the *Cisco Wide Area Application Services Configuration Guide*.

Related Commands

(config) policy-engine application classifier
 (config) policy-engine application map adaptor EPM
 (config) policy-engine application map basic delete
 (config) policy-engine application map basic disable
 (config) policy-engine application map basic insert
 (config) policy-engine application map basic list
 (config) policy-engine application map basic move
 (config) policy-engine application map basic name
 (config) policy-engine application map other optimize DRE
 (config) policy-engine application map other optimize full
 (config) policy-engine application map other pass-through
 (config) policy-engine application name

(config) policy-engine application map basic delete

To delete a specific basic (static) application policy map from the list of application policy maps on a WAE, use the **policy-engine application map basic delete** global configuration command.

```
policy-engine application map basic delete pos
```

Syntax Description	<i>pos</i> Line number indicating the exact position of the policy map in the list.
---------------------------	-------------------------------------------------------------------------------------

Command Modes	global configuration
----------------------	----------------------

Device Modes	application-accelerator
---------------------	-------------------------

Usage Guidelines	A policy map consists of a set of application policies and the order in which they are checked. This command is ignored if the line number specified does not represent a current policy map.
-------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



Note


We strongly recommend that you use the WAAS Central Manager GUI to centrally configure application policies for your WAEs. For more information, see the *Cisco Wide Area Application Services Configuration Guide*.

Related Commands	<p>(config) policy-engine application classifier</p> <p>(config) policy-engine application map adaptor EPM</p> <p>(config) policy-engine application map adaptor WAFS transport</p> <p>(config) policy-engine application map basic disable</p> <p>(config) policy-engine application map basic insert</p> <p>(config) policy-engine application map basic list</p> <p>(config) policy-engine application map basic move</p> <p>(config) policy-engine application map basic name</p> <p>(config) policy-engine application map other optimize DRE</p> <p>(config) policy-engine application map other optimize full</p> <p>(config) policy-engine application map other pass-through</p> <p>(config) policy-engine application name</p>
-------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

(config) policy-engine application map basic disable

To disable a specific basic (static) application policy map from the list of application policy maps on a WAE, use the **policy-engine application map basic disable** global configuration command.

policy-engine application map basic disable *pos*

Syntax Description	<i>pos</i> Line number indicating the exact position of the policy map in the list.
Command Modes	global configuration
Device Modes	application-accelerator
Usage Guidelines	This command is ignored if the line number specified does not represent a current policy map.
 Note	We strongly recommend that you use the WAAS Central Manager GUI to centrally configure application policies for your WAEs. For more information, see the <i>Cisco Wide Area Application Services Configuration Guide</i> .
Related Commands	<p>(config) policy-engine application classifier</p> <p>(config) policy-engine application map adaptor EPM</p> <p>(config) policy-engine application map adaptor WAFS transport</p> <p>(config) policy-engine application map basic delete</p>

(config) policy-engine application map basic insert

To insert a new basic (static) application policy map to the list of application policy maps on a WAE, use the **policy-engine application map basic insert** global configuration command.

```
policy-engine application map basic insert {first | last | pos pos} name app-name
```

Syntax Description		
	first	Inserts the policy map at the beginning of the list.
	last	Inserts the policy map at the end of the list.
	pos	Inserts the policy map at a specific position in the list.
	<i>pos</i>	Line number at which to insert the policy map.
	name	Specifies an already defined application name.
	<i>app-name</i>	Name of the application.

Command Modes global configuration

Device Modes application-accelerator

Usage Guidelines Use the **policy-engine application map basic insert** global configuration command to insert a new basic (static) application policy map to the list of application policy maps on a WAE.



Note

We strongly recommend that you use the WAAS Central Manager GUI to centrally configure application policies for your WAEs. For more information, see the *Cisco Wide Area Application Services Configuration Guide*.

Related Commands

- [\(config\) policy-engine application classifier](#)
- [\(config\) policy-engine application map adaptor EPM](#)
- [\(config\) policy-engine application map adaptor WAFS transport](#)
- [\(config\) policy-engine application map basic delete](#)
- [\(config\) policy-engine application map basic disable](#)
- [\(config\) policy-engine application map basic list](#)
- [\(config\) policy-engine application map basic move](#)
- [\(config\) policy-engine application map basic name](#)
- [\(config\) policy-engine application map other optimize DRE](#)
- [\(config\) policy-engine application map other optimize full](#)
- [\(config\) policy-engine application map other pass-through](#)
- [\(config\) policy-engine application name](#)

(config) policy-engine application map basic list

To display a list of basic (static) application policy maps on a WAE, use the **policy-engine application map basic list** global configuration command.

policy-engine application map basic list [**from** *pos* [**to** *pos*] | **to** *pos*]

Syntax Description	
from	(Optional) Starts the listing from the specified position.
to	(Optional) Stops the listing at the specified position.
<i>pos</i>	Line number indicating the exact position of a policy map in the list.

Command Modes global configuration

Device Modes application-accelerator

Usage Guidelines Use the **policy-engine application map basic list** global configuration command to display a list of basic application policy maps on a WAE.



Note

We strongly recommend that you use the WAAS Central Manager GUI to centrally configure application policies for your WAEs. For more information, see the *Cisco Wide Area Application Services Configuration Guide*.

Related Commands

- (config) [policy-engine application classifier](#)
- (config) [policy-engine application map adaptor EPM](#)
- (config) [policy-engine application map adaptor WAFS transport](#)
- (config) [policy-engine application map basic delete](#)
- (config) [policy-engine application map basic disable](#)
- (config) [policy-engine application map basic insert](#)
- (config) [policy-engine application map basic move](#)
- (config) [policy-engine application map basic name](#)
- (config) [policy-engine application map other optimize DRE](#)
- (config) [policy-engine application map other optimize full](#)
- (config) [policy-engine application map other pass-through](#)
- (config) [policy-engine application name](#)

(config) policy-engine application map basic move

To move the application policy with the basic policy map list based on only L3 or L4 parameters on a WAE, use the **policy-engine application map basic move** global configuration command.

policy-engine application map basic move from *pos* to *pos*

Syntax Description	from	Moves the policy at the specified line number.
	to	Moves the policy to the specified line number.
	<i>pos</i>	Line number indicating the exact position of a policy map in the list.

Command Modes global configuration

Device Modes application-accelerator

Usage Guidelines Use the **policy-engine application map basic move** global configuration command to move the application policy with the basic policy map list based on only Layer 3 or Layer 4 parameters on a WAE.



Note

We strongly recommend that you use the WAAS Central Manager GUI to centrally configure application policies for your WAEs. For more information, see the *Cisco Wide Area Application Services Configuration Guide*.

Examples The following example shows how to move a policy map from line 10 to line 16:

```
WAE(config)# policy-engine application map basic move from 10 to 16
```

Related Commands

- (config) [policy-engine application classifier](#)
- (config) [policy-engine application map adaptor EPM](#)
- (config) [policy-engine application map adaptor WAFS transport](#)
- (config) [policy-engine application map basic delete](#)
- (config) [policy-engine application map basic disable](#)
- (config) [policy-engine application map basic insert](#)
- (config) [policy-engine application map basic list](#)
- (config) [policy-engine application map basic name](#)
- (config) [policy-engine application map other optimize DRE](#)
- (config) [policy-engine application map other optimize full](#)
- (config) [policy-engine application map other pass-through](#)

(config) policy-engine application name

(config) policy-engine application map basic name

To configure the application policy with the basic policy map name, use the **policy-engine application map basic name** global configuration command.

```
policy-engine application map basic name app-name classifier classifier-name { [disable] action
  { optimize { DRE { yes | no } compression { LZ | none } | full } | pass-through } [accelerate { cifs
  | MS-port-mapper } ] }
```

Syntax Description

<i>app-name</i>	Application name.
classifier	Specifies the name of the application traffic classifier.
<i>classifier-name</i>	Name of the classifier.
disable	Disables optimization or pass-through.
action	Specifies whether to optimize the traffic or allow it to pass through.
optimize	Applies general optimization.
DRE	Enables or disables DRE optimization.
yes	Enables DRE optimization.
no	Disables DRE optimization.
compression	Applies compression.
LZ	Applies Lempel-Ziv (LZ) compression.
none	Does not apply any compression.
full	Applies full generic optimization.
pass-through	Allows traffic pass through with no optimization.
accelerate	Accelerates the traffic using a special adapter.
cifs	Accelerates the traffic using the CIFS accelerator.
MS-port-mapper	Accelerates the traffic using the Microsoft EndPoint Port Mapper (EPM).

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

Use the **policy-engine application map basic name** global configuration command to configure the application policy with the basic policy map name.

To view WAFS dynamic accept or deny list entries, use the **show policy-engine application dynamic** command.



Note

We strongly recommend that you use the WAAS Central Manager GUI to centrally configure application policies for your WAEs. For more information, see the *Cisco Wide Area Application Services Configuration Guide*.

Related Commands

(config) policy-engine application classifier
(config) policy-engine application map adaptor EPM
(config) policy-engine application map adaptor WAFS transport
(config) policy-engine application map basic delete
(config) policy-engine application map basic disable
(config) policy-engine application map basic insert
(config) policy-engine application map basic list
(config) policy-engine application map basic move
(config) policy-engine application map other optimize DRE
(config) policy-engine application map other optimize full
(config) policy-engine application map other pass-through
(config) policy-engine application name
show policy-engine application dynamic

(config) policy-engine application map other optimize DRE

To configure the optimize DRE action on non-classified traffic on a WAE, use the **policy-engine application map other optimize DRE** global configuration command.

```
policy-engine application map other optimize DRE {yes | no} compression {LZ | none}
```

Syntax Description

yes	Applies the optimize DRE action on non-classified traffic.
no	Does not apply the optimize DRE action on non-classified traffic.
compression	Applies the specified compression.
LZ	Applies the Lempel-Ziv (LZ) compression.
none	Applies no compression.

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

Use the **policy-engine application map other optimize DRE** global configuration command to configure the optimize DRE action on nonclassified traffic on a WAE.



Note

We strongly recommend that you use the WAAS Central Manager GUI to centrally configure application policies for your WAEs. For more information, see the *Cisco Wide Area Application Services Configuration Guide*.

Examples

The following example shows how to configure the optimize DRE action on nonclassified traffic with no compression:

```
WAE(config)# policy-engine application map other optimize DRE yes compression none
```

Related Commands

(config) [policy-engine application classifier](#)
 (config) [policy-engine application map adaptor EPM](#)
 (config) [policy-engine application map adaptor WAFS transport](#)
 (config) [policy-engine application map basic delete](#)
 (config) [policy-engine application map basic disable](#)
 (config) [policy-engine application map basic insert](#)
 (config) [policy-engine application map basic list](#)
 (config) [policy-engine application map basic move](#)
 (config) [policy-engine application map basic name](#)

(config) policy-engine application map other optimize full

(config) policy-engine application map other pass-through

(config) policy-engine application name

(config) policy-engine application map other optimize full

To configure the application policy on non-classified traffic with the optimize full action, use the **policy-engine application map other optimize full** global configuration command.

policy-engine application map other optimize full

Syntax Description This command has no keywords or arguments.

Command Modes global configuration

Device Modes application-accelerator

Usage Guidelines Use the **policy-engine application map other optimize full** global configuration command to configure the application policy on non-classified traffic with the optimize full action.



Note

We strongly recommend that you use the WAAS Central Manager GUI to centrally configure application policies for your WAEs. For more information, see the *Cisco Wide Area Application Services Configuration Guide*.

Related Commands

- [\(config\) policy-engine application classifier](#)
- [\(config\) policy-engine application map adaptor EPM](#)
- [\(config\) policy-engine application map adaptor WAFS transport](#)
- [\(config\) policy-engine application map basic delete](#)
- [\(config\) policy-engine application map other optimize DRE](#)
- [\(config\) policy-engine application map other pass-through](#)
- [\(config\) policy-engine application name](#)

(config) policy-engine application map other pass-through

To configure the application policy on nonclassified traffic with the pass-through action on a WAE, use the **policy-engine application map other pass-through** global configuration command.

policy-engine application map other pass-through

Command Modes global configuration

Device Modes application-accelerator

Usage Guidelines Use the **policy-engine application map other pass-through** global configuration command to configure the application policy on nonclassified traffic with the pass-through action on a WAE.



Note

We strongly recommend that you use the WAAS Central Manager GUI to centrally configure application policies for your WAEs. For more information, see the *Cisco Wide Area Application Services Configuration Guide*.

Related Commands

- [\(config\) policy-engine application map basic delete](#)
- [\(config\) policy-engine application map basic disable](#)
- [\(config\) policy-engine application map basic insert](#)
- [\(config\) policy-engine application map basic list](#)
- [\(config\) policy-engine application map basic move](#)
- [\(config\) policy-engine application map basic name](#)
- [\(config\) policy-engine application map basic name](#)
- [\(config\) policy-engine application map other optimize full](#)

(config) policy-engine application name

To create a new application definition that specifies general information about an application on a WAE, use the **policy-engine application name** global configuration command. To delete the application definition, use the **no** form of this command.

policy-engine application name *app-name*

Syntax Description	<i>app-name</i>	Application name (up to 30 characters). The name cannot contain spaces or special characters.
---------------------------	-----------------	-----------------------------------------------------------------------------------------------

Command Modes	global configuration
----------------------	----------------------

Device Modes	application-accelerator
---------------------	-------------------------

Usage Guidelines	Use this command to create a new application name that can be used later to gather statistics about an application. Deleting an application name fails if there are policies using this name. Successful deletion clears all statistics that were once associated with this application.
-------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



Note

There is a limitation of 256 different application names.



Note

We strongly recommend that you use the WAAS Central Manager GUI to centrally configure application policies for your WAEs. For more information, see the *Cisco Wide Area Application Services Configuration Guide*.

Examples	The following example shows how to create an application definition for the Payroll application:
-----------------	--------------------------------------------------------------------------------------------------

```
WAE(config)# policy-engine application name Payroll
```

Related Commands	<p>(config) policy-engine application classifier</p> <p>(config) policy-engine application map adaptor EPM</p> <p>(config) policy-engine application map adaptor WAFS transport</p> <p>(config) policy-engine application map basic delete</p> <p>(config) policy-engine application map basic disable</p> <p>(config) policy-engine application map basic insert</p> <p>(config) policy-engine application map basic list</p> <p>(config) policy-engine application map basic move</p> <p>(config) policy-engine application map basic name</p>
-------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

(config) policy-engine application map basic name

(config) policy-engine application map other optimize DRE

(config) policy-engine application map other optimize full

(config) policy-engine application map other pass-through

(config) policy-engine config

To remove application policy configurations or replace application policy configurations with factory defaults on a WAE, use the **policy-engine config** global configuration command.

policy-engine config {remove-all | restore-predefined}

Syntax Description	remove-all	Restores the application policy configurations all together and resets other changed configurations.
	restore-predefined	Replaces application policy configurations (including the application names, classifiers, and policy maps) with factory defaults.

Command Modes global configuration

Device Modes application-accelerator

Usage Guidelines This action includes but is not limited to the following:

- Remove all application names except “other.”
- Remove all classifiers.
- Remove all policy maps.
- Reset the default action to pass-through.



Note

We strongly recommend that you use the WAAS Central Manager GUI to centrally configure application policies for your WAEs. For more information, see the *Cisco Wide Area Application Services Configuration Guide*.

Related Commands [show policy-engine status](#)

(config) port-channel

To configure the port channel load-balancing options on a WAAS device, use the **port-channel** global configuration command. Use the **no** form of this command to set load balancing on the port channel to its default method.

port-channel load-balance {dst-ip | dst-mac | round-robin}

Syntax	Description
load-balance	Configures the load-balancing method.
dst-ip	Specifies the load-balancing method using destination IP addresses.
dst-mac	Specifies the load-balancing method using destination MAC addresses.
round-robin	Specifies the load-balancing method using round-robin sequential, cyclical resource allocation.

Defaults Round-robin is the default load-balancing method.

Command Modes global configuration

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines The **port-channel load-balance** command configures one of three load-balancing algorithms and provides flexibility in choosing interfaces when an Ethernet frame is sent. The **round-robin** option allows evenly balanced usage of identical network interfaces in a channel group. Because this command takes effect globally, if two channel groups are configured, they must use the same load-balancing option.

Examples The following example configures destination IP load balancing on a port channel and then disables it:

```
WAE(config)# port-channel load-balance dst-ip
WAE(config)# no port-channel load-balance
```

(config) primary-interface

To configure the primary interface for a WAAS device, use the **primary-interface** command in global configuration mode. To remove the configured primary interface, use the **no** form of the command.

```
primary-interface { GigabitEthernet 1-2/port | PortChannel 1-2 | Standby group_num }
```

Syntax	Description
GigabitEthernet	Selects a Gigabit Ethernet interface as the primary interface of the WAAS device.
<i>1-2/</i>	Gigabit Ethernet slot number 1 or 2.
<i>port</i>	Port number of the Gigabit Ethernet interface.
PortChannel	Selects a port channel interface as the primary interface of the WAAS device.
<i>1-2</i>	Port Channel number 1 or 2.
Standby	Selects a standby group as the primary interface of the WAAS device.
<i>group_num</i>	Standby group number 1–4.

Defaults

The default primary interface is the Gigabit Ethernet 1/0 interface. If this is not configured, then the first operational interface on which a link beat is detected becomes the default primary interface. Interfaces with lower-number IDs are polled first (for example, Gigabit Ethernet 1/0 is checked before 2/0). The Gigabit Ethernet interfaces are polled before the Port Channel interfaces.

Command Modes

global configuration

Device Modes

application-accelerator
 replication-accelerator
 central-manager

Usage Guidelines

The **primary-interface** global configuration command permits the administrator to specify the primary interface for the WAAS device.

The primary interface can be changed without disabling the WAAS device. To change the primary interface, reenter 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. If you want to reenable the WAAS device after using the **restore factory-default preserve basic-config** command, make sure to reconfigure the primary interface after the factory defaults are restored.

Setting the primary interface to be a Standby group does not imply that Standby functionality is available. You must configure relevant Standby interfaces using the **interface standby** global configuration command.

Examples

The following example shows how to specify the Gigabit Ethernet slot 1 port 0 as the primary interface on a WAAS device:

```
WAE(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 a WAAS device:

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

Related Commands

[\(config\) interface](#)

(config) print-services

To enable print services and designate a group name for administrators allowed configuration access on a WAAS device, use the **print-services** global configuration command. To disable print services on a WAAS device or to clear the administrative group, use the **no** form of this command.

```
print-services {enable | admin-group admin-group-name | guest-print enable}
```

Syntax Description

enable	Enables print services on the WAAS device.
admin-group	Configures a group of administrators with print services configuration privileges.
<i>admin-group-name</i>	Name of the administrative group, up to 127 characters. No spaces are allowed.
guest-print enable	Enables the guest print service. Guest printing allows any user to print to the WAAS print server.
Note	This option is available only in the application-accelerator device mode.

Defaults

By default, print services are disabled and no administrative group is defined (*admin-group-name* is null).

Command Modes

global configuration

Device Modes

application-accelerator
 replication-accelerator
 central-manager

Usage Guidelines

WAAS print services are typically enabled on WAEs residing in branch offices. The WAE acts as a print server and handles requests from multiple clients for access to multiple printers. The WAAS print services feature enables administrators to perform the following print-related tasks:

- Add, modify, and delete printers from the printer list
- Add, modify, and delete a group of printers (Printer Cluster)
- View and control print jobs
- Monitor the status of individual printers
- Perform diagnostics and troubleshooting
- Install client printer driver from the print server
- Download log files using FTP
- Enforce printing quotas (1 GB total for spooling)
- Allow any user to print to the WAAS print server

From the WAAS CLI, you can start and stop WAAS print services, configure a print services administrative group, and debug the print spooler. WAAS print services provide an alternative to Windows print services.

Starting and Stopping Print Services

When the **print-services enable** command is executed, the following sequence of events occurs:

- The node manager starts the CUPS process (cupsd), checking every second for an updated timestamp in the *printcap* file.
CUPS must start within 30 seconds or print services are not enabled, and a “CUPS fails to start” message is logged by the node manager.
- The node manager starts the Samba process (smbd).
If Samba could not be started, a “Samba fails to start” message is logged by the node manager. CUPS is not stopped.
- Success messages are logged by the node manager.
- The DataServer value (cfg/print-services/enable) is set to one.

Stopping print services is accomplished using the **no print-services enable** command. Entering this command causes the following sequence of events:

- The node manager stops the Samba process (smbd).
- The node manager stops the CUPS process (cupsd).
- The corresponding DataServer value is set to zero.

Configuring the Print Services Administrative Group

You can define a set of administrators to have control over WAAS print services on a particular Edge WAE using the **print-services admin-group** command. When this command is entered, the following events occur:

- The *smb.conf* file is updated with the specified administrative group.
If the update fails, and the print services administrative group can be returned to its original value, the error message “Failed to configure print-services admin group” is displayed. If the update fails, and the print services administrative group cannot be returned to its original value, two error messages, “Failed to configure print-services admin group.” and “Failed to revert back the print-services admin group changes.” are displayed.
- The *cupsd.conf* file is updated with the specified administrative group.
If the update fails, the old setting is restored, the changes to the *smb.conf* file are reverted, and the error message: “Failed to configure print-services admin group” is displayed. If the update fails and the old setting cannot be restored, two error messages, “Failed to configure print-services admin group.” and “Failed to revert back the print-services admin group changes.” are displayed.
- The DataServer value (/cfg/print-services/administrators) is updated with the specified administrative group.
If setting the DataServer value fails, both configurations of *smb.conf* and *cupsd.conf* are reverted, and an error message is displayed.

You can delete a print services administrative group using the **no print-services admin-group** command. When this command is executed, the following events occur:

- The *smb.conf* setting is cleared.
If the clear fails, the old setting is restored and the error message “Failed to configure print-services admin group” is displayed. If the clear fails and the old setting cannot be restored, two error messages, “Failed to configure print-services admin group.” and “Failed to revert back the print-services admin group changes.” are displayed.
- The *cupsd.conf* file is modified to clear the admin group setting.
If the clear fails, the old setting is restored, and changes in the *smb.conf* are reverted, the error message “Failed to configure print-services admin group” is displayed. If the clear fails and the old setting cannot be restored, two error messages, “Failed to configure print-services admin group.” and “Failed to revert back the print-services admin group changes.” are displayed.
- The corresponding DataServer value is cleared.
If clearing the DataServer value fails, both configurations of *smb.conf* and *cupsd.conf* are reverted, and an error message is displayed.

The Samba and CUPS processes must be manually restarted for this change to take effect.

Examples

The following example enables print services on a WAAS device:

```
WAE(config)# print-services enable
```

The following example adds a print services administrative group called *printAdmins*:

```
WAE(config)# print-services admin-group printAdmins  
The new print-services administrator group is configured successfully. Please restart  
print services for the change to take effect.  
WAE(config)# no print-services enable  
WAE(config)# print-services enable
```

The following example removes the print services administrative group from the WAAS device:

```
WAE(config)# no print-services admin-group printAdmins  
The print-services administrator group is removed successfully. Please restart print  
services for the change to take effect.  
WAE(config)# no print-services enable  
WAE(config)# print-services enable
```

Related Commands

[debug](#)
[show print-services](#)
[show running-config](#)
[show startup-config](#)

(config) radius-server

To configure a set of RADIUS authentication server settings on the WAAS device, use the **radius-server** command in global configuration mode. To disable RADIUS authentication server settings, use the **no** form of this command.

```
radius-server {host hostname | hostipaddr [primary] | key keyword | retransmit retries | timeout
seconds}
```

Syntax Description

host	Specifies a RADIUS server. You can specify up to five servers.
<i>hostname</i>	Hostname of the RADIUS server.
<i>hostipaddr</i>	IP address of the RADIUS server.
primary	(Optional) Sets the server as the primary server.
key	Specifies the encryption key shared with the RADIUS servers.
<i>keyword</i>	Text of the shared key (15 characters maximum).
retransmit	Specifies the number of transmission attempts to an active server.
<i>retries</i>	Number of transmission attempts for a transaction (1–3). The default is 2.
timeout	Specifies the time to wait for a RADIUS server to reply. The range is 1 to 20 seconds.
<i>seconds</i>	Wait time in seconds (1–20). The default is 5 seconds.

Defaults

```
retransmit retries: 2
timeout seconds: 5
```

Command Modes

```
global configuration
```

Device Modes

```
application-accelerator
replication-accelerator
central-manager
```

Usage Guidelines

RADIUS is a client/server authentication and authorization access protocol used by a NAS to authenticate users attempting to connect to a network device. The NAS functions as a client, passing user information to one or more RADIUS servers. The NAS permits or denies network access to a user based on the response it receives from one or more RADIUS servers. RADIUS uses UDP for transport between the RADIUS client and server.

You can configure a RADIUS key on the client and server. If you configure a key on the client, it must be the same as the one configured on the RADIUS servers. The RADIUS clients and servers use the key to encrypt all RADIUS packets transmitted. If you do not configure a RADIUS key, packets are not encrypted. The key itself is never transmitted over the network.

**Note**

For more information about how the RADIUS protocol operates, refer to RFC 2138, *Remote Authentication Dial In User Service (RADIUS)*.

RADIUS authentication usually occurs when an administrator first logs in to the WAAS device to configure the WAE for monitoring, configuration, or troubleshooting purposes.

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. (See the “(config) authentication” command.)

Examples

The following example specifies a RADIUS server, specifies the RADIUS key, and accepts retransmit defaults. Configuration can be verified with the **show radius-server** command.

```
WAE(config)# radius-server host 172.16.90.121
WAE(config)# radius-server key myradiuskey
WAE# show radius-server
Radius Configuration:
-----
Radius Authentication is on
  Timeout      = 5
  Retransmit   = 3
  Key          = ****
  Servers
-----
```

Related Commands [show radius-server](#)

(config) smb-conf

To manually configure the parameters for a WAAS device's Samba configuration file, *smb.conf*, use the **smb-conf** global configuration command. To return a parameter to its default value, use the **no** form of this command.

smb-conf section { global | print\$ | printers } name attr-name value attr-value [service print]

Syntax Description		
global		Specifies one of the global print parameters.
print\$		Specifies one of the print\$ parameters.
printers		Specifies one of the printers parameters.
name		Specifies the name of the parameter in the specified section that you want to manually configure.
<i>attr-name</i>		Parameter name, up to 80 characters.
value		Specifies the value of the parameter.
<i>attr-value</i>		Parameter value, up to 255 characters.
service print		(Optional) Updates the Samba configuration file for print services. Without this option, the smb-conf command updates the Samba configuration file that is used for windows authentication.

See [Table 3-101](#) for a description of the global, print\$, and printers parameters, including names and default values.

Defaults No default behavior or values

Command Modes global configuration

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines The *smb.conf* file contains a variety of print-related parameters. The *global* parameters apply to the server as a whole. Service level parameters that define default settings for all other sections and shares are included in this set of parameters. This avoids the need to set the same value repeatedly. You can override these globally set share settings and specify other values for each individual section or share. The *print\$* parameters apply to the printers. The *printers* parameters apply to the shares. They make it possible to share all printers with minimal configuration. These parameters apply as default to all printers.

[Table 3-101](#) describes the print-related parameters.

Table 3-101 Print-Related Parameters

Parameter Name	Default Value	Parameter Description
global parameters		
idmap uid	70000-200000	Range of user IDs allocated for mapping UNIX users to NT user SIDs.
idmap gid	70000-200000	Range of group IDs allocated for mapping UNIX groups to NT group SIDs.
winbind enum users	no	Do not enumerate domain users using MSRPC.
winbind enum groups	no	Do not enumerate domain groups using MSRPC.
winbind cache time	10	Time that domain user or group information remains in the cache before expiring.
winbind use default domain	yes	Use default domain for users and groups.
printcap name	cups	Use CUPS to determine available printer names.
load printers	yes	Automatically create all available printer shares.
printing	cups	Use CUPS-compatible print commands.
cups options	raw	Sets the format of the print output to raw.
force printername	yes	Enforce the same printer name specified in the CUPS GUI to be used as the printer name in Samba.
lpq cache time	0	Controls the cache time for the results of the lpq command.
log file	/local/local1/errorlog/samba.log	Location where print-related errors are logged.
max log size	50	Maximum number of errors the log file can contain. After 50 errors, for each new error logged, the oldest error is removed.
socket options	TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192	Set controls on the network layer of the operating system to allow the connection with the client to be tuned. This option is typically used to tune your Samba server for optimal performance for your local network.
smb ports	50139	Available ports on the Samba server.
local master	no	Sets <i>nmbd</i> to be a local master browser on a subnet.
domain master	no	Sets <i>nmbd</i> to be a domain master browser for its given workgroup.
preferred master	no	Sets <i>nmbd</i> to be a preferred master browser for its workgroup.
dns proxy	no	DNS proxy is not enabled.
template homedir	/local/local1/	Home directory on File Engine or WAE.
template shell	/admin-shell	Directory of the administrative shell.
comment	Comment:	Optional description of print server (or share) that is visible when a client queries the server. Can also be set by the windows-domain comment command.
netbios name	MYFILEENGINE	Name of the Samba server hosting print services. Can also be set by the windows-domain netbios-name command.

Table 3-101 Print-Related Parameters (continued)

Parameter Name	Default Value	Parameter Description
realm	CISCO	Active Directory domain name. Always uppercase. Can also be set by the windows-domain realm command.
wins server	10.10.10.1	IP address of the Windows domain server used to authenticate user access to print services. Can also be set by the windows-domain wins-server command.
password server	10.10.10.10	Optional IP address of the password server used for authentication of users. Can also be set by the windows-domain password-server command.
security	domain	Use Windows domain server for authentication. Can also be set by the windows-domain security command.
client schannel	no	Secure channel indicator used for Windows domain server authentication.
ldap ssl	on	Defines whether or not Samba should use SSL when connecting to the LDAP server. Default is to always use SSL when contacting the LDAP server. If set to "off," SSL is never used when querying the directory server. If set to "start_tls," LDAPv3 StartTLS extended operation (RFC2830) is used for communicating with the directory server.
print\$ Parameters		
path	/state/samba/printers	Location of printer list.
guest ok	yes	A password is not required to connect to the printer.
browseable	yes	Allows the printer to be visible in the list of printers.
read only	yes	Prevents users from creating or modifying the printer list.
write list	root	Allows the printer administrator (root user) to modify the printer list.
printers Parameters		
path	/local/local1/spool/samba	Location where incoming files are spooled for printing.
browseable	no	Always set to no if printable = yes. It makes the printer share invisible in the list of available shares.
guest ok	yes	A password is not required to connect to the printer's service.
writable	no	Prevents users from creating or modifying files in the print service directory.
printable	yes	Allows connected clients to open, write to and submit spool files into the directory specified with the path parameter for printing. Used by Samba to differentiate printer shares from file shares. If this is set to no, printing is not allowed.
printer admin	root	Lets the print administrator (root user) add drivers and set printer properties.

Examples

The following example shows how to change the maximum size of the Samba error log file from the default of 50 errors to 75 errors:

```
WAE# smb-conf global max log size 75
```

The following example shows how to change the realm from the default of CISCO to MYCOMPANYNAME:

```
WAE# smb-conf global realm MYCOMPANYNAME
```

The following example shows how to enable and then disable LDAP server signing:

```
WAE# smb-conf global name "ldap ssl" value "start_tls"
```

Related Commands

[show smb-conf](#)

[windows-domain](#)

[\(config\) windows-domain](#)

(config) snmp-server access-list

To configure a standard access control list on a WAAS device to allow access through an SNMP agent, use the **snmp-server access-list** global configuration command. To remove a standard access control list, use the **no** form of this command.

```
snmp-server access-list {num | name}
```

Syntax Description

<i>num</i>	Standard access list number (1–99).
<i>name</i>	Standard access list name, up to a maximum of 30 characters.

Defaults

No default behavior or values

Command Modes

global configuration

Device Modes

application-accelerator
 replication-accelerator
 central-manager

Usage Guidelines

The **snmp-server access-list** *number* global configuration command configures an access control list to allow access to an SNMP agent. The *number* variable is a number in the range 1 to 99, indicating a standard access control list. SNMP checks against the specified access control list before accepting or dropping incoming packets.

Examples

The following example allows the SNMP agent to check against access control list *12* before accepting or dropping packets:

```
WAE(config)# snmp-server access-list 12
```



Note

You must first create access list 12 using the **ip access-list standard** global configuration command.

Related Commands

(config) [ip access-list](#)
[show running-config](#)

(config) snmp-server community

To enable the SNMP agent on a WAAS device and to set up the community access string to permit access to the SNMP agent, use the **snmp-server community** global configuration command. To disable the SNMP agent and remove the previously configured community string, use the **no** form of this command.

```
snmp-server community string [group groupname | rw]
```

Syntax Description

<i>string</i>	Community string that acts like a password and permits access to the SNMP agent. Supports up to a maximum of 64 characters.
group	(Optional) Specifies the group to which the community string belongs.
<i>groupname</i>	Name of the group. Supports up to a maximum of 64 characters.
rw	(Optional) Enables read-write access to this community string.

Defaults

The SNMP agent is disabled and a community string is not configured. When configured, an SNMP community string by default permits read-only access to all objects.

Usage Guidelines

The SNMP community string is used as a password for authentication when accessing the SNMP agent on the WAE. To be authenticated, the Community Name field of any SNMP message sent to the WAAS device must match the SNMP community string defined on the WAAS device.

The SNMP agent on the WAAS device is enabled when an SNMP community string is defined on the WAAS device. The maximum number of SNMP communities that can be created is 10.

The **snmp-server community string** global configuration command provides view-based access control for SNMPv1, SNMPv2c, and SNMPv3, yet continues to provide backward compatibility between different versions.



Tip Any SNMP message sent to the WAAS device must have the “Community Name” field of the message match the community string defined here to be authenticated.

It is possible to configure a community string that grants access to only part of the MIB subtree. To provide backward compatibility with previous versions of this command, a default read group or default write group (if the **rw** option is specified on the command line) is associated with the community string if no group name is specified. Both of these default groups are hidden from users and not displayed in the configuration file or in the **show snmp group EXEC** command, but are created during initialization of the SNMP agent.

Command Modes

global configuration

Device Modes

application-accelerator
 replication-accelerator
 central-manager

Examples

The following example enables the SNMP agent and assigns the community string comaccess to SNMP:

```
WAE(config)# snmp-server community comaccess
```

The following example disables the SNMP agent and removes the previously defined community string:

```
WAE(config)# no snmp-server community
```

Related Commands

- (config) snmp-server community
- (config) snmp-server contact
- (config) snmp-server enable traps
- (config) snmp-server group
- (config) snmp-server host
- (config) snmp-server location
- (config) snmp-server mib persist event
- (config) snmp-server notify inform
- (config) snmp-server trap-source
- (config) snmp-server user
- (config) snmp-server view
- snmp trigger

(config) snmp-server contact

To set the system server contact string on a WAAS device, use the **snmp-server contact** global configuration command. To remove the system contact information, use the **no** form of this command.

snmp-server contact *line*

Syntax Description	contact	line
	Specifies text for MIB-II object <i>sysContact</i> .	Identification of the contact person for this managed node.

Command Modes global configuration

Device Modes application-accelerator
replication-accelerator
central-manager

Defaults No system contact string is set.

Usage Guidelines The system contact string is the value stored in the MIB-II system group *sysContact* object.

Examples The following example sets a system contact string and then removes it:

```
WAE(config)# snmp-server contact Dial System Operator at beeper # 27345
WAE(config)# no snmp-server contact
```

Related Commands

- [\(config\) snmp-server community](#)
- [\(config\) snmp-server enable traps](#)
- [\(config\) snmp-server group](#)
- [\(config\) snmp-server host](#)
- [\(config\) snmp-server location](#)
- [\(config\) snmp-server mib persist event](#)
- [\(config\) snmp-server notify inform](#)
- [\(config\) snmp-server trap-source](#)
- [\(config\) snmp-server user](#)
- [\(config\) snmp-server view](#)
- [snmp trigger](#)

(config) snmp-server enable traps

To enable the WAAS device to send SNMP traps, use the **snmp-server enable traps** global configuration command. To disable all SNMP traps or only SNMP authentication traps, use the **no** form of this command.

```
snmp-server enable traps [alarm [clear-critical | clear-major | clear-minor | raise-critical |
raise-major | raise-minor] | config | content-engine [disk-fail | disk-read | disk-write |
overload-bypass | transaction-log] | entity | event | snmp [authentication | cold-start] |
wafs [cslog | eslog | mgrlog]]
```

Syntax Description

alarm	(Optional) Enables WAAS alarm traps.
clear-critical	(Optional) Enables clear-critical alarm trap.
clear-major	(Optional) Enables clear-major alarm trap.
clear-minor	(Optional) Enables clear-minor alarm trap.
raise-critical	(Optional) Enables raise-critical alarm trap.
raise-major	(Optional) Enables raise-major alarm trap.
raise-minor	(Optional) Enables raise-minor alarm trap.
config	(Optional) Enables CiscoConfigManEvent traps.
content-engine	(Optional) Enables SNMP WAAS traps.
disk-fail	(Optional) Enables disk failure error trap.
disk-read	(Optional) Enables disk read error trap.
disk-write	(Optional) Enables disk write error trap.
overload-bypass	(Optional) Enables WCCP overload bypass error trap.
transaction-log	(Optional) Enables transaction log write error trap.
entity	(Optional) Enables SNMP entity traps.
event	(Optional) Enables Event MIB traps.
snmp	(Optional) Enables SNMP-specific traps.
authentication	(Optional) Enables authentication trap.
cold-start	(Optional) Enables cold start trap.
wafs	(Optional) Enables all WAFS-specific traps.
cslog	(Optional) Enables the CS log traps.
eslog	(Optional) Enables the ES log traps.
mgrlog	(Optional) Enables the Manager log traps.

Defaults

This command is disabled by default. No traps are enabled.

Command Modes

global configuration

Device Modes

application-accelerator
 replication-accelerator
 central-manager

Usage Guidelines

You can configure a WAAS device to generate an SNMP trap for a specific alarm condition. You can configure the generation of SNMP alarm traps on the WAAS device based on the following:

- The severity of the alarm (critical, major, or minor)
- The action (the alarm is raised or cleared).

In the WAAS software release, the following six generic alarm traps are available in the CISCO-CONTENT-ENGINE-MIB.

Name of Alarm Trap	Severity	Action
cceAlarmCriticalRaised	Critical	Raised
cceAlarmCriticalCleared	Critical	Cleared
cceAlarmMajorRaised	Major	Raised
cceAlarmMajorCleared	Major	Cleared
cceAlarmMinorRaised	Minor	Raised
cceAlarmMinorCleared	Minor	Cleared

**Note**

By default, these six general alarm traps are disabled.

These six general alarm traps provide SNMP and Node Health Manager integration. Each of these six alarm traps can be enabled or disabled through the WAAS CLI.

To configure traps, you must enter the **snmp-server enable traps** command. If you do not enter an **snmp-server enable traps** command, no traps are sent.

The **snmp-server enable traps** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP traps. To send traps, you must configure at least one host using the **snmp-server host** command.

For a host to receive a trap, both the **snmp-server enable traps** command and the **snmp-server host** command for that host must be enabled.

In addition, SNMP must be enabled with the **snmp-server community** command.

To disable the sending of the MIB-II SNMP authentication trap, you must enter the command **no snmp-server enable traps snmp authentication**.

Examples

The following example enables the WAAS device to send all traps to the host 172.31.2.160 using the community string public:

```
WAE(config)# snmp-server enable traps
WAE(config)# snmp-server host 172.31.2.160 public
```

The following example disables all traps:

```
WAE(config)# no snmp-server enable traps
```

Related Commands

(config) snmp-server community
(config) snmp-server contact
(config) snmp-server group
(config) snmp-server host
(config) snmp-server location
(config) snmp-server mib persist event
(config) snmp-server notify inform
(config) snmp-server trap-source
(config) snmp-server user
(config) snmp-server view
snmp trigger

(config) snmp-server group

To define a user security model group for a WAAS device, use the **snmp-server group** global configuration command. To remove the specified group, use the **no** form of this command.

```
snmp-server group name {v1 [notify name] [read name] [write name] | v2c [notify name] [read
name] [write name] | v3 {auth [notify name] [read name] [write name] | noauth [notify name]
[read name] [write name] | priv [notify name] [read name] [write name]}}
```

Syntax	Description
<i>name</i>	Name of the SNMP group. Supports up to a maximum of 64 characters.
v1	Specifies the group using the Version 1 Security Model.
notify	(Optional) Specifies a notify view for the group that enables you to specify a notify, inform, or trap.
<i>name</i>	Notify view name. Supports up to a maximum of 64 characters.
read	(Optional) Specifies a read view for the group that enables you only to view the contents of the agent.
<i>name</i>	Read view name. Supports up to a maximum of 64 characters.
write	(Optional) Specifies a write view for the group that enables you to enter data and configure the contents of the agent.
<i>name</i>	Write view name. Supports up to a maximum of 64 characters.
v2c	Specifies the group using the Version 2c Security Model.
v3	Specifies the group using the User Security Model (SNMPv3).
auth	Specifies the group using the AuthNoPriv Security Level.
noauth	Specifies the group using the noAuthNoPriv Security Level.
priv	Specifies the group using the AuthPriv Security Level.

Defaults The default is that no user security model group is defined.

Command Modes global configuration

Device Modes application-accelerator
 replication-accelerator
 central-manager

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).

Examples

The following example defines a user security model group named *acme* that uses SNMP version 1 security model and a view name of *mymib* for notifications:

```
WAE(config)# snmp-server group acme v1 notify mymib
```

Related Commands

- (config) snmp-server community
- (config) snmp-server contact
- (config) snmp-server enable traps
- (config) snmp-server host
- (config) snmp-server location
- (config) snmp-server mib persist event
- (config) snmp-server notify inform
- (config) snmp-server trap-source
- (config) snmp-server user
- (config) snmp-server view
- snmp trigger

(config) snmp-server host

To specify the recipient of a host SNMP trap operation, use the **snmp-server host** global configuration command. To remove the specified host, use the **no** form of this command.

```
snmp-server host {hostname | ip-address} communitystring [v2c [retry number] [timeout
seconds] | [v3 {auth [retry number] [timeout seconds] | noauth [retry number] [timeout
seconds] | priv [retry number] [timeout seconds}]}
```

Syntax	Description
<i>hostname</i>	Hostname of the SNMP trap host that will be sent in the SNMP trap messages from the WAAS device.
<i>ip-address</i>	IP address of the SNMP trap host that will be sent in the SNMP trap messages from the WAAS device.
<i>communitystring</i>	Password-like community string sent in the SNMP trap messages from the WAE. You can enter a maximum of 64 characters.
v2c	(Optional) Specifies the Version 2c Security Model.
retry	(Optional) Sets the count for the number of retries for the inform request. (The default is 2 tries.)
<i>number</i>	Number of retries for the inform request (1–10).
timeout	(Optional) Sets the timeout for the inform request (1–1000). (The default is 15 seconds.)
<i>seconds</i>	Timeout value in seconds.
v3	(Optional) Specifies the User Security Model (SNMPv3).
auth	Sends notification using the AuthNoPriv Security Level.
noauth	Sends notification using the noAuthNoPriv Security Level.
priv	Sends notification using the AuthPriv Security Level.

Defaults

This command is disabled by default. No traps are sent. If enabled, the default version of the SNMP protocol used to send the traps is SNMP Version 1.

retry number: 2 retries

timeout: 15 seconds

Command Modes

global configuration

Device Modes

application-accelerator

replication-accelerator

central-manager

Usage Guidelines

If you do not enter an **snmp-server host** command, no traps are sent. To configure the WAAS device to send SNMP traps, you must enter at least one **snmp-server host** command. To enable multiple hosts, you must issue a separate **snmp-server host** command for each host. The maximum number of **snmp-server host** commands is four.

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 in conjunction with the **snmp-server enable traps** command to enable SNMP traps.

In addition, SNMP must be enabled 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:

```
WAE(config)# snmp-server enable traps
WAE(config)# snmp-server host 172.16.2.160 comaccess
```

The following example removes the host 172.16.2.160 from the SNMP trap recipient list:

```
WAE(config)# no snmp-server host 172.16.2.160
```

Related Commands

- [\(config\) snmp-server community](#)
- [\(config\) snmp-server contact](#)
- [\(config\) snmp-server enable traps](#)
- [\(config\) snmp-server group](#)
- [\(config\) snmp-server location](#)
- [\(config\) snmp-server mib persist event](#)
- [\(config\) snmp-server notify inform](#)
- [\(config\) snmp-server trap-source](#)
- [\(config\) snmp-server user](#)
- [\(config\) snmp-server view](#)
- [snmp trigger](#)

(config) snmp-server location

To set the SNMP system location string on a WAAS device, use the **snmp-server location** global configuration command. To remove the location string, use the **no** form of this command.

snmp-server location *line*

Syntax Description

location	Specifies text for MIB-II object <i>sysLocation</i> .
<i>line</i>	String that describes the physical location of this node.

Defaults

No system location string is set.

Command Modes

global configuration

Device Modes

application-accelerator
 replication-accelerator
 central-manager

Usage Guidelines

The system location string is the value stored in the MIB-II system group system location object. You can see the system location string with the **show snmp EXEC** command.

Examples

The following example shows a system location string:

```
WAE(config)# snmp-server location Building 3/Room 214
```

Related Commands

(config) snmp-server community
 (config) snmp-server contact
 (config) snmp-server enable traps
 (config) snmp-server group
 (config) snmp-server host
 (config) snmp-server mib persist event
 (config) snmp-server notify inform
 (config) snmp-server trap-source
 (config) snmp-server user
 (config) snmp-server view
 snmp trigger

(config) snmp-server mib persist event

To configure persistence for the SNMP Event MIB, use the **snmp-server mib persist event** global configuration command. To disable the Event MIB, use the **no** form of this command.

snmp-server mib persist event

Syntax Description

This command has no keywords or arguments.

Defaults

No default behavior or values

Command Modes

global configuration

Device Modes

application-accelerator
replication-accelerator
central-manager

Usage Guidelines

The Event MIB can set the threshold on any MIB variables supported by WAAS software and store the threshold permanently on disk.

The WAAS software implementation of SNMP supports the following MIBs:

- ACTONA-ACTASTORE-MIB
- CISCO-CONFIG-MAN-MIB
- CISCO-CDP-MIB
- CISCO-CONTENT-ENGINE-MIB (partial)
- CISCO-ENTITY-ASSET-MIB
- CISCO-SMI
- CISCO-TC
- ENTITY-MIB
- EVENT-MIB
- HOST-RESOURCES-MIB
- MIB-II
- SNMP-COMMUNITY-MIB
- SNMP-FRAMEWORK-MIB
- SNMP-NOTIFICATION-MIB
- SNMP-TARGET-MIB
- SNMP-USM-MIB
- SNMPv2

- SNMP-VACM-MIB

**Note**

In WAAS software, there are six generic alarm traps in the CISCO-CONTENT-ENGINE-MIB for SNMP and Node Health Manager integration.

In WAAS software, you can use IP ACLs to control SNMP access on a WAAS device.

Downloading MIB Files to WAEs

From the following Cisco FTP site you can download the MIB files for all of the MIBS that are supported by a WAAS device that is running WAAS software:

ftp://ftp.cisco.com/pub/mibs/v2

The MIB objects that are defined in each MIB are described in the MIB files at the above FTP site are self explanatory.

Examples

The following example sets persistence for the Event MIB:

```
WAE(config)# snmp-server mib persist event
```

Related Commands

(config) snmp-server community
 (config) snmp-server contact
 (config) snmp-server enable traps
 (config) snmp-server group
 (config) snmp-server host
 (config) snmp-server location
 (config) snmp-server notify inform
 (config) snmp-server trap-source
 (config) snmp-server user
 (config) snmp-server view
 snmp trigger

(config) snmp-server notify inform

To configure the SNMP notify inform request on WAAS device, use the **snmp-server notify inform** global configuration command. To return the setting to the default value, use the **no** form of this command.

snmp-server notify inform

Syntax Description

This command has no arguments or keywords.

Defaults

If you do not issue the **snmp-server notify inform** command, the default is an SNMP trap request.

Command Modes

global configuration

Device Modes

application-accelerator
replication-accelerator
central-manager

Examples

The following example configures an SNMP notify inform request versus the default SNMP trap:

```
WAE(config)# snmp-server notify inform
```

Related Commands

(config) snmp-server community
(config) snmp-server contact
(config) snmp-server enable traps
(config) snmp-server group
(config) snmp-server host
(config) snmp-server location
(config) snmp-server mib persist event
(config) snmp-server trap-source
(config) snmp-server user
(config) snmp-server view
snmp trigger

(config) snmp-server trap-source

To configure the network interface to be used for sending out SNMP trap messages from a WAAS device, use the **snmp-server trap-source** global configuration command. To remove the configured trap-source, use the **no** form of the command.

```
snmp-server trap-source {GigabitEthernet 1-2/port | PortChannel 1-2 | Standby group_num}
```

Syntax	Description
GigabitEthernet	Selects a Gigabit Ethernet interface's IP as trap source for sending SNMP trap messages.
<i>1-2/</i>	Gigabit Ethernet slot number 1 or 2.
<i>port</i>	Port number of the Gigabit Ethernet interface.
PortChannel	Selects a port channel interface's IP as trap source for sending SNMP trap messages.
<i>1-2</i>	Port Channel number 1 or 2.
Standby	Selects a standby group's IP as trap source for sending SNMP trap messages.
<i>group_num</i>	Standby group number 1–4.

Defaults The primary interface's IP is used as default trap source for sending SNMP traps. If the primary interface is not configured, then the local IP address of the WAAS device is used as trap source.

Command Modes global configuration

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines The **snmp-server trap-source** global configuration command allows you to specify the interface with the IP address that will be included in the SNMP trap messages as a trap source. To change the trap-source interface, reenter the command with a different network interface.

If there is no trap-source interface configured in the WAAS device, the IP address of the WAAS device's current primary interface is used. If the primary interface is not configured, the local IP address of the WAAS device is used as a trap source.

Examples The following example shows how to specify the Gigabit Ethernet slot 1 port 0 as the SNMP trap-source interface on a WAAS device:

```
WAE(config)# snmp-server trap-source GigabitEthernet 1/0
```

The following example shows how to specify the Gigabit Ethernet slot 2 port 0 as the SNMP trap-source interface on a WAAS device:

```
WAE(config)# snmp-server trap-source GigabitEthernet 2/0
```

Related Commands

- (config) snmp-server community
- (config) snmp-server contact
- (config) snmp-server enable traps
- (config) snmp-server group
- (config) snmp-server host
- (config) snmp-server location
- (config) snmp-server mib persist event
- (config) snmp-server notify inform
- (config) snmp-server user
- (config) snmp-server view
- snmp trigger

(config) snmp-server user

To define a user who can access the SNMP server, use the **snmp-server user** global configuration command. To remove access, use the **no** form of this command.

```
snmp-server user name group [auth {md5 password [priv password] | sha password [priv password]}] | remote octetstring [auth {md5 password [priv password] | sha password [priv password]}]]
```

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 WAAS device. You can enter a maximum of 64 characters.
<i>group</i>	Name of the group to which the SNMP user belongs. You can enter a maximum of 64 characters.
auth	(Optional) Configures user authentication parameters.
md5	Configures HMAC MD5 authentication algorithm.
<i>password</i>	HMAC-MD5 user authentication password.
priv	(Optional) Configures authentication parameters for the packet.
<i>password</i>	HMAC-MD5 user private password. You can enter a maximum of 256 characters.
sha	Configures HMAC-SHA authentication algorithm.
<i>password</i>	HMAC-SHA authentication password. You can enter a maximum of 256 characters.
remote	(Optional) Specifies engine identity of remote SNMP entity to which the user belongs.
<i>octetstring</i>	Globally unique identifier for a remote SNMP entity (for example, the SNMP network management station) for at least one of the SNMP users. Tip To send an SNMPv3 inform message, at least one SNMPv3 user with a remote SNMP ID option must be configured on the WAAS device. 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.

Defaults

No default behavior or values

Command Modes

global configuration

Device Modes

application-accelerator
replication-accelerator
central-manager

Usage Guidelines

When defining SNMP users for WAAS devices, note the following:

- If the SNMPv3 protocol is going to be used for SNMP requests, you must define at least one SNMPv3 user account on the WAAS device for the WAAS device to be accessed through SNMP.
- A group defined with the SNMPv1 or SNMPv2c security model should not be associated with SNMP users; they should only be associated with the community strings.

Examples

The following example shows how an SNMPv3 user account is created on the WAAS device. 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 WAAS device does not perform authentication on SNMP requests from this user.

```
WAE(config)# snmp-server user acme admin
```

Related Commands

(config) snmp-server community
(config) snmp-server contact
(config) snmp-server enable traps
(config) snmp-server group
(config) snmp-server host
(config) snmp-server location
(config) snmp-server mib persist event
(config) snmp-server notify inform
(config) snmp-server trap-source
(config) snmp-server view
snmp trigger

(config) snmp-server view

To define a SNMPv2 MIB view on a WAAS device, use the **snmp-server view** global configuration command. To remove the MIB view definition, use the **no** form of this command.

```
snmp-server view viewname MIBfamily { excluded | included }
```

Syntax Description		
<i>viewname</i>	Name of this family of view subtrees. You can enter a maximum of 64 characters.	
<i>MIBfamily</i>	Object identifier that identifies a subtree of the MIB. You can enter a maximum of 64 characters.	
excluded	Excludes MIB family from the view.	
included	Includes MIB family in the view.	

Defaults No default behavior or values

Command Modes global configuration

Device Modes application-accelerator
 replication-accelerator
 central-manager

Examples The following example defines an SNMPv2 MIB view:

```
WAE(config)# snmp-server view fileview ciscoFileEngineMIB included
```

Related Commands

- [\(config\) snmp-server community](#)
- [\(config\) snmp-server contact](#)
- [\(config\) snmp-server enable traps](#)
- [\(config\) snmp-server group](#)
- [\(config\) snmp-server host](#)
- [\(config\) snmp-server location](#)
- [\(config\) snmp-server mib persist event](#)
- [\(config\) snmp-server notify inform](#)
- [\(config\) snmp-server trap-source](#)
- [\(config\) snmp-server user](#)
- [snmp trigger](#)

(config) sshd

To enable the SSH daemon on a WAAS device, use the **sshd** command in global configuration mode. To disable the SSH daemon on a WAAS device, use the **no** form of this command.

```
sshd {allow-non-admin-users | enable | password-guesses number | timeout seconds |
      version {1 | 2}}
```

Syntax Description	
allow-non-admin-users	Allows nonadministrative users to gain SSH access to the chosen device (or device group). By default, this option is disabled. Note Nonadministrative users are non-superuser administrators. All non-superuser administrators only have restricted access to a WAAS device because their login accounts have a privilege level of 0. Superuser administrators have full access to a WAAS device because their login accounts have the highest level of privileges, a privilege level of 15.
enable	Enables the SSH daemon on a WAAS device.
password-guesses	Specifies the number of allowable password guesses per connection.
<i>number</i>	Maximum number of incorrect password guesses allowed (1–99). (The default is 3.)
timeout	Configures the number of seconds for which an SSH session will be active during the negotiation (authentication) phase between client and server before it times out. Note If you have established an SSH connection to the WAAS device but have not entered the username when prompted at the login prompt, the connection will be terminated by the WAAS device if the grace period expires even after successful login.
<i>seconds</i>	SSH login grace time value in seconds (1–99999). (The default is 300.)
version	Configures the SSH version to be supported on the WAAS device.
1	Specifies that SSH Version 1 is supported on the WAAS device.
2	Specifies that SSH Version 2 is supported on the WAAS device.

Defaults

By default, the SSH daemon is disabled on a WAAS device. If you use the **sshd enable** command to enable the SSH daemon on a WAAS device, the following default settings are used:

password-guesses *number*: 3 guesses

timeout *seconds*: 300 seconds

version: Both SSH Version 1 and 2 are enabled.

Command Modes

global configuration

Device Modes

application-accelerator

replication-accelerator

central-manager

Usage Guidelines

SSH enables login access to the WAAS device 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.

Before you enable the **sshd** command, use the **ssh-key-generate** command to generate a private and a public host key, which the client programs use to verify the server's identity.

Although the **sshd password-guesses** command specifies the number of allowable password guesses from the SSH server side, the actual number of password guesses for an SSH login session is determined by the combined number of allowable password guesses of the SSH server and the SSH client. Some SSH clients limit the maximum number of allowable password guesses to three (or to one in some cases), even though SSH server side allows more than this number of guesses.

When **sshd password-guesses** is entered, specifying *n* allowable password guesses, certain SSH clients interpret this *number* as *n+1*. For example, when configuring the number of guesses to two by issuing the command **sshd password-guesses 2** for a particular device, SSH sessions from some SSH clients will allow three password guesses.

You can enable both SSH Version 1 and Version 2, or you can enable one version and not the other. When you enable the SSH daemon using the **sshd enable** global configuration command, support for both SSH Version 1 and SSH Version 2 is enabled. If you want the WAAS device to support only one version of SSH (for example SSH version 2), you must disable the other version. For example, to disable SSH Version 1, enter the **no sshd version 1** command.

If the SSH daemon is currently enabled on a WAAS device, at least one version of SSH must be enabled on the device. Before you can disable both versions of SSH, you must enter the **no sshd enable** command to disable the SSH daemon on the WAAS device. If you attempt to disable both versions of SSH before you have disabled the SSH daemon, the following message will appear on your console informing you that you must disable the SSH daemon before you can disable both versions of SSH:

```
WAE(config)# no sshd version 1
WAE(config)# no sshd version 2
Atleast SSHv1 or SSHv2 must be enabled with sshd enabled.
Disable sshd to disable both SSHv1 and SSHv2.
Did not update ssh version support. Please retry.
```

When support for both SSH version 1 and SSH version 2 are enabled in the WAAS device, the **show running-config EXEC** command output does not display any SSHD configuration.

If you have disabled the support for one version of SSH, the **show running-config EXEC** command output contains the following line:

```
no sshd version version_number
```



Note

The Telnet daemon can still be used with the WAAS device. SSH does not replace Telnet.

Examples

The following example enables and configures a Secure Shell daemon on the WAAS device:

```
WAE(config)# sshd enable
WAE(config)# sshd password-guesses 4
WAE(config)# sshd timeout 20
```

The following example disables the support for SSH Version 1 in the WAAS device:

```
WAE(config)# no sshd version 1
```

Related Commands [\(config\) ssh-key-generate](#)

(config) ssh-key-generate

To generate the SSH host key for a WAAS device, use the **ssh-key-generate** global configuration command. To remove the SSH key, use the **no** form of the command.

```
ssh-key-generate [key-length length]
```

Syntax Description	key-length	(Optional) Configures the length of the SSH key.
	<i>length</i>	Number of bits to create an SSH key (512–2048).

Defaults **key-length** *length*: 1024 bits

Command Modes global configuration

Device Modes application-accelerator
 replication-accelerator
 central-manager

Usage Guidelines Before you enter the **sshd enable** command, enter the **ssh-key-generate** command to generate a private and a public host key, which the client programs use to verify a server's identity.

When you use an SSH client and log in to a WAAS device, the public key for the SSH daemon that is running on the device is recorded in the client machine known_hosts file in your home directory. If you subsequently regenerate the host key by specifying the number of bits in the **key-length** command option, you must delete the old public key entry associated with the WAAS device in the known_hosts file before running the SSH client program to log in to the WAAS device. When you use the SSH client program after deleting the old entry, the known_hosts file is updated with the new SSH public key for the WAAS device.

Examples The following example generates an SSH public key and then enables the SSH daemon on the WAAS device:

```
WAE(config)# ssh-key-generate
Ssh host key generated successfully
Saving the host key to box ...
Host key saved successfully
WAE(config)# sshd enable
Starting ssh daemon ...
Ssh daemon started successfully
```

Related Commands (config) [sshd](#)

(config) tacacs

To configure TACACS+ server parameters on a WAAS device, 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}
```

Syntax Description

host	Specifies a server address.
<i>hostname</i>	Hostname of the TACACS+ server.
<i>ip-address</i>	IP address of the TACACS+ server.
primary	(Optional) Sets the server as the primary server.
key	Sets the security word.
<i>keyword</i>	Keyword. An empty string is the default.
password <i>ascii</i>	Specifies ASCII as the TACACS+ password type.
retransmit	Sets the number of times that requests are retransmitted to a server.
<i>retries</i>	Number of retry attempts allowed (1–3). The default is 2 retry attempts.
timeout	Sets the number of seconds to wait before a request to a server is timed out.
<i>seconds</i>	Timeout in seconds (1–20). The default is 5 seconds.

Defaults

keyword: none (empty string)

timeout *seconds*: 5

retries: 2

password: The default password type is PAP.

Command Modes

global configuration

Device Modes

application-accelerator

replication-accelerator

central-manager

Usage Guidelines

One primary and two backup TACACS+ servers can be configured on a WAAS device; authentication is attempted on the primary server first, then on the others in the order in which they were configured. The primary server is the first server configured unless another is explicitly specified as primary with the **tacacs host** *hostname* **primary** command.

TACACS+ uses the standard port (port 49) for communication, based on the specified service. Using the **tacacs** command, configure the TACACS+ key, number of retransmits, server hostname or IP address, and timeout.

To enable user authentication with a TACACS+ server, use the **authentication** global configuration command. (See the “(config) authentication” command.)

The TACACS+ remote database can also be used to maintain login and configuration privileges for administrative users. The **tacacs host** command allows you to configure the network parameters required to access the remote database.

Use the **tacacs key** command to specify the TACACS+ key, used to encrypt the packets transmitted to the server. This key must be the same as the one specified on the server daemon. The maximum number of characters in the key should not exceed 99 printable ASCII characters (except tabs). An empty key string is the default. All leading spaces are ignored; spaces within and at the end of the key string are not ignored. Double quotes are not required even if there are spaces in the key, unless the quotes themselves are part of the key.

The **tacacs timeout** is the number of seconds that the WAAS device 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 WAAS device 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 PAP (Password Authentication Protocol). 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 password of the user. The server must have an appropriately configured account for the user.

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 account exists for a user, the client sends another Continue request with the password of the user. The authentication server must have an appropriately configured account for the user to support either type of password.

Examples

The following example configures the key used in encrypting packets:

```
WAE(config)# tacacs key human789
```

The following example configures the host named spearhead as the primary TACACS+ server:

```
WAE(config)# tacacs host spearhead primary
```

The following example sets the timeout interval for the TACACS+ server:

```
WAE(config)# tacacs timeout 10
```

The following example sets the number of times that authentication requests are retried (retransmitted) after a timeout:

```
WAE(config)# tacacs retransmit 5
```

The following example shows the password type to be PAP by default:

```
WAE# 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

```

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.

```

WAE(config)# tacacs password ascii
WAE(config)# exit
WAE# show tacacs
Login Authentication for Console/Telnet Session: enabled (secondary)
Configuration Authentication for Console/Telnet Session: enabled (secondary)

TACACS+ Configuration:
-----
TACACS+ Authentication is off
Key          = *****
Timeout      = 5
Retransmit   = 2
Password type: ascii

Server                               Status
-----
10.107.192.148                       primary
10.107.192.168
10.77.140.77

```

Related Commands

- [\(config\) authentication](#)
- [show authentication](#)
- [show statistics authentication](#)
- [show statistics tacacs](#)
- [show tacacs](#)

(config) tcp

To configure TCP parameters on a WAAS device, use the **tcp** global configuration command. To disable TCP parameters, use the **no** form of this command.

tcp cwnd-base *segments*

tcp ecn enable

tcp increase-xmit-timer-value *value*

tcp init-ss-threshold *value*

tcp keepalive-probe-cnt *count*

tcp keepalive-probe-interval *seconds*

tcp keepalive-timeout *seconds*

tcp memory-limit low-water-mark *low* **high-water-mark-pressure** *high*
high-water-mark-absolute *absolute*

Syntax Description

cwnd-base	Sets initial send congestion window in segments.
<i>segments</i>	Initial send congestion window segments (1–10).
ecn enable	Enables TCP explicit congestion notification.
increase-xmit-timer-value	Specifies the factor (1-3) used to modify the length of the retransmit timer by 1 to 3 times the base value determined by the TCP algorithm.
Note	Modify this factor with caution. It can improve throughput when TCP is used over slow reliable connections but should never be changed in an unreliable packet delivery environment.
<i>value</i>	Retransmit multiple (1–3).
init-ss-threshold	Sets initial slow-start threshold value.
<i>value</i>	Slow-start threshold value.
keepalive-probe-cnt	Specifies the length of time that the WAAS device keeps an idle connection open.
<i>count</i>	Number of probe counts (1–10).
keepalive-probe-interval	Specifies the number of times that the WAAS device retries a connection.
<i>seconds</i>	Keepalive probe interval in seconds (1–300).
keepalive-timeout	Specifies the length of time that the WAAS device keeps a connection open before disconnecting.
<i>seconds</i>	Keepalive timeout in seconds (1–3600).
memory-limit	Specifies the system TCP memory usage limit (including send and receive buffer usage of all connections).



Caution

To prevent TCP buffer overflow, do not modify the default values unless you are sure of the procedure.

low-water-mark	Specifies the memory usage mark (in megabytes) below which TCP goes out of the memory pressure mode and enters into the normal memory allocation mode.
<i>low</i>	Memory usage in megabytes (4–600).
high-water-mark-pressure	Specifies the memory usage mark (in megabytes) above which TCP goes out of the normal memory allocation mode and enters the memory pressure mode.
<i>high</i>	Memory usage in megabytes (5–610).
high-water-mark-absolute	Specifies the absolute hard limit on TCP memory usage (in megabytes).
<i>absolute</i>	Memory usage in megabytes (6–620).

Defaults

tcp cwnd-base: 2
tcp increase-xmit-timer-value: 1
tcp init-ss-threshold: 2 segments
tcp keepalive-probe-cnt: 4
tcp keepalive-probe-interval: 75 seconds
tcp keepalive-timeout: 90 seconds

Command Modes

global configuration

Device Modes

application-accelerator
 replication-accelerator
 central-manager

Usage Guidelines

You can adjust the TCP stack parameters to maximize cache performance and throughput of HTTP streams over TCP end to end. The relevant TCP parameters to maximize cache performance and throughput include the ability to tune timeout periods, client and server receive and send buffer sizes, and TCP window scaling behavior.



Note

Because of the complexities involved in TCP parameters, care is advised in tuning these parameters. In nearly all environments, the default TCP settings are adequate. Fine tuning of TCP settings is for network administrators with adequate experience and full understanding of TCP operation details. See the *Cisco Wide Area Application Services Configuration Guide* for more information.

Use the **tcp keepalive-probe-cnt** global configuration command to specify how many times the WAAS device should attempt to connect to the device before closing the connection. The count can be from 1 to 10. The default is 4 attempts.

Use the **tcp keepalive-probe-interval** global configuration command to specify how often the WAAS device is to send out a TCP keepalive. The interval can be from 1 to 120 seconds. The default is 75 seconds.

Use the **tcp keepalive-timeout** global configuration command to wait for a response (the device does not respond) before the WAAS device logs a miss. The timeout can be from 1 to 120 seconds. The default is 90 seconds.

Examples

The following example enables TCP explicit congestion notification:

```
WAE(config)# tcp ecn enable
```

The following example specifies a low watermark memory usage of 100 MB, a high watermark memory usage of 450 MB, and an absolute high watermark memory usage of 500 MB:

```
WAE(config)# tcp memory-limit low-water-mark 100 high-water-mark-pressure 450  
high-water-mark-absolute 500
```

Related Commands

[clear](#)

[show statistics tcp](#)

[show tcp](#)

(config) telnet enable

To enable Telnet on a WAAS device, use the **telnet enable** global configuration command.

telnet enable

Syntax Description This command has no arguments or keywords.

Defaults By default, the Telnet service is enabled on a WAAS device.

Command Modes global configuration

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines Use terminal emulation software to start a Telnet session with a WAAS device. You must use a console connection instead of a Telnet session to define device network settings on the WAAS device. However, after you have used a console connection to define the device network settings, you can use a Telnet session to perform subsequent configuration tasks.



Note

Messages transported between the client and the device are not encrypted.

Examples The following example enables the use of Telnet on the WAAS device:

```
WAE(config)# telnet enable
```

Related Commands [telnet](#)
[show telnet](#)

(config) tfo auto-discovery

To configure a WAE to automatically discover origin servers (such as those servers behind firewalls) that cannot receive TCP packets with setup options and add these server IP addresses to a blacklist for a specified number of minutes, use the **tfo auto-discovery blacklist** global configuration command. To disable TFO auto-discovery, use the **no** form of this command .

```
tfo auto-discovery [blacklist] {enable | hold-time minutes}
```

Syntax Description		
enable		Activates the TFO auto-discovery feature.
blacklist enable		Activates the TFO auto-discovery blacklist feature.
blacklist hold-time		Specifies the maximum time to hold the blacklisted server address in the cache.
<i>minutes</i>		Number of minutes to hold the server blacklist entry. The range is 1–10080 minutes. The default is 60 minutes.

Defaults The default TFO auto-discovery blacklist hold time is 60 minutes.

Command Modes global configuration

Device Modes application-accelerator

Usage Guidelines Use the **tfo auto-discovery blacklist hold-time** command to adjust the blacklist hold time for the TFO auto-discovery feature. With auto-discovery, the WAE keeps track of origin servers (such as those servers behind firewalls) that cannot receive optioned TCP packets and learns not to send out TCP packets with options to these blacklisted servers. When a server IP address is added to the blacklist, it remains on the blacklist for the configured number of minutes. After the hold time expires, subsequent connection attempts will again include TCP options so that the WAE can redetermine if the server can receive them. Resending TCP options periodically is useful because network packet loss could cause a server to be blacklisted erroneously.

Related Commands [show statistics tfo](#)
[show tfo status](#)

(config) tfo optimize

To configure a WAE for Traffic Flow Optimization (TFO), use the **tfo optimize** global configuration command. Use the **no** form of this command to disable TFO optimization.

```
tfo optimize {DRE {yes | no} compression {LZ | none} | full}
```

Syntax Description	DRE	Configures TFO optimization with or without Data Redundancy Elimination (DRE).
	yes	Enables DRE.
	no	Disables DRE.
compression		Configures TFO optimization with or without generic compression.
	LZ	Configures TFO optimization with Lempel-Ziv (LZ) compression.
	none	Configures TFO optimization with no compression.
	full	Configures TFO optimization with DRE and LZ compression. Using this keyword is the same as specifying the tfo optimize DRE yes compression LZ command.

Defaults The default TFO optimization on a WAAS device is **tfo optimize full**.

Command Modes global configuration

Device Modes application-accelerator

Related Commands

- [show statistics tfo](#)
- [show tfo bufpool](#)
- [show tfo status](#)

(config) tfo tcp keepalive

To configure a WAE for Traffic Flow Optimization (TFO) optimization with TCP keepalive, use the **tfo tcp keepalive** global configuration command.

tfo tcp keepalive

Syntax Description	This command has no keywords or arguments.
Defaults	Keepalive is disabled by default.
Command Modes	global configuration
Device Modes	application-accelerator
Usage Guidelines	This command enables TCP keepalive on the TFO optimized sockets (the connection between two peer WAE's).
Related Commands	(config) tfo tcp optimized-mss (config) tfo tcp optimized-receive-buffer (config) tfo tcp optimized-send-buffer (config) tfo tcp original-mss (config) tfo tcp original-receive-buffer (config) tfo tcp original-send-buffer

(config) tfo tcp optimized-mss

To configure a WAE for Traffic Flow Optimization (TFO) optimization with an optimized-side TCP maximum segment size, use the **tfo tcp optimized-mss** global configuration command.

tfo tcp optimized-mss *segment-size*

Syntax Description	<i>segment-size</i> Segment size (512–1460).
Defaults	The default value of the segment size is 1432 bytes.
Command Modes	global configuration
Device Modes	application-accelerator
Usage Guidelines	This command sets the TCP maximum segment size on TFO optimized sockets (the connection between two peer WAEs).
Related Commands	(config) tfo tcp keepalive (config) tfo tcp optimized-receive-buffer (config) tfo tcp optimized-send-buffer (config) tfo tcp original-mss (config) tfo tcp original-receive-buffer (config) tfo tcp original-send-buffer

(config) tfo tcp optimized-receive-buffer

To configure a WAE for Traffic Flow Optimization (TFO) optimization with an optimized-side receive buffer, use the **tfo tcp optimized-receive-buffer** global configuration command.

tfo tcp optimized-receive-buffer *buffer-size*

Syntax Description	<i>buffer-size</i>	Receive buffer size in kilobytes.
---------------------------	--------------------	-----------------------------------

Defaults	32 KB
-----------------	-------

Command Modes	global configuration
----------------------	----------------------

Device Modes	application-accelerator
---------------------	-------------------------

Usage Guidelines	This command sets the TCP receive buffer size on TFO optimized sockets (the connection between two peer WAEs). For high Bandwidth Delay Product (BDP) links, you should use a value larger than the default.
-------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

The buffer should be equal to or greater than the BDP. The BDP is equivalent to the bandwidth (in bits per second) * latency (in seconds). For example, for a 45-Mbps link with a 150-ms (0.15 sec) round-trip delay, the BDP is 45 Mbps * 0.15 sec = 6.75 Mb, or 0.844 MB (844 KB). In this case, you could set the buffer size to 1024 KB.

Related Commands	<p>(config) tfo tcp keepalive</p> <p>(config) tfo tcp optimized-mss</p> <p>(config) tfo tcp optimized-send-buffer</p> <p>(config) tfo tcp original-mss</p> <p>(config) tfo tcp original-receive-buffer</p> <p>(config) tfo tcp original-send-buffer</p>
-------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

(config) tfo tcp optimized-send-buffer

To configure a WAE for Traffic Flow Optimization (TFO) optimization with an optimized-side send buffer, use the **tfo tcp optimized-send-buffer** global configuration command.

tfo tcp optimized-send-buffer *buffer-size*

Syntax Description	<i>buffer-size</i> Send buffer size in kilobytes.
Defaults	32 KB
Command Modes	global configuration
Device Modes	application-accelerator
Usage Guidelines	<p>This command sets the TCP send buffer size on TFO optimized sockets (the connection between two peer WAEs). For high Bandwidth Delay Product (BDP) links, you should use a value larger than the default.</p> <p>The buffer should be equal to or greater than the BDP. The BDP is equivalent to the bandwidth (in bits per second) * latency (in seconds). For example, for a 45-Mbps link with a 150-ms (0.15 sec) round-trip delay, the BDP is 45 Mbps * 0.15 sec = 6.75 Mb, or 0.844 MB (844 KB). In this case, you could set the buffer size to 1024 KB.</p>
Related Commands	<p>(config) tfo tcp keepalive</p> <p>(config) tfo tcp optimized-mss</p> <p>(config) tfo tcp optimized-receive-buffer</p> <p>(config) tfo tcp original-mss</p> <p>(config) tfo tcp original-receive-buffer</p> <p>(config) tfo tcp original-send-buffer</p>

(config) tfo tcp original-mss

To configure a WAE for Traffic Flow Optimization (TFO) optimization with an unoptimized-side TCP maximum segment size, use the **tfo tcp original-mss** global configuration command.

tfo tcp original-mss *segment-size*

Syntax Description	<i>segment-size</i> Segment size (512–1460).
Defaults	1432 bytes
Command Modes	global configuration
Device Modes	application-accelerator
Usage Guidelines	This command sets the TCP maximum segment size on TFO unoptimized sockets (the connection between the WAE and the client or the WAE and the server).
Related Commands	<p>(config) tfo tcp keepalive</p> <p>(config) tfo tcp optimized-mss</p> <p>(config) tfo tcp optimized-receive-buffer</p> <p>(config) tfo tcp optimized-send-buffer</p> <p>(config) tfo tcp original-receive-buffer</p> <p>(config) tfo tcp original-send-buffer</p>

(config) tfo tcp original-receive-buffer

To configure a WAE for Traffic Flow Optimization (TFO) optimization with an unoptimized-side receive buffer, use the **tfo tcp original-receive-buffer** global configuration command.

```
tfo tcp original-receive-buffer buffer-size
```

Syntax Description	<i>buffer-size</i> Receive buffer size in kilobytes.
Defaults	32 KB
Command Modes	global configuration
Device Modes	application-accelerator
Usage Guidelines	This command sets the TCP receive buffer size on TFO unoptimized sockets (the connection between the WAE and the client or the WAE and the server).
Related Commands	(config) tfo tcp keepalive (config) tfo tcp optimized-mss (config) tfo tcp optimized-receive-buffer (config) tfo tcp optimized-send-buffer (config) tfo tcp original-mss (config) tfo tcp original-send-buffer

(config) tfo tcp original-send-buffer

To configure a WAE for Traffic Flow Optimization (TFO) optimization with an unoptimized-side send buffer, use the **tfo tcp original-send-buffer** global configuration command.

tfo tcp original-send-buffer *buffer-size*

Syntax Description	<i>buffer-size</i> Send buffer size in kilobytes.
Defaults	32 KB
Command Modes	global configuration
Device Modes	application-accelerator
Usage Guidelines	This command sets the TCP send buffer size on TFO unoptimized sockets (the connection between the WAE and the client or the WAE and the server).
Related Commands	(config) tfo tcp keepalive (config) tfo tcp optimized-mss (config) tfo tcp optimized-receive-buffer (config) tfo tcp optimized-send-buffer (config) tfo tcp original-mss (config) tfo tcp original-receive-buffer

(config) transaction-logs

To configure and enable transaction logging on a WAE, use the **transaction-logs** global configuration command. To disable a transaction logging option, use the **no** form of this command.

transaction-logs tfo enable

transaction-logs tfo logging {enable | facility *parameter* | host {*hostname* | *ip-address*} [**port** *port-num*]} [**rate-limit** *number-message-per-sec*]

transaction-logs tfo archive interval *seconds*

transaction-logs tfo archive interval every-day {**at** *hour:minute* | **every** *hours*}

transaction-logs tfo archive interval every-hour {**at** *minute* | **every** *minutes*}

transaction-logs tfo archive interval every-week [**on** *weekdays* **at** *hour:minute*]

transaction-logs tfo archive max-file-size *filesize*

transaction-logs export compress

transaction-logs export enable

transaction-logs export ftp-server {*hostname* | *servipaddrs*} *login passw directory*

transaction-logs export interval *minutes*

transaction-logs export interval every-day {**at** *hour:minute* | **every** *hours*}

transaction-logs export interval every-hour {**at** *minute* | **every** *minutes*}

transaction-logs export interval every-week [**on** *weekdays* **at** *hour:minute*]

transaction-logs export sftp-server {*hostname* | *servipaddrs*} *login passw directory*

Syntax Description

tfo	Specifies the TFO transaction log feature.
enable	Enables the TFO transaction log feature.
logging	Specifies logging TFO transactions to a remote syslog host.
enable	Enables logging TFO transactions to a remote syslog host.
facility	Specifies the appropriate transaction log facility. This drop-down list is set to an initial value of Do not set. This setting denotes that the facility sent to the syslog host will be the facility on the local host that is sending the syslog message. For instance, in the case of the transaction logging module that sends the real-time transaction log message, the facility is the “user” facility.

<i>parameter</i>	Specifies one of the following facilities: auth Authorization system daemon System daemons kern Kernel local0 Local use local1 Local use local2 Local use local3 Local use local4 Local use local5 Local use local6 Local use local7 Local use mail Mail system news USENET news syslog Syslog itself user User process uucp UUCP system
host	Configures the remote syslog server.
<i>hostname</i>	Hostname or IP address of the remote syslog server to which transaction logs must be sent. No remote syslog server is specified by default.
<i>ip-address</i>	IP address of the remote syslog server.
port	(Optional) Configures the port to use when sending transaction log messages to the syslog server.
<i>port-num</i>	Destination port on the remote syslog host to which the WAE should send the transaction log files. The default port number is 514. This port is a well-known port for system logging.
rate-limit	(Optional) Configures the rate at which the transaction logger is allowed to send messages to the remote syslog server.
<i>number-message-per-sec</i>	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, the specified remote syslog host drops the messages. There is no default rate limit (rate-limit is set to 0), and by default all syslog messages are sent to all of the configured syslog hosts. The range is 1 to 10,000 messages per second.
archive	Configures archive parameters.
interval	Determines how frequently the archive file is to be saved.
<i>seconds</i>	Frequency of archiving in seconds (120–604800).
every-day	Archives using intervals of 1 day or less.
at	Specifies the local time at which to archive each day.
<i>hour:minute</i>	Time of day at which to archive in local time (hh:mm).
every	Specifies the interval in hours. Interval aligns with midnight.

<i>hours</i>	Number of hours for daily file archive. 1 Hourly 12 Every 12 hours 2 Every 2 hours 24 Every 24 hours 3 Every 3 hours 4 Every 4 hours 6 Every 6 hours 8 Every 8 hours
every-hour	Specifies the archives using intervals of 1 hour or less.
at	Sets the time to archive at each hour.
<i>minute</i>	Minute alignment for the hourly archive (0–59).
every	Specifies the interval in minutes for hourly archive that aligns with the top of the hour.
<i>minutes</i>	Number of minutes for hourly archive. 10 Every 10 minutes 15 Every 15 minutes 2 Every 2 minutes 20 Every 20 minutes 30 Every 30 minutes 5 Every 5 minutes
every-week	Archives using intervals of 1 or more times a week.
on	(Optional) Sets the day of the week on which to archive.
<i>weekdays</i>	Weekdays on which to archive. One or more weekdays can be specified. Fri Every Friday Mon Every Monday Sat Every Saturday Sun Every Sunday Thu Every Thursday Tue Every Tuesday Wed Every Wednesday
at	(Optional) Sets the local time at which to archive each day.
<i>hour:minute</i>	Time of day at which to archive in local time (hh:mm).
max-file-size	Specifies the maximum size (in kilobytes) of the archive file to be maintained on the local disk.
<i>filesize</i>	Maximum archive file size in kilobytes (1000–2000000). This value is the maximum size of the archived file to be maintained on the local disk.
export	Configures file export parameters. The FTP export feature can support up to four servers. Each server must be configured with a username, password, and directory that are valid for that server.
compress	Enables compression of archived log files into zip format before exporting them to external FTP servers.
enable	Enables the exporting of log files at the specified interval.
ftp-server	Sets the FTP server to receive exported archived files.
<i>hostname</i>	Hostname of the target FTP server.
<i>servipaddr</i>	IP address of the target FTP server.

<i>login</i>	User login to target FTP server.
<i>passwd</i>	User password to target FTP server.
<i>directory</i>	Target directory path for exported files on FTP server.
interval	Specifies the interval at which the working log should be cleared by moving data to the FTP server.
<i>minutes</i>	Number of minutes in the interval at which to export a file (1–10080).
every-day	Specifies the exports using intervals of 1 day or less.
at	Specifies the local time at which to export each day.
<i>hour:minute</i>	Time of day at which to export in local time (hh:mm).
every	Specifies the interval in hours for the daily export.
<i>hours</i>	Number of hours for the daily export. 1 Hourly 12 Every 12 hours 2 Every 2 hours 24 Every 24 hours 3 Every 3 hours 4 Every 4 hours 6 Every 6 hours 8 Every 8 hours
every-hour	Specifies the exports using intervals of 1 hour or less.
at	Specifies the time at which to export each hour.
<i>minute</i>	Minute (0–59) alignment for the hourly export.
every	Specifies the interval in minutes that align with the top of the hour.
<i>minutes</i>	Number of minutes for the hourly export. 10 Every 10 minutes 15 Every 15 minutes 2 Every 2 minutes 20 Every 20 minutes 30 Every 30 minutes 5 Every 5 minutes
every-week	Specifies the exports using intervals of 1 or more times a week.
on	(Optional) Specifies the days of the week for the export.
<i>weekdays</i>	Weekdays on which to export. One or more weekdays can be specified. Fri Every Friday Mon Every Monday Sat Every Saturday Sun Every Sunday Thu Every Thursday Tue Every Tuesday Wed Every Wednesday
at	(Optional) Specifies the time of day at which to perform the weekly export.
<i>hour:minute</i>	Time of day at which to export in the local time (hh:mm).
sftp-server	Sets the Secure File Transfer Protocol (SFTP) server to receive exported archived files.
<i>hostname</i>	Hostname of the target SFTP server.

<i>servipaddr</i>	IP address of the target SFTP server.
<i>login</i>	User login to the target SFTP server (less than 40 characters).
<i>passwd</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.

Defaults

archive: disabled
enable: disabled
export compress: disabled
export: disabled
archive interval: every day, every one hour
archive max-file-size: 2,000,000 KB
export interval: every day, every one hour
logging port *port-num*: 514

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

Depending upon where the sysfs is mounted, transactions are logged to a working log on the local disk in one of these files:

- /local1/logs/working.log
- /local2/logs/working.log

When you enable transaction logging, you can specify the interval at which the working log should be cleared by moving the data to an archive log. The archive log files are located on the local disk in the directory /local1/logs/ or /local2/logs/, depending upon where the sysfs is mounted.

Because multiple archive files are saved, the filename includes the time stamp when the file was archived. Because the files can be exported to an FTP/SFTP server, the filename also contains the IP address of this WAE.

The archive file name uses this format:

celog_IPADDRESS_YYYYMMDD_HHMMSS.txt.

You can monitor transaction logs in real-time for particular errors such as authentication errors. By sending HTTP transaction log messages to a remote syslog server, you can monitor the remote syslog server for HTTP request authentication failures in real-time. This real-time transaction log feature 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.

For this purpose, you must configure the WAE to send transaction log messages to a remote syslog server using UDP as the transport protocol. Because UDP is an unreliable transport protocol, message transport to a remote syslog host is not reliable and you must monitor the syslog messages received at the remote

syslog server. You can limit the rate at which the transaction logging module is allowed to send messages to the remote syslog server. The format of the syslog message is in standard syslog message format with the transaction log message as the payload of the syslog message.

Real-time transaction logging to a remote syslog server uses the standard syslog message format with the message payload as the transaction log entry. A new syslog error identifier is defined for this type of real-time transaction log message. You can configure a WAE to send transaction log messages in real-time to one remote syslog host. The message format of the transaction log entry to the remote syslog host is the same as in the transaction log file and prepended with Cisco's standard syslog header information.

The following is an example of the format of the real-time syslog message sent from the transaction logging module (WAE) to the remote syslog host:

```
fac-pri Apr 22 20:10:46 ce-host cache: %CE-TRNSLG-6-460012: translog formatted msg
```

The fields in the message are described as follows:

- *fac-pri* denotes the facility parameter and priority for transaction log messages encoded (as in standard syslog format) as a 32-bit decimal value between 0 and 1023 (0x0000 and 0x03FF). The least significant 3 bits denote priority (0-7) and the next least significant 7 bits denote facility (0-127).

The facility parameter used by the transaction logging module when a real-time transaction log message is logged to the remote syslog host is *user*. The same facility is sent to the remote syslog host unless you configure a different facility parameter for transaction logging. The priority field is always set to LOG_INFO for real-time transaction log messages.

In the above example, the default value of *fac-pri* is 14 (0x000E) where facility = user (LOG_USER (1)) and priority = LOG_INFO (6).

- The next field in the message is the date, which follows the format as shown in the above example.
- *ce-host* is the hostname or IP of the WAE that is sending the message.
- *cache* is the name of the process on the WAE that is sending the message.
- %CE-TRNSLG-6-460012 is the Cisco standard formatted syslog header on the WAE for a real-time transaction log message. This identifier indicates a priority level of 6, which denotes informational messages.



Note The WAAS system syslog messages report communication errors with the remote syslog host that is configured for transaction logging. These syslog messages are in the error message range: %CE-TRNSLG-6-460013 to %CE-TRNSLG-3-460016. The last error message (%CE-TRNSLG-3-460016), shows level “3” (for error-level messages) instead of “6” (for information-level messages). Information-level messages are reported when messages are dropped due to rate limiting and the number of dropped messages are reported. For more information about these syslog messages, see the *Cisco WAAS System Messages Reference*.

- *translog formatted msg* is the transaction log message as it appears in the transaction log file.



Note The total length of the real-time syslog message is 1024 characters. If the actual transaction log entry exceeds this limit, it is truncated.

When the remote syslog server logs this message to a file, the format appears as follows:

```
Apr 22 20:10:46 ce-host cache: %CE-TRNSLG-6-460012: translog formatted msg
```

where ce-host is the hostname of the WAE that sent the real-time transaction log message to the remote syslog server.

The configuration of host settings for transaction logs is identical to the configuration settings for syslog messages except that you need not specify the priority level of the message for real time transaction logs. All messages are associated with the priority level of 6 (LOG_INFO). You are not required to filter messages based on priority levels.

Related Commands

[clear](#)

[show transaction-logging](#)

[transaction-log](#)

(config) username

To establish username authentication on a WAAS device, use the **username** global configuration command.

```
username name {passwd | print-admin-passwd | privilege {0 | 15}}
```

Syntax Description

<i>name</i>	Username.
passwd	Specifies the password for the user interactively. You are prompted to enter the password, and then prompted again to re-enter the password to confirm it.
print-admin-passwd	Sets the user's print administration password interactively. You are prompted to enter the password, and then prompted again to re-enter the password to confirm it.
privilege	Sets the user privilege level.
0	Specifies the user privilege level for normal user.
15	Specifies the user privilege level for superuser.

Defaults

Default administrator account:

- Username: admin
- Password: default
- Privilege: superuser (15)

Command Modes

global configuration

Device Modes

application-accelerator
 replication-accelerator
 central-manager

Usage Guidelines

A system administrator can log in to a WAAS device that is functioning as a Core or Edge WAE through the console port or the WAE Device Manager GUI. An administrator can log in to the WAAS Central Manager through the console port or the WAAS Central Manager GUI.

When the system administrator logs in to a WAAS device before authentication and authorization have been configured, the administrator can access the WAAS device by using the predefined superuser account (the predefined username is *admin* and the predefined password is *default*). When you log in to a WAAS device using this predefined superuser account, you are granted access to all the WAAS services and entities in the WAAS system.

After you have initially configured your WAAS devices, we strongly recommend that you immediately change the password for the predefined superuser account (the predefined username is *admin*, the password is *default*, and the privilege level is superuser, privilege level 15) on each WAAS device.

If the predefined password for this superuser account has not been changed on a WAAS device, the following message is displayed each time you use this superuser account to log in to the WAAS CLI:

```
Device is configured with a (well known) default username/password
for ease of initial configuration. This default username/password
should be changed in order to avoid unwanted access to the device.
```

```
System Initialization Finished.
waas-cm#
```

If the predefined password for this superuser account has not been changed on a WAAS Central Manager, a dialog box is also displayed each time you use this superuser account to log in to the WAAS Central Manager GUI.



Note We strongly recommend that you use the WAAS Central Manager GUI instead of the WAAS CLI to configure passwords and privilege levels for users on your WAAS devices, if possible. For information about how to use the WAAS Central Manager GUI to centrally configure and administer users on an single WAE or group of WAEs, which are registered with a WAAS Central Manager, see the *Cisco Wide Area Application Services Configuration Guide*.

The **username** global configuration command allows you to change the password and privilege level for existing user accounts. To change the password for the predefined superuser account on a per device basis, use the **passwd** option of the **username** global configuration command:

```
waas-cm(config)# username admin passwd
```

For example, change the predefined password for the superuser account to *mysecret* for the WAAS Central Manager named *waas-cm*, as follows:

```
waas-cm# config
waas-cm(config)# username admin passwd
Warning: User configuration performed via CLI may be overwritten
by the central manager. Please use the central manager to configure
user accounts.
New UNIX password: mysecret (Note that the text is not displayed)
Retype new UNIX password: mysecret
waas-cm(config)# exit
```

User Authentication

User access is controlled at the authentication level. For every HTTP request, including every WAAS CLI request, that arrives at the WAAS device, 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 EXEC** command.

User Authorization

Domains and roles are applied by the WAAS device at the authorization level. Requests must be accepted by the authentication level before they are considered by the authorization level. The authorization level regulates access to resources based on the specified role in WAAS Central Manager GUI and domain configuration.

Regardless of the authentication mechanism, all user authorization configuration is visible in the GUI.

Examples

The following example demonstrates how passwords and privilege levels are reconfigured:

```
WAE# show user username abeddoe
Uid           : 2003
Username      : abeddoe
Password      : *****
Privilege     : normal user
```

```
WAE# show user username bwhidney
Uid           : 2002
Username      : bwhidney
Password      : *****
Privilege     : normal user
```

```
WAE(config)# username bwhidney passwd
Warning: User configuration performed via CLI may be overwritten
by the central manager. Please use the central manager to configure
user accounts.
New UNIX password: newpassword (Note that the text is not displayed)
Retype new UNIX password: newpassword
```

```
WAE(config)# username abeddoe privilege 15
Warning: User configuration performed via CLI may be overwritten
by the central manager. Please use the central manager to configure
user accounts.
```

```
WAE# show user username abeddoe
Uid           : 2003
Username      : abeddoe
Password      : *****
Privilege     : super user
Configured in : Local database
```

```
WAE# show user username bwhidney
Uid           : 2002
Username      : bwhidney
Password      : *****
Privilege     : normal user
Configured in : Local database
```

Related Commands

[show user](#)

(config) wccp access-list

To configure an IP access list on a WAE for inbound WCCP GRE encapsulated traffic, use the **wccp access-list** global configuration command.

```
wccp access-list {acl-number | ext-acl-number | acl-name}
```

Syntax Description

<i>acl-number</i>	Standard IP access list number (1–99).
<i>ext-acl-number</i>	Extended IP access list number (100–199).
<i>acl-name</i>	Name of the access list (30 characters maximum).

Defaults

WCCP access lists are not configured by default.

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

The **wccp access-list** *number* global configuration command configures an access control list to allow access to WCCP applications. The *number* variable is a number in the range 1 to 99, indicating a standard access control list or a number in the range 100 to 199, indicating an extended access control list. WCCP checks against the specified access control list before accepting or dropping incoming packets.

See the *Cisco Wide Area Application Services Configuration Guide* for a detailed description of how to use standard IP ACLs to control WCCP access on a WAE.



Note

WCCP works only with IPv4 networks.

Examples

The following example configures the WAE to apply IP access list number 10 to inbound WCCP traffic:

```
WAE(config)# wccp access-list 10
```

The following example shows sample output from the **show ip access-list EXEC** command from a WAE that has several WCCP access lists configured:

```
WAE(config)# show ip access-list
Space available:
  40 access lists
  489 access list conditions

Standard IP access list 10
  1 deny 10.1.1.1
  2 deny any
    (implicit deny any: 0 matches)
  total invocations: 0
Standard IP access list 98
  1 permit any
```

```

        (implicit deny any: 0 matches)
    total invocations: 0
Extended IP access list 100
  1 permit icmp any any
    (implicit fragment permit: 0 matches)
    (implicit deny ip any any: 0 matches)
  total invocations: 0
Extended IP access list 101
  1 permit ip any any
    (implicit fragment permit: 0 matches)
    (implicit deny ip any any: 0 matches)
  total invocations: 0
Extended IP access list 102
  1 permit icmp 0.0.1.1 255.255.0.0 any
    (implicit fragment permit: 0 matches)
    (implicit deny ip any any: 0 matches)
  total invocations: 0
Extended IP access list 111
  1 permit gre 0.1.1.1 255.0.0.0 any
    (implicit fragment permit: 0 matches)
    (implicit deny ip any any: 0 matches)
  total invocations: 0
Extended IP access list 112
  1 permit ip any any
    (implicit fragment permit: 0 matches)
    (implicit deny ip any any: 0 matches)
  total invocations: 0
Extended IP access list 113
  1 permit gre 0.1.1.1 255.0.0.0 any
    (implicit fragment permit: 0 matches)
    (implicit deny ip any any: 0 matches)
  total invocations: 0
Extended IP access list ext_acl_2
  1 permit gre any any
    (implicit fragment permit: 0 matches)
    (implicit deny ip any any: 0 matches)
  total invocations: 0
Extended IP access list extended_ip_acl
  1 permit tcp any eq 2 any eq exec
    (implicit fragment permit: 0 matches)
    (implicit deny ip any any: 0 matches)
  total invocations: 0

Interface access list references:
PortChannel    2    inbound  extended_ip_acl
PortChannel    2    outbound 101

Application access list references:
snmp-server          standard 2
  UDP ports: none (List Not Defined)
WCCP                  either 10
  Any IP Protocol

```

The following example shows sample output from the **show wccp gre EXEC** command when WCCP access lists are defined on the WAE:

```

WAE# show wccp gre
Transparent GRE packets received:          366
Transparent non-GRE packets received:      0
Transparent non-GRE packets passed through: 0
Total packets accepted:                    337
Invalid packets received:                   0
Packets received with invalid service:      0
Packets received on a disabled service:     0

```

```
Packets received too small: 0
Packets dropped due to zero TTL: 0
Packets dropped due to bad buckets: 0
Packets dropped due to no redirect address: 0
Packets dropped due to loopback redirect: 0
Connections bypassed due to load: 0
Packets sent back to router: 0
Packets sent to another CE: 0
GRE fragments redirected: 0
Packets failed GRE encapsulation: 0
Packets dropped due to invalid fwd method: 0
Packets dropped due to insufficient memory: 0
Packets bypassed, no conn at all: 0
Packets bypassed, no pending connection: 0
Packets due to clean wccp shutdown: 0
Packets bypassed due to bypass-list lookup: 0
Packets received with client IP addresses: 0
Conditionally Accepted connections: 0
Conditionally Bypassed connections: 0
L2 Bypass packets destined for loopback: 0
Packets w/WCCP GRE received too small: 0
Packets dropped due to IP access-list deny: 29
L2 Packets fragmented for bypass: 0
```

Related Commands[\(config\) egress-method](#)[show ip access-list](#)[show wccp](#)

(config) wccp flow-redirect enable

To enable WCCP flow redirection on a WAE, use the **wccp flow-redirect** global configuration command. To disable flow redirection, use the **no** form of this command.

wccp flow-redirect enable

Syntax Description This command has no keywords or arguments.

Defaults Enabled

Command Modes global configuration

Device Modes application-accelerator

Usage Guidelines WCCP flow protection is a mechanism that ensures that no existing flows are broken when a new WAE is brought online or removed from a service group. When transparent traffic interception or redirection first begins, WCCP flow protection ensures that no existing HTTP flows are broken by allowing preexisting, established HTTP flows to continue on. WCCP flow protection also ensures that when a new WAE joins an existing WAE group, existing flows serviced by preexisting WAEs in the cluster continue to receive those existing flows.

The mechanisms used by WCCP flow protection result in all of the benefits of maintaining per flow state information in a centralized location but without the overhead, scaling issues, and redundancy or resiliency issues (for example, asymmetrical traffic flows) associated with keeping per flow state information in the switching layer.

Use the **wccp flow-redirect** global configuration command to implement WCCP flow protection. Flow protection is designed to keep the TCP flow intact as well as to not overwhelm WAEs when they are first started up or are reassigned new traffic. This feature also has a slow start mechanism whereby the WAEs try to take a load appropriate for their capacity.



Note

When bypass is enabled, the client itself tries to reach the origin web server. You must disable all bypass options to eliminate an unnecessary burden on the network.

WCCP works only with IPv4 networks.

Examples The following example shows how to enable WCCP flow protection on a WAE:

```
WAE(config)# wccp flow-redirect enable
```

(config) wccp router-list

To configure a router list for WCCP Version 2, use the **wccp router-list** global configuration command. To disable this function, use the **no** form of this command.

wccp router-list *number ip-address*

Syntax Description

<i>number</i>	Router list number (1–8).
<i>ip-address</i>	IP address of router to add to the list.

Defaults

Disabled

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

As part of configuring a WCCP Version 2 service on a WAE, you must create a list of WCCP Version 2-enabled routers that support the CIFS cache service for the WAE.

Each router list can contain up to eight routers. You can add up to 8 router lists and up to 32 IP addresses per list.



Note

The **ip wccp** global configuration command must be used to enable WCCP on each router that is included on the router list.

WCCP works only with IPv4 networks.

Examples

The following example shows that router list number 7 is created, and contains a single router (the WCCP Version 2-enabled router with IP address 192.168.68.98):

```
WAE(config)# wccp router-list 7 192.168.68.98
```

The following example deletes the router list number 7 created in the previous example:

```
WAE(config)# no wccp router-list 7 192.168.68.98
```

The following example shows how to create a router list (router list 1) and then configure the WAE to accept redirected TCP traffic from the WCCP Version 2-enabled router on router list 1:

```
WAE(config)# wccp router-list 1 10.10.10.2
WAE(config)# wccp tcp-promiscuous router-list 1
WAE(config)# wccp version 2
```

Related Commands

(config) [wccp version](#)

(config) wccp shutdown

To set the maximum time interval after which the WAE will perform a clean shutdown of WCCP, use the **wccp shutdown** global configuration command. To disable the clean shutdown, use the **no** form of the command.

```
wccp shutdown {max-wait seconds}
```

Syntax Description

max-wait	Sets the clean shutdown time interval.
<i>seconds</i>	Time in seconds (0–86400). The default is 120 seconds.

Defaults

The maximum time interval before a clean shutdown is 120 seconds by default.

Command Modes

global configuration

Device Modes

application-accelerator

Usage Guidelines

To prevent broken TCP connections, the WAE performs a clean shutdown of WCCP after a **reload** or **wccp version** command is issued. The WAE does not reboot until either all connections have been serviced or the configured **max-wait** interval has elapsed.

During a clean shutdown, the WAE continues to service the flows it is handling, but starts to bypass new flows. When the number of flows goes down to zero, the WAE takes itself out of the cluster by having its buckets reassigned to other WAEs by the lead WAE. TCP connections can still be broken if the WAE crashes or is rebooted without WCCP being cleanly shut down. The clean shutdown can be aborted while in progress.

You cannot shut down an individual WCCP service on a particular port on a WAE; you must shut down WCCP on the WAE. After WCCP is shut down on the WAE, the WAE preserves its WCCP configuration settings and services proxy-style requests (for example, HTTP requests that the FWAE receives directly from a client browser).



Note

WCCP works only with IPv4 networks.

Examples

The following example shows how to configure the WAE to wait 1000 seconds:

```
WAE(config)# wccp shutdown max-wait 1000
```

The following example shows how to shut down WCCP Version 2 on the WAE by entering the **no wccp version 2** command. In this case, after you enter the **no wccp version 2** command, the WAE waits 1000 seconds before it shuts down WCCP Version 2.

```
WAE(config)# no wccp version 2
```

A countdown message appears, indicating how many seconds remain before WCCP will be shut down on the WAE:

```
Waiting (999 seconds) for WCCP shutdown. Press ^C to skip shutdown
```

The clean shutdown can be aborted while in progress by simultaneously pressing **^C** after the countdown message appears.

Related Commands

[\(config\) wccp flow-redirect enable](#)

[\(config\) wccp version](#)

(config) wccp tcp-promiscuous

To configure the Web Cache Coordination Protocol (WCCP) Version 2 TCP promiscuous mode service (WCCP Version 2 services 61 and 62) on a WAE, use the **wccp tcp-promiscuous** global configuration command.

```
wccp tcp-promiscuous {mask {dst-ip-mask mask | src-ip-mask mask} | router-list-num number
[assign-method-strict | hash-destination-ip | hash-source-ip | l2-redirect | l2-return |
mask-assign | password password | weight weight]}
```

Syntax Description		
mask		Specifies the mask used for WAE assignment.
dst-ip-mask		Specifies the IP address mask defined by a hexadecimal number (for example, 0xFE000000) used to match the packet destination IP address. The range is 0x00000000–0xFE000000. The default is 0x00000000.
src-ip-mask		Specifies the IP address mask defined by a hexadecimal number (for example, 0xFE000000) used to match the packet source IP address. The range is 0x00000000–0xFE000000. The default is 0x00001741.
<i>mask</i>		Mask in hexadecimal (0x00000000–0xFE000000).
router-list-num		Specifies the number of the WCCP router list that should be associated with the TCP promiscuous mode service.
<i>number</i>		Number of the WCCP router list (1–8) that should be associated with the TCP promiscuous mode service. (These WCCP Version 2-enabled routers will transparently redirect TCP traffic to the WAE.)
assign-method-strict		(Optional) Specifies that only the configured assignment method be used.
hash-destination-ip		(Optional) Specifies that the load-balancing hash method should make use of the destination IP address. You can specify both the hash-destination-ip option and the hash-source-ip option.
hash-source-ip		(Optional) Specifies that the load-balancing hash method should make use of the source IP address. This is the default.
l2-redirect		(Optional) Specifies that Layer 2 redirection be used for packet forwarding. If the WAE has a Layer 2 connection with the device, and the device is configured for Layer 2 redirection, Layer 2 redirection permits the WAE to receive transparently redirected traffic from a WCCP Version 2-enabled switch or router.
l2-return		(Optional) Specifies that Layer 2 rewriting be used for packet return.
mask-assign		(Optional) Specifies that the mask method be used for WAE assignment.
password		(Optional) Specifies the password to be used for secure traffic between the WAEs within a cluster and the router for a specified service. Be sure to enable all other WAEs and routers within the cluster with the same password.
<i>password</i>		WCCP service password. Passwords must not exceed 8 characters in length.

weight	(Optional) Specifies that a weight percentage be used. The weight represents a percentage of the total load redirected to the device for load-balancing purposes (for example, a WAE with a weight of 30 receives 30 percent of the total load).
<i>weight</i>	Weight percentage. The weight value ranges from 0 to 100%. By default, weights are not assigned and the traffic load is distributed evenly between the WAEs in a service groups.

Command Modes global configuration

Device Modes application-accelerator

Usage Guidelines WCCP provides the mechanism to transparently redirect client requests to a WAE for processing. To configure basic WCCP, you must enable the WCCP service on the router and the Core WAE in the data center and the router and Edge WAE in the branch office. It is not necessary to configure all of the available WCCP features or services to get a WAE up and running.

This WCCP service requires that WCCP Version 2 is running on the router and the WAE.

The TCP promiscuous mode service is a WCCP service that intercepts all TCP traffic and redirects it to the local WAE.

In order for the WAE to function as a promiscuous TCP device for TCP traffic that is transparently redirected to it by the specified WCCP Version 2 routers, the WAE uses WCCP Version 2 services 61 and 62. The WCCP services 61 and 62 are represented by the canonical name of “tcp-promiscuous” on the WAE in the WAAS CLI.

To configure the egress method for WCCP intercepted connections, use the **egress-method** global configuration command.



Note WCCP works with IPv4 networks only.

Examples The following example shows how to turn on the TCP promiscuous mode service and associate this service with the router list by using the **wccp tcp-promiscuous router-list-num** command:

```
WAE # wccp tcp-promiscuous router-list-num 1
WCCP configuration for TCP Promiscuous service 61 succeeded.
WCCP configuration for TCP Promiscuous succeeded.
Please remember to configure WCCP service 61 and 62 on the corresponding router.
```

Related Commands [\(config\) egress-method](#)
[\(config\) wccp router-list](#)
[show wccp](#)

(config) wccp version

To specify the version of WCCP that the WAE should use, enter the **wccp version** global configuration command. To disable the currently running version, use the **no** form of the command.

```
wccp version {2}
```

Syntax Description	2	Configures the WAE to use WCCP Version 2.
---------------------------	----------	-------------------------------------------

Defaults	No default behavior or values
-----------------	-------------------------------

Command Modes	global configuration
----------------------	----------------------

Device Modes	application-accelerator
---------------------	-------------------------

Usage Guidelines	You must configure a WAE to use WCCP Version 2 instead of WCCP Version 1 because WCCP Version 1 only supports web traffic (port 80).
-------------------------	--------------------------------------------------------------------------------------------------------------------------------------

The WAE performs a clean shutdown after a **reload** or **no wccp version 2** command is entered. A clean shutdown prevents broken TCP connections.

The following sequence of events details the interaction between WAEs and routers that have been configured to run WCCP Version 2:

1. Each WAE is configured with a router list. (See the “(config) wccp router-list” command.)
2. Each WAE announces its presence and a list of all routers with which it has established communications. The routers reply with their view (list) of WAEs in the group.

Routers and WAEs become aware of one another and form a WCCP service group using a management protocol. The WAEs also send periodic “Here I am” messages to the routers that allow the routers to rediscover the WAEs. To properly depict the view, the protocol needs to include the list of routers in the service group as part of its messages.

3. Once the view is consistent across all the WAEs in the WAE cluster, one WAE is designated the lead. When there is a group of WAEs, the one seen by all routers and the one that has the lowest IP address becomes the lead WAE.

The role of this lead WAE is to determine how traffic should be allocated across the WAEs in the WAE group. The lead WAE sets the policy that the WCCP-enabled routers must adhere to when redirecting packets to the WAEs in this cluster. The assignment information is passed to the entire service group from the designated WAE so that the routers in the service group can redirect the packets properly and the WAEs in the service group can better manage their load.



Note

WCCP works only with IPv4 networks.

Examples

The following example shows how to enable WCCP Version 2 on a WAE:

```
WAE(config)# wccp version 2
```

Related Commands

[\(config\) wccp tcp-promiscuous](#)

[\(config\) wccp router-list](#)

(config) windows-domain

To configure Windows domain server options on a WAAS device, use the **windows-domain** global configuration command.

```
windows-domain { administrative group { normal-user | super-user } groupname | comment
                string | netbios-name name | password-server { hostname | ipaddress } | realm kerberos-realm
                | wins-server { hostname | ipaddress } | workgroup name | security ADS }
```

Syntax Description

administrative	Sets administrative options.
group	Sets an administrative group name.
normal-user	Sets the administrative group name for the normal user (privilege 0).
super-user	Sets the administrative group name for the superuser (privilege 15).
<i>groupname</i>	Name of the administrative group.
comment	Specifies a comment for the Windows domain server.
<i>string</i>	Text string.
netbios-name	Specifies the NetBIOS name of the WAE. This is the name provided when the Edge FE announces its availability for print services.
<i>name</i>	NetBIOS name.
password-server	Specifies the password server used to verify a client's password.
<i>hostname</i>	Hostname of the password server.
<i>ipaddress</i>	IP address of the password server.
realm	Specifies the Kerberos realm to use for authentication. The realm is used as the Active Directory Service (ADS) equivalent of the NT4 domain. This argument is valid only when Kerberos ADS mode is used.
<i>kerberos-realm</i>	IP address or name (in UPPERCASE letters) of the Kerberos realm. The Kerberos realm is typically set to the DNS name of the Kerberos server or Active Directory domain. The default value is a NULL string. Example: kerberos-realm = MYBOX.MYCOMPANY.COM
wins-server	Specifies the Windows Internet Naming Service (WINS) server.
<i>hostname</i>	Hostname of the WINS server.
<i>ipaddress</i>	IP address of the WINS server.
workgroup	Specifies the workgroup (or domain) in which the WAAS device resides.
<i>name</i>	Name of the workgroup or domain.
security	Sets Kerberos authentication.
ADS	Specifies the Active Directory Service.

Defaults

Windows domain options are disabled by default.

Command Modes

global configuration

Device Modes

application-accelerator
 replication-accelerator
 central-manager

Usage Guidelines

Use this global configuration command to set the Windows domain server parameters for a WAAS device.

When Kerberos authentication is enabled, the default **realm** is DOMAIN.COM and the **security** is ADS. If Kerberos authentication is disabled, **security** is domain.

Examples

The following example shows how to configure the Windows domain server at *10.10.24.1* for an Edge FE with a NetBIOS name of *myFileEngine* in the *ABD* domain. It also identifies the password server:

```
WAE(config)# windows-domain wins-server 10.10.24.1
WAE(config)# windows-domain password-server 10.10.100.4
WAE(config)# windows-domain netbios-name myFileEngine
WAE(config)# windows-domain workgroup ABC
```

The following example shows how to configure the windows domain server when Kerberos authentication is enabled using the **kerberos** command:

```
WAE(config)# windows-domain realm ABC.COM
WAE(config)# windows security ADS

===== checking new config using testparm =====

Load smb config files from /state/actona/conf/smb.conf
Processing section "[print$]"
Processing section "[printers]"
Loaded services file OK.

WAE(config)# exit
WAE# show windows-domain
  Login Authentication for Console/Telnet Session: enabled

Windows domain Configuration:
-----
  Workgroup:
  Comment: Comment:
  Net BIOS: MYFILEENGINE
  Realm: ABC
  WINS Server: 10.10.10.1
  Password Server: 10.10.10.10
  Security: ADS
```

Related Commands

[\(config\) kerberos](#)
[show windows-domain](#)
[windows-domain](#)

Interface Configuration Mode Commands

Use the interface configuration mode for setting, viewing, and testing the configuration of WAAS 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:

```
WAE# configure
WAE(config)# interface ?
  GigabitEthernet  Select a gigabit ethernet interface to configure
  InlineGroup      Select an inline group interface to configure
  PortChannel       Ethernet Channel of interfaces
  Standby           Standby groups
WAE(config)# interface gigabitethernet ?
  <1-2>/ GigabitEthernet slot/port
WAE(config)# interface gigabitethernet 1/0
WAE(config-if)#
```

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

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

(config-if) autosense

To enable autosense on an interface, use the **autosense** interface configuration command. To disable this function, use the **no** form of this command.

autosense

Syntax Description This command has no arguments or keywords.

Defaults Autosense is enabled by default.

Command Modes interface configuration

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines Cisco router Ethernet interfaces do not negotiate duplex settings. If the WAAS device is connected to a router directly with a crossover cable, the WAAS device interface must be manually set to match the router interface settings. Disable **autosense** before configuring an Ethernet interface. When **autosense** is on, manual configurations are overridden. You must reboot the WAAS device to start autosensing.

Examples The following example disables autosense on Gigabit Ethernet port 1/0:

```
WAE(config)# interface GigabitEthernet 1/0
WAE(config-if)# no autosense
```

The following example reenables autosense on Gigabit Ethernet port 1/0:

```
WAE(config)# interface GigabitEthernet 1/0
WAE(config-if)# autosense
WAE(config-if)# exit
WAE(config)# exit
WAE# reload
```

Related Commands [\(config\) interface](#)
[show interface](#)
[show running-config](#)
[show startup-config](#)

(config-if) bandwidth

To configure the link speed on a network interface, use the **bandwidth** interface configuration command. To restore default values, use the **no** form of this command.

bandwidth { 10 | 100 | 1000 }

Syntax Description	10	Sets the link speed to 10 megabits per second (Mbps).
	100	Sets the link speed to 100 Mbps.
	1000	Sets the link speed to 1000 Mbps. This option is not available on all ports and is the same as autosense.

Defaults No default behaviors or values

Command Modes interface configuration

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines To configure the link speed of a network interface on a WAAS device, use the **bandwidth** interface configuration command. The speed is specified in megabits per second (Mbps). The WAAS software automatically enables autosense if the speed is set to 1000 Mbps.

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

```
WAE(config-if)# bandwidth 10
WAE(config-if)# bandwidth 100
WAE(config-if)# bandwidth 1000
WAE(config-if)# autosense
WAE(config-if)# half-duplex
WAE(config-if)# full-duplex
```



Note

We strongly recommend that you do not use half-duplex connections on the WAE or on routers, switches, or other devices. Use of half-duplex impedes the system's ability to improve performance and should not be used. Double-check each Cisco WAE interface as well as the port configuration on the adjacent device (router, switch, firewall, WAE) to verify that full-duplex is configured.

Examples

The following example shows how to set an interface bandwidth to 1000 Mbps:

```
WAE(config-if)# bandwidth 1000
```

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

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

Related Commands

[\(config-if\) autosense](#)

[\(config\) interface](#)

(config-if) cdp

To enable the Cisco Discovery Protocol (CDP) on a particular interface on a WAAS device, rather than on all interfaces, use the **cdp** command in interface configuration mode.

cdp {enable}

Syntax Description	enable	Enables CDP on an interface.
--------------------	--------	------------------------------

Defaults No default behavior or values

Command Modes interface configuration

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines Using the **cdp enable** command in global configuration mode enables CDP globally on all the interfaces of the WAAS device. If you want to control CDP behavior per interface, then use the **cdp enable** command in interface configuration mode.



Note

Enabling CDP at the interface level overrides the global control. However, you must enable CDP globally on the WAAS device before you enable CDP on an interface. Otherwise, the following message is displayed in the command output:

```
WAE(config-if)# cdp enable
Cannot enable CDP on this interface, CDP Global is disabled
```

Examples The following example enables CDP on Gigabit Ethernet interface (slot 1/port 0) of the WAAS device:

```
WAE# configure
WAE(config)# cdp enable
WAE(config)# enable interface GigabitEthernet 1/0
WAE(config-if)# cdp enable
```

Related Commands

- [\(config\) cdp](#)
- [show cdp](#)
- [show interface](#)
- [show running-config](#)
- [show startup-config](#)

(config-if) exit

To terminate interface configuration mode and return to the global configuration mode, use the **exit** command.

exit

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes All modes

Device Modes application-accelerator
replication-accelerator
central-manager

Examples The following example terminates interface configuration mode and returns to global configuration mode:

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

(config-if) failover timeout

To set the maximum time for the inline interface to transition traffic to another port after a failure event, use the **failover timeout** command. To disable this function, use the **no** form of this command.

failover timeout { 1 | 3 | 5 }

Syntax Description	1	3	5
	Specifies the number of seconds to a failover.	Specifies the number of seconds to a failover.	Specifies the number of seconds to a failover.

Defaults The default is 1 second.

Command Modes interface configuration

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines The **failover timeout** command is used in inlineGroup interface scope. It sets the maximum time (in seconds) for the inline interface to transition to a fail-to-wire mode of operation after a failure event occurs (such as a power outage and kernel crash). For example, if the timeout is set to 3 seconds, traffic is dropped for a maximum of 3 seconds after the WAE loses power or suffers a kernel crash. After this time, all traffic received on either port of the group interface is sent out of the other port in the group. The default timeout is 1 second.

Examples The following example sets the failover time limit for the inline group 0 of the adapter that is installed in slot 1 to 5 seconds and then removes that setting:

```
(config)# interface inlineGroup 1/0
(config-if)# failover timeout 5
(config-if)# no failover timeout 5
```

Related Commands [\(config\) interface](#)
[\(config-if\) inline](#)
[\(config-if\) shutdown](#)

(config-if) full-duplex

To configure an interface for full-duplex operation on a WAAS device, use the **full-duplex** interface configuration command. To disable this function, use the **no** form of this command.

full-duplex

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

interface configuration

Device Modes

application-accelerator
replication-accelerator
central-manager

Usage Guidelines

Use this EXEC command to configure an interface for full-duplex operation. Full duplex allows data to travel in both directions at the same time through an interface or a cable. A half-duplex setting ensures that data only travels in one direction at any given time. Although full duplex is faster, the interfaces sometimes cannot operate effectively in this mode. If you encounter excessive collisions or network errors, configure the interface for half duplex rather than full duplex.



Note

We strongly recommend that you do not use half-duplex connections on the WAE or on routers, switches, or other devices. Use of half-duplex impedes the system's ability to improve performance and should not be used. Double-check each Cisco WAE interface as well as the port configuration on the adjacent device (router, switch, firewall, WAE) to verify that full-duplex is configured.

Examples

The following example configures full-duplex operation on a Gigabit Ethernet interface in slot 1/port 0:

```
WAE# configure  
WAE(config)# interface GigabitEthernet 1/0  
WAE(config-if)# full-duplex
```

The following example disables full-duplex operation:

```
WAE(config-if)# no full-duplex
```

Related Commands

[\(config-if\) half-duplex](#)
[\(config\) interface](#)
[show interface](#)

show running-config
show startup-config

(config-if) half-duplex

To configure an interface for half-duplex operation on a WAAS device, use the **half-duplex** interface configuration command. To disable this function, use the **no** form of this command.

half-duplex

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

interface configuration

Device Modes

application-accelerator
replication-accelerator
central-manager

Usage Guidelines

Use this interface configuration command to configure an interface for half-duplex operation. Full duplex allows data to travel in both directions at the same time through an interface or a cable. A half-duplex setting ensures that data only travels in one direction at any given time. Although full duplex is faster, the interfaces sometimes cannot operate effectively in this mode. If you encounter excessive collisions or network errors, configure the interface for half duplex rather than full duplex.

**Note**

We strongly recommend that you do not use half-duplex connections on the WAE or on routers, switches, or other devices. Use of half-duplex impedes the system's ability to improve performance and should not be used. Double-check each Cisco WAE interface as well as the port configuration on the adjacent device (router, switch, firewall, WAE) to verify that full-duplex is configured.

Examples

The following example configures half-duplex operation on the Gigabit Ethernet interface in slot 1/port 0:

```
WAE# configure  
WAE(config)# interface GigabitEthernet 1/0  
WAE(config-if)# half-duplex
```

The following example disables half-duplex operation:

```
WAE(config-if)# no half-duplex
```

Related Commands

[\(config-if\) full-duplex](#)
[\(config\) interface](#)

`show interface`
`show running-config`
`show startup-config`

(config-if) inline

To enable inline interception for an inlineGroup interface, use the **inline** interface configuration command. To disable inline interception, use the **no** form of this command.

```
inline [vlan {all | native | vlan_list}]
```

Syntax Description	
vlan	(Optional) Modifies the VLAN list parameters.
all	Applies the command to all tagged and untagged packets.
native	Specifies untagged packets.
<i>vlan_list</i>	List of VLAN IDs to either allow or restrict on this interface. A comma (,) is used to separate list entries. A hyphen (-) is used to specify a range of VLAN IDs. The valid range is 0 to 4095.

Defaults The default is enabled for all VLANs if you have a WAE inline network adapter installed.

Command Modes interface configuration

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines The **inline** command is used in inlineGroup interface scope. It enables or disables inline interception. If the VLAN list is omitted, the command applies to all VLAN tagged or untagged packets. You can restrict the inline feature to any specified set of VLANs.

The VLAN list can be “all” or a comma-separated list of VLAN IDs or ranges of VLAN IDs. The special VLAN ID “native” can be included to specify untagged packets.



Note When inline inspection is active, you cannot configure WCCP until you explicitly disable the inline capability on all VLANs. Conversely, you cannot enable inline interception on any inline groups until you disable WCCP.

Examples The following example shows how to enable inline interception for all untagged and tagged packets with any VLAN ID received on ports in inlineGroup 0 of the adapter that is installed in slot 1:

```
(config)# interface inlineGroup 1/0
(config-if)# inline
(config-if)# exit
```

The following example shows how to disable inline interception on the same ports for 802.1Q-encapsulated packets that have the VLAN ID 5 or any VLAN ID between 10 and 15, inclusive. If the two VLANs are combined in the given order, inline interception is performed for all packets received on ports in group 0 of slot 1, except those on VLANs 5, 10, 11, 12, 13, 14 and 15.

```
(config)# interface inlineGroup 1/0  
(config-if)# no inline vlan 5,10-15  
(config-if)# exit
```

The following example shows how to enable inline interception for all untagged traffic and traffic only on VLANs 0 through 100 on the ports in group 1 in slot 2:

```
(config)# interface inlineGroup 2/1  
(config-if)# no inline vlan 101-4095  
(config-if)# exit
```

The following example shows how to enable inline interception for traffic only on VLAN 395 on the ports in group 1 in slot 2. Because the default behavior is to enable traffic on all VLANs, you must first disable all VLANs, then enable just the set that you want.

```
(config)# interface inlineGroup 2/1  
(config-if)# no inline vlan all  
(config-if)# inline vlan 395  
(config-if)# exit
```

Related Commands [show interface](#)

(config-if) ip

To configure the IP address or subnet mask, or to negotiate an IP address from DHCP on the interface of the WAAS device, use the **ip** interface configuration command. To disable this function, use the **no** form of this command.

```
ip address { ip-address ip-subnet [secondary] | dhcp [client-id id [hostname name] | hostname name [client-id id]] }
```

Syntax Description	Field	Description
	address	Sets the IP address of an interface.
	<i>ip-address</i>	IP address.
	<i>ip-subnet</i>	IP subnet mask.
	secondary	(Optional) Makes this IP address a secondary address.
	dhcp	Sets the IP address negotiated over DHCP.
	client-id	(Optional) Specifies client identifier.
	<i>id</i>	Client identifier.
	hostname	(Optional) Specifies the hostname.
	<i>name</i>	Hostname.

Defaults No default behavior or values

Command Modes interface configuration

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines Use this command to set or change the IP address, subnet mask, or DHCP IP address negotiation of the network interfaces of the WAAS device. The change in the IP address takes place immediately.

The **ip address** interface configuration command allows configuration of secondary IP addresses for a specified interface as follows.

```
WAE(config-if)# ip address ip_address netmask [secondary]
```

Up to four secondary IP addresses can be specified for each interface. The same IP address cannot be assigned to more than one interface. The secondary IP address becomes active only after a primary IP address is configured. The following command configures the primary IP address.

```
WAE(config-if)# ip address ip_address netmask
```

The secondary IP addresses are disabled when the interface is shut down, and are enabled when the interface is brought up.

Use the **no** form of the command to disable a specific IP address.

```
WAE(config-if)# no ip address ip_address netmask
```

**Note**

No two interfaces can have IP addresses in the same subnet.

Use the **ip-address dhcp** command to negotiate a reusable IP address from DHCP.

Examples

The following example shows how to configure the port channel interface with an IP address of 10.10.10.10 and a netmask of 255.0.0.0:

```
WAE# configure
WAE(config)# interface PortChannel 2
WAE(config-if)# ip address 10.10.10.10 255.0.0.0
```

The following example deletes the IP address configured on the interface:

```
WAE(config-if)# no ip address
```

The following example enables an interface for DHCP:

```
WAE(config-if)# ip address dhcp
```

The following example configures a client identifier and hostname on the WAAS device to be sent to the DHCP server:

```
WAE(config-if)# ip address dhcp client-id myclient hostname myhost
```

Related Commands

[\(config\) interface](#)

[show interface](#)

[show running-config](#)

[show startup-config](#)

(config-if) ip access-group

To control connections on a specific interface of a WAAS device by applying a predefined access list, use the **ip access-group** interface configuration command. To disable an access list, use the **no** form of the command.

```
ip access-group {acl-name | acl-num} {in | out}
```

Syntax Description		
<i>acl-name</i>		Alphanumeric identifier of up to 30 characters, beginning with a letter that identifies the ACL to apply to the current interface.
<i>acl-num</i>		Numeric identifier that identifies the access list to apply to the current interface. For standard access lists, the valid range is 1 to 99; for extended access lists, the valid range is 100 to 199.
in		Applies the specified access list to inbound packets on the current interface.
out		Applies the specified access list to outbound packets on the current interface.

Defaults No default behavior or values

Command Modes interface configuration

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines Use the **ip access-group** interface configuration command to activate an access list on a particular interface. You can use one outbound access list and one inbound access list on each interface. Before entering the **ip access-group** command, enter interface configuration mode for the interface to which you want to apply the access list. Define the access list to apply using the **ip access-list** command.

Examples The following example shows how to apply the access list named *acl-out* to outbound traffic on the interface Gigabit Ethernet 1/2:

```
WAE(config)# interface GigabitEthernet 1/2
WAE(config-if)# ip access-group acl-out out
```

Related Commands [clear](#)
[\(config\) ip access-list](#)
[show ip access-list](#)

■ (config-if) ip access-group

(config-if) mtu

To set the interface Maximum Transmission Unit (MTU) packet size, use the **mtu** interface configuration command. Use the **no** form of this command to reset the MTU packet size.

mtu *mtusize*

Syntax Description	<i>mtusize</i> MTU packet size in bytes (88–1500).
Defaults	No default behavior or values
Command Modes	interface configuration
Device Modes	application-accelerator replication-accelerator central-manager
Usage Guidelines	The MTU is the largest size of IP datagram that can be transferred using a specific data link connection. Use the mtu command to set the maximum packet size in bytes.
Examples	The following example sets the MTU to 1500 bytes, and then removes that setting: <pre>WAE(config-if)# mtu 1500 WAE(config-if)# no mtu 1500</pre>
Related Commands	show interface show running-config show startup-config

(config-if) no

To negate a Gigabit Ethernet interface configuration command or set its defaults, use the following **no** command from GigabitEthernet interface configuration mode.

```
no [autosense | bandwidth {10 | 100 | 1000} | cdp enable | channel-group {1 | 2} | description
text | full-duplex | half-duplex | ip {access-group {acl-num | acl_name} {in | out} | address
{ip_address netmask [secondary] | dhcp [client-id id hostname name | hostname name
client-id id}} | mtu mtusize | shutdown | standby grpnumber [priority priority]]
```

To negate an InlineGroup interface configuration command or set its defaults, use the following **no** commands from the InlineGroup interface configuration mode.

```
no [autosense | bandwidth {10 | 100 | 1000} | failover timeout {1 | 3 | 5} | full-duplex | half-duplex
| inline [vlan {all | native | vlan_list}] | shutdown]
```

To negate a PortChannel interface configuration command or set its defaults, use the following **no** commands from the Port Channel interface configuration mode.

```
no [description text | ip {access-group {acl-num | acl_name} {in | out} | address ip-address
netmask} | shutdown]
```

Syntax Description

The command options vary. For more information on the syntax description, see the [“\(config\) interface”](#) command.

Command Defaults

No default behavior or values

Command Modes

interface configuration

Device Modes

application-accelerator
 replication-accelerator
 central-manager

Usage Guidelines

The command options **for** the no interface configuration command vary depending on the current interface configuration mode. For example, if you are in Gigabit interface configuration mode, there are 11 options for the **no** command.

```
WAE(config)# interface GigabitEthernet 2/0
WAE(config-if)# no ?
  autosense      Interface autosense
  bandwidth      Interface bandwidth
  cdp            Cisco Discovery Protocol Interface Config commands
  channel-group  Configure EtherChannel group
  description    Interface specific description
  full-duplex    Interface fullduplex
  half-duplex    Interface halfduplex
  ip            Interface Internet Protocol Config commands
```



```
mtu          Set the interface Maximum Transmission Unit (MTU)
shutdown     Shutdown the specific interface
standby      Standby interface config commands
WAE(config-if)# no
```

However, if you are in Standby interface configuration mode, there are only 4 options for the **no** command:

```
WAE(config)# interface standby 4
WAE(config-if)# no ?
description  Standby interface description
errors       Set the maximum number of errors allowed on this interface
ip           Set the IP address of a standby group
shutdown     Shutdown this interface
WAE(config-if)# no
```

Examples

The following example configures the Gigabit Ethernet interface in slot 2, port 0 not to autosense the interface bandwidth:

```
WAE(config)# interface GigabitEthernet 2/0
WAE(config-if)# no autosense
```

Related Commands

[\(config\) interface](#)
[show interface](#)
[show running-config](#)
[show startup-config](#)

(config-if) shutdown

To shut down a specific hardware interface on a WAAS device, use the **shutdown** interface configuration command. To restore an interface to operation, use the **no** form of this command.

shutdown

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes interface configuration

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines See the “(config) interface” command for alternative syntax.

Examples The following example shuts down a Gigabit Ethernet interface on the WAAS device:

```
WAE# configure
WAE(config)# interface GigabitEthernet 2/0
WAE(config-if)# shutdown
```

Related Commands [\(config\) interface](#)
[show interface](#)
[show running-config](#)
[show startup-config](#)

(config-if) standby

To configure an interface on a WAAS device to be a backup for another interface, use the **standby** command in interface configuration mode. Use the **no** form of the command to restore the default configuration of the interface.

```
standby group_number { description text | errors max-errors | ip ip-address netmask | priority
priority_level | shutdown }
```

Syntax	Description
<i>group_number</i>	Standby group number (1–4).
description	(Optional) Sets the description for the specified interface.
<i>text</i>	Description for the specified interface. The maximum length of the description text is 240 characters.
errors	Sets the maximum number of errors allowed on the active interface before the interface is shut down and the standby interface is brought up. This option is disabled by default.
<i>max-errors</i>	Maximum number of errors (0–4294967295).
ip	Sets the IP address for the specified standby group (Standby Group 1, 2, 3, or 4).
<i>ip-address</i>	IP address of the specified standby group (Standby Group 1, 2, 3, or 4). The group IP address and netmask of a standby group must be configured on all of the member interfaces.
<i>netmask</i>	Netmask of the specified standby group (Standby Group 1, 2, 3, or 4).
priority	Sets the priority of the member interface within a standby group. The priority of a member interface can be changed at runtime. The member interface that has the highest priority after this change becomes the new active interface (the default action is to preempt the currently active interface if an interface with higher priority exists).
<i>priority_level</i>	Each member interface is assigned a priority number. The member interface with the highest priority number is the active interface for that standby group. Only the active interface uses the group IP address. If the priority option is specified without a priority number, the default value of 100 is used.
shutdown	(Optional) Shuts down the specified standby group (Standby Group 1, 2, 3, or 4). You can shut down a standby group even if you have not configured a group IP address for the standby group. Note When a standby group is shut down, all of the alarms previously raised by this standby group are cleared.

Defaults

There are no standby interfaces by default. The **errors** option is disabled by default.

Command Modes

interface configuration

Device Modes

application-accelerator
 replication-accelerator
 central-manager

Usage Guidelines

You can configure one or more interfaces to act as a backup interface (a standby interface) for another interface on a WAAS device. This feature is called “standby interface support.” Standby groups, which are logical groups of interfaces, are used to implement this feature. When an active network interface fails (because of cable trouble, Layer 2 switch failure, high error count, or other failures) and that interface is part of a standby group, a standby interface can become active and take the load off the failed interface.

There must be at least two interfaces in a standby group. Interfaces that are part of a standby group are called “member interfaces.” After you create a standby group, you define which interfaces should be assigned to this logical group. As part of defining the member interfaces, you specify the priority of each member interface in a standby group. The member interface with the highest assigned priority is the active interface for that particular standby group. If the active interface fails, the operational member interface with the next highest priority in the standby group comes up, and so forth. If all member interfaces of a particular standby group are down and then one of the member interfaces comes up, the WAAS software detects this situation and brings up the standby group on the member interface that just came up.

The failure or failover of member interfaces within a standby group triggers alarms and traps (if alarms and traps are enabled on the WAAS device). Alarms are sent out when failover occurs between member interfaces in a standby group. Specifically, minor alarms are sent out when member interfaces fail, and these alarms are cleared automatically when the interface failover has been successfully completed. Major alarms are sent out if the standby group goes down (that is, no member interface in a standby group can be brought up.)

**Note**

A physical interface can belong to more than one standby group. Consequently, a single interface can act as a standby interface for more than one standby group.

To configure standby interfaces, interfaces are logically assigned to standby groups. The following rules define the standby group relationships:

- Each standby group is assigned a unique standby IP address, shared by all member interfaces of the standby group. The IP address of the standby group is shared among the member interfaces; however, only the active interface of the standby group uses this shared IP address at any one time. This shared IP address is configured as an alias on the active interface.
- Configure the duplex and speed settings of the member interfaces for better reliability.
- If all the member interfaces of a standby group fail and then one recovers, the WAAS software brings up the standby group on the operational member interface.
- If a physical interface is a member of a port channel group, it cannot join a standby group. Likewise, if a physical interface is a member of a standby group, it cannot join a port channel group.
- A standby group comprises two or more interfaces.
- The maximum number of standby groups on a WAAS device is four.

**Note**

Interface IP addresses and standby group IP addresses must be on different subnets to ensure reliable operation. You can use dummy IP addresses in the private address space to serve as interface primary IP addresses, and use the real WAAS device's IP address to serve as the standby group IP address in a different subnet to satisfy this requirement. When dummy IP addresses are used, these interface IP addresses serve only as substitutes to bring up the interface. For example, the WAAS device's interface requires an IP address on an interface for initialization. Make sure to configure the interface default gateway using the **ip default-gateway** global configuration command instead of the **ip route** command.

- Each interface in a standby group is assigned a priority. The operational interface with the highest priority in a standby group is the active interface. Only the active interface uses the group IP address.
- The priority of an interface in a standby group can be changed at runtime. The member interface that has the highest priority after this change becomes the new active interface (the default action is to preempt the currently active interface if an interface with higher priority exists).
- The maximum number of errors allowed on the active interface before the interface is shut down and the standby is brought up is configured with the **errors** option, which is disabled by default.

**Tip**

If an interface belongs to more than one standby group, you can configure the interface with a different priority in each standby group for better load-balancing. For example, interfaces Gigabit Ethernet 1/0 and Gigabit Ethernet 2/0 are both in standby group 1 and in standby group 2. If you configure Gigabit Ethernet 1/0 with the highest priority in standby group 1 and configure Gigabit Ethernet 2/0 with the highest priority in standby group 2, standby group 1 uses Gigabit Ethernet 1/0 as the active interface, while standby group 2 uses Gigabit Ethernet 2/0 as the active interface. This configuration allows each interface to back up the other one, if one of them fails.

**Note**

Unlike port channels, standby groups do not support IP ACLs at a group level. However, you can configure a member interface of a standby group to support an IP ACL at the interface level. For example, you can individually configure the two member interfaces of Standby Group 1 (the Gigabit Ethernet slot 1/port 0 interface and the Gigabit Ethernet slot 2/port 0 interface) to support an IP ACL named ACL1, but you cannot configure the Standby Group 1 to support ACL1.

Examples

The following example configures two Gigabit Ethernet interfaces to be part of the same standby group, with interface 1/0 as the active interface:

```
WAE(config-if)# interface gigabitEthernet 1/0 standby 1 ip 10.16.10.10 255.255.254.0
WAE(config-if)# interface gigabitEthernet 2/0 standby 1 ip 10.16.10.10 255.255.254.0
WAE(config-if)# interface gigabitEthernet 1/0 standby 1 priority 300
WAE(config-if)# interface gigabitEthernet 2/0 standby 1 priority 200
WAE(config-if)# interface gigabitEthernet 1/0 standby 1 errors 10000
WAE(config-if)# interface gigabitEthernet 2/0 standby 1 errors 10000
```

The following example displays information about the standby group configuration by entering the **show standby EXEC** command. In the following sample command output, one standby group (Standby Group 1) is configured on this WAAS device. The command output also shows which member interface is the active interface. In this case, the active interface is the Gigabit Ethernet slot 1/port 0 interface.

```
WAE# show standby
Standby Group: 1
  Description: This a backup for Gigabit Ethernet 2/0.
  IP address: 10.16.10.10, netmask: 255.0.0.0
```

```
Member interfaces: none
Active interface: Gigabit Ethernet 1/0
Maximum errors allowed on the active interface: 500
```



Note To display information about a specific standby group configuration, enter the **show interface standby group_number EXEC** command.

The following example creates a standby group, Standby Group 1:

```
WAE# configure
WAE(config)# interface standby 1
WAE(config-if)#
```

The following example assigns a group IP address of 10.10.10.10 and a netmask of 255.0.0.0 to Standby Group 1. You can configure a group IP address regardless of whether the standby group is shut down or not.

```
WAE(config-if)# ip address 10.10.10.10 255.0.0.0
WAE(config-if)# errors 500
```

The following example shows how to add two Gigabit Ethernet interfaces to Standby Group 1 and then assign each of these member interfaces a priority within the group:

- a. First a Gigabit Ethernet interface (slot 1/port 0) is added to Standby Group 1 and assigned a priority of 150.

```
WAE(config)# interface gigabitEthernet 1/0
WAE(config-if)# standby 1 priority 150
```

- b. Next, a second Gigabit Ethernet interface (slot 2/port 0) is added to Standby Group 1 and assigned a priority of 100 (the default value).

```
WAE(config)# interface gigabitEthernet 2/0
WAE(config-if)# standby 1
WAE(config-if)# exit
WAE(config)#
```

Because GigabitEthernet 0/0 is assigned the highest priority (a priority number of 150) of all the member interfaces in the group, it is chosen as the active interface for the group if it can be brought up.

The following example removes the GigabitEthernet slot 1/port 0 interface from Standby Group 1 using the **no** form of the **standby** command:

```
WAE(config)# interface gigabitEthernet 1/0
WAE(config-if)# no standby 1
WAE(config-if)# exit
WAE(config)#
```

The following example shows how to shut down Standby Group 1. When a standby group is shut down, all of the alarms previously raised by this standby group are cleared:

```
WAE(config)# interface standby 1
WAE(config-if)# exit
WAE(config)# exit
```

The following example shows how to tear down Standby Group 1:

```
WAE(config)# interface standby 1
WAE(config-if)# no ip address 10.10.10.10 255.0.0.0
Please remove member interface(s) from this standby group first.
WAE(config)# interface GigabitEthernet 2/0
WAE(config-if)# no standby 1
```

```
WAE(config-if)# exit
WAE(config)# interface standby 1
WAE(config-if)# no ip address 10.10.10.10 255.0.0.0
WAE(config-if)# exit
WAE(config)# no interface standby 1
WAE(config)# exit
```

Related Commands

[\(config\) interface](#)

[show interface](#)

[show running-config](#)

[show standby](#)

[show startup-config](#)

Standard ACL Configuration Mode Commands

From global configuration mode, you can enter the standard and extended ACL configuration modes.

- 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 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 exit an ACL configuration mode, enter **exit** to return to global configuration mode:

```
WAE(config-std-nacl)# exit  
WAE(config)#
```

To return to global configuration mode, enter the **exit** command.

(config) ip access-list standard

To create and modify standard access lists on a WAAS device for controlling access to interfaces or applications, use the **ip access-list standard** global configuration command. To disable a standard access list, use the **no** form of the command.

```
ip access-list standard {acl-name | acl-num}
```

Syntax Description	standard	Enables standard ACL configuration mode. The CLI enters the standard ACL configuration mode in which all subsequent commands apply to the current standard access list. The (config-std-nacl) prompt appears: WAE(config-std-nacl)#
	<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.
	<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.

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

Command Modes Global configuration

Device Modes application-accelerator
replication-accelerator
central-manager

Usage Guidelines Use access lists to control access to specific applications or interfaces on a WAAS device. An access control list consists of one or more condition entries that specify the kind of packets that the WAAS device will drop or accept for further processing. The WAAS device 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.



Note

IP ACLs that are defined on a router take precedence over the IP ACLs that are defined on the WAE. IP ACLs that are defined on a WAE take precedence over the WAAS application definition policies that are defined on the WAE.

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 will be 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 WAAS device 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. Therefore, 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 create a standard access list, enter the **ip access-list standard** 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.

**Note**

You must use a standard access list for providing access to the SNMP server or to the TFTP gateway/server. However, you can use either a standard access list or an extended access list for providing access to the WCCP application.

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 host 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.

After you identify the standard access list, the CLI enters the standard ACL configuration mode and all subsequent commands apply to the specified access list.

```
WAE(config)# ip access-list standard teststdacl
WAE(config-std-nacl)# exit
```

Examples

The following example creates a standard access list on the WAAS device that permits any packets from source IP address 192.168.1.0 for further processing:

```
WAE(config)# ip access-list standard teststdacl
WAE(config-std-nacl)# permit 192.168.1.0 any
WAE(config-std-nacl)# exit
```

The following commands activate the access list for an interface:

```
WAE(config)# interface gigabitethernet 1/0
WAE(config-if)# ip access-group teststdacl in
WAE(config-if)# exit
```

The following example shows how this configuration appears when you enter the **show running-configuration** command:

```
...
!
interface GigabitEthernet 1/0
 ip address 10.1.1.50 255.255.0.0
 ip access-group teststdacl in
 exit
```

```
. . .  
ip access-list standard teststdacl  
  permit 192.168.1.0 any  
  exit  
. . .
```

Related Commands

clear
show ip access-list
(config-if) ip access-group
(config-std-nacl) deny
(config-std-nacl) delete
(config-std-nacl) list
(config-std-nacl) move
(config-std-nacl) permit

(config-std-nacl) delete

To delete a line from the standard IP ACL, use the **delete** command.

delete *line-num*

Syntax Description	<i>line-num</i>	Entry at a specific line number in the access list.
--------------------	-----------------	-----------------------------------------------------

Command Modes	Standard ACL configuration mode
---------------	---------------------------------

Device Modes	application-accelerator replication-accelerator central-manager
--------------	-----------------------------------------------------------------------

Examples	The following example deletes line 10 from the standard IP ACL teststdacl:
----------	----------------------------------------------------------------------------

```
WAE(config)# ip access-list standard teststdacl
WAE(config-std-nacl)# delete 10
```

Related Commands	(config-std-nacl) deny (config-std-nacl) delete (config-std-nacl) list (config-std-nacl) move (config-std-nacl) permit
------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

(config-std-nacl) deny

To add a line to a standard access-list that specifies the type of packets that you want the WAAS device to drop, use the **deny** command.

```
[insert line-num] deny {source-ip [wildcard] | host source-ip | any}
```

To negate a standard IP ACL, use the following syntax.

```
no deny {source-ip [wildcard] | host source-ip | any}
```

Syntax Description		
insert	(Optional) Inserts the conditions following the specified line number into the access list.	
<i>line-num</i>	Entry at a specific line number in the access list.	
deny	Causes packets that match the specified conditions to be dropped.	
<i>source-ip</i>	Source IP address. The number of the network or host from which the packet is being sent, specified as a 32-bit quantity in 4-part dotted-decimal format (for example, 0.0.0.0).	
<i>wildcard</i>	(Optional) Portions of the preceding IP address to match, expressed using 4-digit, dotted-decimal notation. Bits to match are identified by a digital value of 0; bits to ignore are identified by a 1.	
	Note For standard IP ACLs, the <i>wildcard</i> parameter of the ip access-list command is always optional. If the host keyword is specified for a standard IP ACL, then the <i>wildcard</i> parameter is not allowed.	
host	Matches the following IP address.	
any	Matches any IP address.	

Defaults

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

Command Modes

Standard ACL configuration mode

Device Modes

application-accelerator
 replication-accelerator
 central-manager

Usage Guidelines

To create an entry, use a **deny** or **permit** keyword and specify the type of packets that you want the WAAS device 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. Therefore, you must include at least one **permit** entry to create a valid access list.

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 host** *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.

Examples

The following example creates standard access-list that denies any packets from source IP address 192.168.1.0 for processing:

```
WAE(config)# ip access-list standard teststdacl
WAE(config-std-nacl)# deny 192.168.1.0 any
WAE(config-std-nacl)# exit
```

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

```
WAE(config)# interface gigabitethernet 1/0
WAE(config-if)# ip access-group teststdacl in
WAE(config-if)# exit
```

The following example shows how this configuration appears when you enter the **show running-configuration** command:

```
...
!
interface GigabitEthernet 1/0
 ip address 10.1.1.50 255.255.0.0
 ip access-group teststdacl in
 exit
...
ip access-list standard example
 deny 192.168.1.0 any
 exit
...

```

Related Commands

- [\(config-std-nacl\) delete](#)
- [\(config-std-nacl\) list](#)
- [\(config-std-nacl\) move](#)
- [\(config-std-nacl\) permit](#)

(config-std-nacl) exit

To terminate standard ACL configuration mode and return to the global configuration mode, use the **exit** command.

exit

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes All modes

Device Modes application-accelerator
replication-accelerator
central-manager

Examples The following example terminates standard ACL configuration mode and returns to global configuration mode:

```
WAE(config-std-nacl)# exit  
WAE(config)#
```

(config-std-nacl) list

To display a list of specified entries within the standard IP ACL, use the **list** command.

list [*start-line-num* [*end-line-num*]]

Syntax	Description
<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.

Command Modes Standard ACL configuration mode

Device Modes application-accelerator
replication-accelerator
central-manager

Examples The following example displays a list of specified entries within the standard IP ACL:

```
WAE(config)# ip access-list standard teststdacl
WAE(config-std-nacl)# list 25 50
```

Related Commands [\(config-std-nacl\) delete](#)
[\(config-std-nacl\) move](#)

(config-std-nacl) move

To move a line to a new position within the standard IP ACL, use the **move** command.

```
move old-line-num new-line-num
```

Syntax Description	<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.

Command Modes Standard ACL configuration mode

Device Modes application-accelerator
replication-accelerator
central-manager

Examples The following example moves a line to a new position within the standard IP ACL:

```
WAE(config)# ip access-list standard teststdacl  
WAE(config-std-nacl)# move 25 30
```

Related Commands [\(config-std-nacl\) delete](#)
[\(config-std-nacl\) list](#)

(config-std-nacl) permit

To add a line to a standard access-list that specifies the type of packets that you want the WAAS device to accept for further processing, use the **permit** command.

```
[insert line-num] permit {source-ip [wildcard] | host source-ip | any}
```

To negate a standard IP ACL, use the following syntax.

```
no permit {source-ip [wildcard] | host source-ip | any}
```

Syntax Description		
insert	(Optional) Inserts the conditions following the specified line number into the access list.	
<i>line-num</i>	Entry at a specific line number in the access list.	
<i>source-ip</i>	Source IP address. The number of the network or host from which the packet is being sent, specified as a 32-bit quantity in 4-part dotted-decimal format (for example, 0.0.0.0).	
<i>wildcard</i>	(Optional) Portions of the preceding IP address to match, expressed using 4-digit, dotted-decimal notation. Bits to match are identified by a digital value of 0; bits to ignore are identified by a 1.	
	Note For standard IP ACLs, the <i>wildcard</i> parameter of the ip access-list command is always optional. If the host keyword is specified for a standard IP ACL, then the <i>wildcard</i> parameter is not allowed.	
host	Matches the following IP address.	
any	Matches any IP address.	

Defaults

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

Command Modes

Standard ACL configuration mode

Device Modes

application-accelerator
 replication-accelerator
 central-manager

Usage Guidelines

To create an entry, use a **deny** or **permit** keyword and specify the type of packets that you want the WAAS device 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. Therefore, you must include at least one **permit** entry to create a valid access list.

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 host** *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.

Examples

The following example creates standard access-list that permits any packets from source IP address 192.168.1.0 for further processing:

```
WAE(config)# ip access-list standard teststdacl
WAE(config-std-nacl)# permit 192.168.1.0 any
WAE(config-std-nacl)# exit
```

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

```
WAE(config)# interface gigabitEthernet 1/0
WAE(config-if)# ip access-group teststdacl in
WAE(config-if)# exit
```

The following example shows how this configuration appears when you enter the **show running-configuration** command:

```
...
!
interface GigabitEthernet 1/0
 ip address 10.1.1.50 255.255.0.0
 ip access-group teststdacl in
 exit
...
ip access-list standard example
 permit 192.168.1.0 any
 exit
...

```

Related Commands

[\(config-std-nacl\) delete](#)
[\(config-std-nacl\) deny](#)
[\(config-std-nacl\) list](#)
[\(config-std-nacl\) move](#)

Extended ACL Configuration Mode Commands

To create and modify extended access lists on a WAAS device for controlling access to interfaces or applications, use the **ip access-list extended** global configuration command. To disable an extended access list, use the **no** form of the command.

```
ip access-list extended {acl-name | acl-num}
```

Syntax Description

extended	Enables extended ACL configuration mode. The CLI enters the extended ACL configuration mode in which all subsequent commands apply to the current extended access list. The (config-ext-nacl) prompt appears: WAE(config-ext-nacl)#
<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.
<i>acl-num</i>	Access list to which all commands entered from access list configuration mode apply, using a numeric identifier. For extended access lists, the valid range is 100 to 199.

Defaults

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

Command Modes

Global configuration

Device Modes

application-accelerator
replication-accelerator
central-manager

Usage Guidelines

Use access lists to control access to specific applications or interfaces on a WAAS device. An access control list consists of one or more condition entries that specify the kind of packets that the WAAS device will drop or accept for further processing. The WAAS device 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 list contains examples of how ACLs can be used in environments that use WAAS devices:

- A WAAS device 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.
- A WAAS device is deployed anywhere within the enterprise. As with routers and switches, the administrator wants to limit Telnet, SSH, and WAAS GUI access to the IT source subnets.

- An application layer proxy firewall with a hardened outside interface has no ports exposed. (*Hardened* means that the interface carefully restricts which ports are available for access, primarily for security reasons. With an outside interface, many types of security attacks are possible.) The WAE's outside address is Internet global, and its inside address is private. The inside interface has an ACL to limit Telnet, SSH, and WAAS GUI access to the device.
- A WAAS device using WCCP is positioned between a firewall and an Internet router or a subnet off the Internet router. Both the WAAS device and the router must have ACLs.

**Note**

ACLs that are defined on a router take precedence over the ACLs that are defined on the WAE. ACLs that are defined on a WAE take precedence over the WAAS application definition policies that are defined on the WAE.

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 will be 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 WAAS device 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. Therefore, 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 create an extended access list, enter the **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 an extended access list, it must be from 100 to 199

**Note**

You must use a standard access list for providing access to the SNMP server or to the TFTP gateway/server. However, you can use either a standard access list or an extended access list for providing access to the WCCP application.

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 host 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.

After you identify the extended access list, the CLI enters the extended ACL configuration mode and all subsequent commands apply to the specified access list.

```
WAE(config)# ip access-list extended testextacl
WAE(config-ext-nacl)#
```

Examples

The following example shows how to create an access list on the WAAS device. You create this access list to allow the WAAS device to accept all web traffic that is redirected to it, but limits host administrative access using SSH:

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

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

```
WAE(config)# interface gigabitethernet 1/0
WAE(config-if)# ip access-group testextacl in
WAE(config-if)# exit
```

The following example shows how this configuration appears when you enter the **show running-configuration** command:

```
...
!
interface GigabitEthernet 1/0
 ip address 10.1.1.50 255.255.0.0
 ip access-group testextacl in
 exit
...
ip access-list extended testextacl
 permit tcp any any eq www
 permit tcp host 10.1.1.5 any eq ssh
 exit
...

```

Related Commands

clear
show ip access-list
(config-if) ip access-group
(config-ext-nacl) deny
(config-ext-nacl) delete
(config-ext-nacl) list
(config-ext-nacl) move
(config-ext-nacl) permit

(config-ext-nacl) delete

To delete a line from the extended ACL, use the **delete** command.

delete *line-num*

Syntax Description	<i>line-num</i>	Entry at a specific line number in the access list.
---------------------------	-----------------	-----------------------------------------------------

Command Modes	Extended ACL configuration mode
----------------------	---------------------------------

Device Modes	application-accelerator replication-accelerator central-manager
---------------------	-----------------------------------------------------------------------

Examples	The following example deletes line 10 from the extended ACL testextacl:
-----------------	-------------------------------------------------------------------------

```
WAE(config)# ip access-list extended testextacl
WAE(config-ext-nacl)# delete 10
```

Related Commands	(config-ext-nacl) list (config-ext-nacl) move
-------------------------	----------------------------------------------------------------------------------

(config-ext-nacl) deny

To add a line to an extended access list that specifies the type of packets that you want the WAAS device to drop, use the **deny** command. To add a condition to the extended ACL, note that the options depend on the chosen protocol.

For IP, use the following syntax to add a condition:

```
[insert line-num] deny {gre | icmp | tcp | udp | ip | proto-num} {source-ip [wildcard] | host
source-ip | any} {dest-ip [wildcard] | host dest-ip | any}
```

```
no deny {gre | icmp | tcp | udp | ip | proto-num} {source-ip [wildcard] | host source-ip | any}
{dest-ip [wildcard] | host dest-ip | any}
```

For TCP, use the following syntax to add a condition:

```
[insert line-num] deny tcp {source-ip [wildcard] | host source-ip | any} [operator port [port]]
{dest-ip [wildcard] | host dest-ip | any} [operator port [port]] [established]
```

```
no deny tcp {source-ip [wildcard] | host source-ip | any} [operator port [port]] {dest-ip [wildcard]
| host dest-ip | any} [operator port [port]] [established]
```

For UDP, use the following syntax to add a condition:

```
[insert line-num] deny udp {source-ip [wildcard] | host source-ip | any} [operator port [port]]
{dest-ip [wildcard] | host dest-ip | any} [operator port [port]]
```

```
no deny udp {source-ip [wildcard] | host source-ip | any} [operator port [port]] {dest-ip [wildcard]
| host dest-ip | any} [operator port [port]]
```

For ICMP, use the following syntax to add a condition:

```
[insert line-num] deny icmp {source-ip [wildcard] | host source-ip | any} {dest-ip [wildcard] | host
dest-ip | any} [icmp-type [code] | icmp-msg]
```

```
no deny icmp {source-ip [wildcard] | host source-ip | any} {dest-ip [wildcard] | host dest-ip | any}
[icmp-type [code] | icmp-msg]
```

Syntax	Description
insert	(Optional) Inserts the conditions following the specified line number into the access list.
<i>line-num</i>	Identifies the entry at a specific line number in the access list.
gre	Matches packets using the Generic Routing Encapsulation protocol.
icmp	Matches ICMP packets.
tcp	Matches packets using the TCP protocol.
udp	Matches packets using the UDP protocol.
ip	Matches all IP packets.
<i>proto-num</i>	(Optional) IP protocol number.
<i>source-ip</i>	Source IP address. The number of the network or host from which the packet is being sent, specified as a 32-bit quantity in 4-part dotted-decimal format (for example, 0.0.0.0).

<i>wildcard</i>	(Optional) Portions of the preceding IP address to match, expressed using 4-digit, dotted-decimal notation. Bits to match are identified by a digital value of 0; bits to ignore are identified by a 1. Note For extended IP ACLs, the <i>wildcard</i> parameter of the ip access-list command is always optional. If the host keyword is specified for an extended IP ACL, then the <i>wildcard</i> parameter is not allowed.
host	Matches the following IP address.
any	Matches any IP address.
<i>dest-ip</i>	Destination IP address. The number of the network or host to which the packet is being sent, specified as a 32-bit quantity in 4-part dotted decimal format (for example, 0.0.0.0).
<i>operator</i>	(Optional) Operator to use with specified ports, where lt = less than, gt = greater than, eq = equal to, neq = not equal to, and range = an inclusive range.
<i>port</i>	(Optional) Port, using a number (0–65535) or a keyword; 2 port numbers are required with range . See the Usage Guidelines section for a listing of the UDP and TCP keywords.
established	(Optional) Matches TCP packets with the acknowledgment or reset bits set.
<i>icmp-type</i>	(Optional) Match with ICMP message type (0–255).
<i>code</i>	(Optional) Used with <i>icmp-type</i> to further match by ICMP code type (0–255).
<i>icmp-msg</i>	(Optional) Match combination of ICMP message type and code types, as expressed by the keywords shown in the Usage Guidelines section.

Defaults

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

Command Modes

Extended ACL configuration mode

Device Modes

application-accelerator
replication-accelerator
central-manager

Usage Guidelines

To create an entry, use a **deny** or **permit** keyword and specify the type of packets that you want the WAAS device 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. Therefore, you must include at least one **permit** entry to create a valid access list.

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 host 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.

For extended IP ACLs, the **wildcard** parameter is required if the **host** keyword is not specified.

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 condition.

[Table 3-102](#) lists the UDP keywords that you can use with extended access lists.

Table 3-102 UDP Keywords for Extended Access Lists

CLI UDP Keyword	Description	UDP Port Number
bootpc	Bootstrap Protocol (BOOTP) client	68
bootps	Bootstrap Protocol (BOOTP) server	67
domain	Domain Name System (DNS)	53
mms	Microsoft Media Server	1755
netbios-dgm	NetBIOS datagram service	138
netbios-ns	NetBIOS name service	137
netbios-ss	NetBIOS session service	139
nfs	Network File System service	2049
ntp	Network Time Protocol	123
snmp	Simple Network Management Protocol	161
snmptrap	SNMP traps	162
tacacs	Terminal Access Controller Access Control System	49
tftp	Trivial File Transfer Protocol	69
wccp	Web Cache Communication Protocol	2048

[Table 3-103](#) lists the TCP keywords that you can use with extended access lists.

Table 3-103 TCP Keywords for Extended Access Lists

CLI TCP Keyword	Description	TCP Port Number
domain	Domain Name System	53
exec	Exec (rcp)	512
ftp	File Transfer Protocol	21
ftp-data	FTP data connections (used infrequently)	20
https	Secure HTTP	443
mms	Microsoft Media Server	1755
nfs	Network File System service	2049
ssh	Secure Shell login	22

Table 3-103 TCP Keywords for Extended Access Lists (continued)

CLI TCP Keyword	Description	TCP Port Number
tacacs	Terminal Access Controller Access Control System	49
telnet	Telnet	23
www	World Wide Web (HTTP)	80

Table 3-104 lists the keywords that you can use to match specific ICMP message types and codes.

Table 3-104 Keywords for ICMP Messages

administratively-prohibited	alternate-address	conversion-error
dod-host-prohibited	dod-net-prohibited	echo
echo-reply	general-parameter-problem	host-isolated
host-precedence-unreachable	host-redirect	host-tos-redirect
host-tos-unreachable	host-unknown	host-unreachable
information-reply	information-request	mask-reply
mask-request	mobile-redirect	net-redirect
net-tos-redirect	net-tos-unreachable	net-unreachable
network-unknown	no-room-for-option	option-missing
packet-too-big	parameter-problem	port-unreachable
precedence-unreachable	protocol-unreachable	reassembly-timeout
redirect	router-advertisement	router-solicitation
source-quench	source-route-failed	time-exceeded
timestamp-reply	timestamp-request	traceroute
ttl-exceeded	unreachable	

Examples

The following example shows how to create an access list on the WAAS device. You create this access list to allow the WAAS device to accept all web traffic that is redirected to it, but limits host administrative access using SSH:

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

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

```
WAE(config)# interface gigabitethernet 1/0
WAE(config-if)# ip access-group extended testextacl in
WAE(config-if)# exit
```

The following example shows how this configuration appears when you enter the **show running-configuration** command:

```
...
!
```

(config-ext-nacl) deny

```
interface GigabitEthernet 1/0
 ip address 10.1.1.50 255.255.0.0
 ip access-group extended testextacl in
 exit
. . .
ip access-list extended testextacl
 permit tcp any any eq www
 permit tcp host 10.1.1.5 any eq ssh
 exit
. . .
```

Related Commands[\(config-ext-nacl\) delete](#)[\(config-ext-nacl\) list](#)[\(config-ext-nacl\) move](#)[\(config-ext-nacl\) permit](#)

(config-ext-nacl) exit

To terminate extended ACL configuration mode and return to the global configuration mode, use the **exit** command.

exit

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes All modes

Device Modes application-accelerator
replication-accelerator
central-manager

Examples The following example terminates extended ACL configuration mode and returns to global configuration mode:

```
WAE(config-ext-nacl)# exit  
WAE(config)#
```

(config-ext-nacl) list

To display a list of specified entries within the extended ACL, use the **list** command.

list [*start-line-num* [*end-line-num*]]

Syntax Description	
<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.

Command Modes Extended ACL configuration mode

Device Modes application-accelerator
replication-accelerator
central-manager

Examples The following example shows how to display a list of specified entries within the extended ACL:

```
WAE(config)# ip access-list extended testextacl
WAE(config-ext-nacl)# list 25 50
```

Related Commands [\(config-ext-nacl\) delete](#)
[\(config-ext-nacl\) move](#)

(config-ext-nacl) move

To move a line to a new position within the extended ACL, use the **move** command.

```
move old-line-num new-line-num
```

Syntax Description	<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.

Command Modes Extended ACL configuration mode

Device Modes

- application-accelerator
- replication-accelerator
- central-manager

Examples The following example shows how to move a line to a new position within the extended ACL:

```
WAE(config)# ip access-list extended testextacl
WAE(config-ext-nacl)# move 25 30
```

Related Commands

- [\(config-ext-nacl\) delete](#)
- [\(config-ext-nacl\) list](#)

(config-ext-nacl) permit

To add a line to an extended access-list that specifies the type of packets that you want the WAAS device to accept for further processing, use the **permit** command. To add a condition to the extended ACL, note that the options depend on the chosen protocol.

For IP, use the following syntax to add a condition:

```
[insert line-num] permit {gre | icmp | tcp | udp | ip | proto-num} {source-ip [wildcard] | host
source-ip | any} {dest-ip [wildcard] | host dest-ip | any}

no permit {gre | icmp | tcp | udp | ip | proto-num} {source-ip [wildcard] | host source-ip | any}
{dest-ip [wildcard] | host dest-ip | any}
```

For TCP, use the following syntax to add a condition:

```
[insert line-num] permit tcp {source-ip [wildcard] | host source-ip | any} [operator port [port]]
{dest-ip [wildcard] | host dest-ip | any} [operator port [port]] [established]

no permit tcp {source-ip [wildcard] | host source-ip | any} [operator port [port]] {dest-ip
[wildcard] | host dest-ip | any} [operator port [port]] [established]
```

For UDP, use the following syntax to add a condition:

```
[insert line-num] permit udp {source-ip [wildcard] | host source-ip | any} [operator port [port]]
{dest-ip [wildcard] | host dest-ip | any} [operator port [port]]

no permit udp {source-ip [wildcard] | host source-ip | any} [operator port [port]] {dest-ip
[wildcard] | host dest-ip | any} [operator port [port]]
```

For ICMP, use the following syntax to add a condition:

```
[insert line-num] permit icmp {source-ip [wildcard] | host source-ip | any} {dest-ip [wildcard] |
host dest-ip | any} [icmp-type [code] | icmp-msg]

no permit icmp {source-ip [wildcard] | host source-ip | any} {dest-ip [wildcard] | host dest-ip |
any} [icmp-type [code] | icmp-msg]
```

Syntax	Description
insert	(Optional) Inserts the conditions following the specified line number into the access list.
<i>line-num</i>	Identifies the entry at a specific line number in the access list.
gre	Matches packets using the Generic Routing Encapsulation protocol.
icmp	Matches ICMP packets.
tcp	Matches packets using the TCP protocol.
udp	Matches packets using the UDP protocol.
ip	Matches all IP packets.
<i>proto-num</i>	(Optional) IP protocol number.
<i>source-ip</i>	Source IP address. The number of the network or host from which the packet is being sent, specified as a 32-bit quantity in 4-part dotted-decimal format (for example, 0.0.0.0).

<i>wildcard</i>	(Optional) Portions of the preceding IP address to match, expressed using 4-digit, dotted-decimal notation. Bits to match are identified by a digital value of 0; bits to ignore are identified by a 1. Note For extended IP ACLs, the <i>wildcard</i> parameter of the ip access-list command is always optional. If the host keyword is specified for an extended IP ACL, then the <i>wildcard</i> parameter is not allowed.
host	Matches the following IP address.
any	Matches any IP address.
<i>dest-ip</i>	Destination IP address. The number of the network or host to which the packet is being sent, specified as a 32-bit quantity in 4-part dotted decimal format (for example, 0.0.0.0).
<i>operator</i>	(Optional) Operator to use with specified ports, where lt = less than, gt = greater than, eq = equal to, neq = not equal to, and range = an inclusive range.
<i>port</i>	(Optional) Port, using a number (0–65535) or a keyword; 2 port numbers are required with range . See the Usage Guidelines section for a listing of the UDP and TCP keywords.
established	(Optional) Matches TCP packets with the acknowledgment or reset bits set.
<i>icmp-type</i>	(Optional) Match with ICMP message type (0–255).
<i>code</i>	(Optional) Used with <i>icmp-type</i> to further match by ICMP code type (0–255).
<i>icmp-msg</i>	(Optional) Match combination of ICMP message type and code types, as expressed by the keywords shown in the Usage Guidelines section.

Defaults

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

Command Modes

Extended ACL configuration mode

Device Modes

application-accelerator
 replication-accelerator
 central-manager

Usage Guidelines

To create an entry, use a **deny** or **permit** keyword and specify the type of packets that you want the WAAS device 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. Therefore, you must include at least one **permit** entry to create a valid access list.

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 host 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.

For extended IP ACLs, the **wildcard** parameter is required if the **host** keyword is not specified.

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 condition.

[Table 3-105](#) lists the UDP keywords that you can use with extended access lists.

Table 3-105 UDP Keywords for Extended Access Lists

CLI UDP Keyword	Description	UDP Port Number
bootpc	Bootstrap Protocol (BOOTP) client	68
bootps	Bootstrap Protocol (BOOTP) server	67
domain	Domain Name System (DNS)	53
mms	Microsoft Media Server	1755
netbios-dgm	NetBIOS datagram service	138
netbios-ns	NetBIOS name service	137
netbios-ss	NetBIOS session service	139
nfs	Network File System service	2049
ntp	Network Time Protocol	123
snmp	Simple Network Management Protocol	161
snmptrap	SNMP traps	162
tacacs	Terminal Access Controller Access Control System	49
tftp	Trivial File Transfer Protocol	69
wccp	Web Cache Communication Protocol	2048

[Table 3-106](#) lists the TCP keywords that you can use with extended access lists.

Table 3-106 TCP Keywords for Extended Access Lists

CLI TCP Keyword	Description	TCP Port Number
domain	Domain Name System	53
exec	Exec (rcp)	512
ftp	File Transfer Protocol	21
ftp-data	FTP data connections (used infrequently)	20
https	Secure HTTP	443
mms	Microsoft Media Server	1755
nfs	Network File System service	2049
ssh	Secure Shell login	22

Table 3-106 TCP Keywords for Extended Access Lists (continued)

CLI TCP Keyword	Description	TCP Port Number
tacacs	Terminal Access Controller Access Control System	49
telnet	Telnet	23
www	World Wide Web (HTTP)	80

Table 3-107 lists the keywords that you can use to match specific ICMP message types and codes.

Table 3-107 Keywords for ICMP Messages

administratively-prohibited	alternate-address	conversion-error
dod-host-prohibited	dod-net-prohibited	echo
echo-reply	general-parameter-problem	host-isolated
host-precedence-unreachable	host-redirect	host-tos-redirect
host-tos-unreachable	host-unknown	host-unreachable
information-reply	information-request	mask-reply
mask-request	mobile-redirect	net-redirect
net-tos-redirect	net-tos-unreachable	net-unreachable
network-unknown	no-room-for-option	option-missing
packet-too-big	parameter-problem	port-unreachable
precedence-unreachable	protocol-unreachable	reassembly-timeout
redirect	router-advertisement	router-solicitation
source-quench	source-route-failed	time-exceeded
timestamp-reply	timestamp-request	traceroute
ttl-exceeded	unreachable	

Examples

The following example shows how to create an access list on the WAAS device. You create this access list to allow the WAAS device to accept all web traffic that is redirected to it, but limits host administrative access using SSH:

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

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

```
WAE(config)# interface gigabitethernet 1/0
WAE(config-if)# ip access-group example in
WAE(config-if)# exit
```

The following example shows how this configuration appears when you enter the **show running-configuration** command:

```
...
!
```

(config-ext-nacl) permit

```
interface GigabitEthernet 1/0
 ip address 10.1.1.50 255.255.0.0
 ip access-group testextacl in
 exit
. . .
ip access-list extended testextacl
 permit tcp any any eq www
 permit tcp host 10.1.1.5 any eq ssh
 exit
. . .
```

Related Commands[\(config-ext-nacl\) delete](#)[\(config-ext-nacl\) deny](#)[\(config-ext-nacl\) list](#)[\(config-ext-nacl\) move](#)



APPENDIX **A**

Acronyms and Abbreviations

[Table A-1](#) defines the acronyms and abbreviations that are used in this publication.

Table A-1 *List of Acronyms and Abbreviations*

Acronym	Expansion
AAA	authentication, authorization, and accounting
ACL	access control list
ACPI	Advanced Configuration and Power Interface
ADS	Active Directory Service
ARP	Address Resolution Protocol
BIOS	Basic Input Output System
BOOTP	Bootstrap Protocol
CBA	cipher block chaining
CDP	Cisco Discovery Protocol
CIFS	Common Internet File System
CLI	command-line interface
CUPS	Common UNIX Printing System
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DSCP	differentiated services code point
ECN	Explicit Congestion Notification
FTP	file transfer protocol
GMT	Greenwich Mean Time (now known as UTC)
GRE	generic routing encapsulation
GUI	graphical user interface
HMAC	Hash-Based Message Authentication Code
ICMP	Internet Control Message Protocol
IDE	Integrated Drive Electronics
IP	Internet Protocol

Table A-1 *List of Acronyms and Abbreviations (continued)*

Acronym	Expansion
KDC	key distribution center
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
Mbps	megabits per second
MD5	Message Digest 5
MIB	Management Information Base
MSRPC	Microsoft Remote Procedure Call
MTU	maximum transmission unit
NAS	network access server/network attached storage
NetBIOS	Network Basic Input/Output System
NMS	Network Management system
NTP	Network Time Protocol
NTLM	NT LAN Manager
NVRAM	nonvolatile RAM
PAP	Password Authentication Protocol
PDC	primary domain controller
PID	product ID
POST	Power-on Self Test
RADIUS	Remote Access Dial-In User Service
RAID	Redundant Array of Independent Disks
RAM	random access memory
rcp	remote copy protocol
RMSS	receiver maximum segment size
ROM	read-only memory
SCSI	Small Computer Systems Interface
SHA	Secure Hash Algorithm
SMART	Self Monitoring, Analysis, and Reporting Technology
SMB	Server Message Block
SMSS	sender maximum segment size
SN	serial number
SNMP	Simple Network Management Protocol
SSH	Secure Shell Protocol
SYSFS	System File System
TAC	Technical Assistance Center
TACACS+	Terminal Access Controller Access Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol

Table A-1 *List of Acronyms and Abbreviations (continued)*

Acronym	Expansion
TDB	Trivial DataBase
TFTP	Trivial File Transfer Protocol
ToS	type of service
UDI	unique device identifier
UDP	User Datagram Protocol
UPS	uninterruptible power supply
USB	Universal Serial Bus
UTC	Coordinated Universal Time
UUCP	Unix-to-Unix Copy Program
VID	version ID
WAE	Wide Area Application Engine
WAAS	Wide Area Application Services
WAFSFS	Wide Area File Services File System
WCCP	Web Cache Communication Protocol
WINS	Windows naming service



CLI COMMAND SUMMARY BY MODE

Configuration Mode Commands

- (config) aaa accounting [3-281](#)
- (config) adapter [3-285](#)
- (config) alarm overload-detect [3-286](#)
- (config) asset [3-288](#)
- (config) authentication [3-289](#)
- (config) auto-register [3-296](#)
- (config) banner [3-299](#)
- (config) bypass [3-302](#)
- (config) cdp [3-304](#)
- (config) central-manager [3-306](#)
- (config) clock [3-310](#)
- (config) cms [3-314](#)
- (config) device mode [3-316](#)
- (config) disk disk-name [3-318](#)
- (config) disk encrypt [3-320](#)
- (config) disk error-handling [3-322](#)
- (config) disk logical shutdown [3-324](#)
- (config) egress-method [3-325](#)
- (config) end [3-327](#)
- (config) exec-timeout [3-328](#)
- (config) exit [3-329](#)
- (config) external-ip [3-330](#)
- (config) flow monitor [3-332](#)
- (config) help [3-333](#)
- (config) hostname [3-335](#)
- (config) inetd [3-337](#)
- (config) interface [3-338](#)
- (config) ip [3-344](#)
- (config) ip access-list [3-347](#)
- (config) kerberos [3-350](#)
- (config) kernel [3-352](#)
- (config) line [3-353](#)
- (config) logging [3-354](#)
- (config) no [3-358](#)
- (config) ntp [3-360](#)
- (config) policy-engine application classifier [3-362](#)
- (config) policy-engine application map adaptor EPM [3-364](#)
- (config) policy-engine application map adaptor WAFS transport [3-366](#)
- (config) policy-engine application map basic delete [3-368](#)
- (config) policy-engine application map basic disable [3-369](#)
- (config) policy-engine application map basic insert [3-370](#)
- (config) policy-engine application map basic list [3-371](#)
- (config) policy-engine application map basic move [3-372](#)
- (config) policy-engine application map basic name [3-374](#)
- (config) policy-engine application map other optimize DRE [3-376](#)
- (config) policy-engine application map other optimize full [3-378](#)
- (config) policy-engine application map other pass-through [3-379](#)
- (config) policy-engine application name [3-380](#)
- (config) policy-engine config [3-382](#)
- (config) port-channel [3-383](#)
- (config) primary-interface [3-384](#)
- (config) print-services [3-386](#)
- (config) radius-server [3-389](#)
- (config) smb-conf [3-391](#)
- (config) snmp-server access-list [3-395](#)
- (config) snmp-server community [3-396](#)

- (config) snmp-server contact [3-398](#)
- (config) snmp-server enable traps [3-399](#)
- (config) snmp-server group [3-402](#)
- (config) snmp-server host [3-404](#)
- (config) snmp-server location [3-406](#)
- (config) snmp-server mib [3-407](#)
- (config) snmp-server notify inform [3-409](#)
- (config) snmp-server user [3-412](#)
- (config) snmp-server view [3-414](#)
- (config) sshd [3-415](#)
- (config) ssh-key-generate [3-418](#)
- (config) tacacs [3-419](#)
- (config) tcp [3-422](#)
- (config) telnet enable [3-425](#)
- (config) tfo auto-discovery [3-426](#)
- (config) tfo optimize [3-427](#)
- (config) tfo tcp keepalive [3-428](#)
- (config) tfo tcp optimized-mss [3-429](#)
- (config) tfo tcp optimized-receive-buffer [3-430](#)
- (config) tfo tcp optimized-send-buffer [3-431](#)
- (config) tfo tcp original-mss [3-432](#)
- (config) tfo tcp original-receive-buffer [3-433](#)
- (config) tfo tcp original-send-buffer [3-434](#)
- (config) transaction-logs [3-435](#)
- (config) username [3-442](#)
- (config) wccp access-list [3-445](#)
- (config) wccp flow-redirect [3-448](#)
- (config) wccp router-list [3-449](#)
- (config) wccp shutdown [3-450](#)
- (config) wccp tcp-promiscuous [3-452](#)
- (config) wccp version [3-454](#)
- (config) windows-domain [3-456](#)
- clear users [3-8](#)
- clock [3-10](#)
- cms [3-11](#)
- cms secure-store [3-14](#)
- configure [3-16](#)
- copy cdrom [3-17](#)
- copy compactflash [3-18](#)
- copy disk [3-19](#)
- copy ftp [3-20](#)
- copy http [3-25](#)
- copy running-config [3-29](#)
- copy startup-config [3-30](#)
- copy sysreport [3-31](#)
- copy system-status [3-33](#)
- copy tech-support [3-34](#)
- copy tftp [3-35](#)
- cpfile [3-37](#)
- debug [3-38](#)
- delfile [3-44](#)
- deltree [3-45](#)
- dir [3-46](#)
- disable [3-48](#)
- disk [3-49](#)
- dnslookup [3-53](#)
- enable [3-54](#)
- exit [3-55](#)
- find-pattern [3-56](#)
- help [3-58](#)
- install [3-59](#)
- less [3-61](#)
- lls [3-62](#)
- ls [3-64](#)
- mkdir [3-66](#)
- mkfile [3-67](#)
- ntpdate [3-68](#)
- ping [3-69](#)
- pwd [3-70](#)
- reload [3-71](#)
- rename [3-72](#)

EXEC Mode Commands

- authentication strict-password-policy [3-294](#)
- cd [3-3](#)
- cifs [3-4](#)
- clear [3-5](#)

- clear users [3-8](#)
- clock [3-10](#)
- cms [3-11](#)
- cms secure-store [3-14](#)
- configure [3-16](#)
- copy cdrom [3-17](#)
- copy compactflash [3-18](#)
- copy disk [3-19](#)
- copy ftp [3-20](#)
- copy http [3-25](#)
- copy running-config [3-29](#)
- copy startup-config [3-30](#)
- copy sysreport [3-31](#)
- copy system-status [3-33](#)
- copy tech-support [3-34](#)
- copy tftp [3-35](#)
- cpfile [3-37](#)
- debug [3-38](#)
- delfile [3-44](#)
- deltree [3-45](#)
- dir [3-46](#)
- disable [3-48](#)
- disk [3-49](#)
- dnslookup [3-53](#)
- enable [3-54](#)
- exit [3-55](#)
- find-pattern [3-56](#)
- help [3-58](#)
- install [3-59](#)
- less [3-61](#)
- lls [3-62](#)
- ls [3-64](#)
- mkdir [3-66](#)
- mkfile [3-67](#)
- ntpdate [3-68](#)
- ping [3-69](#)
- pwd [3-70](#)
- reload [3-71](#)
- rename [3-72](#)

- restore [3-73](#)
- rmdir [3-77](#)
- scp [3-78](#)
- script [3-80](#)
- setup [3-81](#)
- show aaa accounting [3-82](#)
- show adapter [3-84](#)
- show alarms [3-85](#)
- show arp [3-88](#)
- show authentication [3-89](#)
- show auto-register [3-91](#)
- show banner [3-92](#)
- show bypass [3-93](#)
- show cdp [3-94](#)
- show cifs [3-100](#)
- show clock [3-102](#)
- show cms [3-104](#)
- show cms secure-store [3-107](#)
- show debugging [3-108](#)
- show device-mode [3-109](#)
- show disks [3-111](#)
- show egress-methods [3-118](#)
- show flash [3-119](#)
- show hardware [3-120](#)
- show hosts [3-123](#)
- show inetd [3-124](#)
- show interface [3-125](#)
- show inventory [3-130](#)
- show ip access-list [3-131](#)
- show ip routes [3-133](#)
- show kerberos [3-134](#)
- show key-manager [3-135](#)
- show logging [3-136](#)
- show memory [3-137](#)
- show ntp [3-138](#)
- show policy-engine application [3-140](#)
- show policy-engine status [3-144](#)
- show print-services [3-146](#)
- show processes [3-148](#)
- show radius-server [3-150](#)
- show running-config [3-152](#)
- show services [3-154](#)
- show smb-conf [3-155](#)
- show snmp [3-157](#)
- show ssh [3-163](#)
- show standby [3-164](#)
- show startup-config [3-166](#)
- show statistics authentication [3-168](#)
- show statistics cifs [3-169](#)
- show statistics content-distribution-network [3-171](#)
- show statistics dre [3-172](#)
- show statistics dre connection [3-174](#)
- show statistics dre peer [3-176](#)
- show statistics epm [3-179](#)
- show statistics flow [3-180](#)
- show statistics icmp [3-183](#)
- show statistics ip [3-185](#)
- show statistics key-manager [3-188](#)
- show statistics netstat [3-189](#)
- show statistics radius [3-190](#)
- show statistics services [3-192](#)
- show statistics snmp [3-193](#)
- show statistics tacacs [3-195](#)
- show statistics tcp [3-197](#)
- show statistics tfo [3-203](#)
- show statistics udp [3-205](#)
- show statistics wccp [3-206](#)
- show statistics windows-domain [3-211](#)
- show sysfs [3-213](#)
- show tacacs [3-214](#)
- show tcp [3-216](#)
- show tech-support [3-218](#)
- show telnet [3-221](#)
- show tfo accelerators [3-222](#)
- show tfo auto-discovery [3-223](#)
- show tfo bufpool [3-225](#)
- show tfo connection [3-227](#)
- show tfo egress connection [3-229](#)

show tfo filtering [3-233](#)
 show tfo status [3-235](#)
 show tfo synq [3-236](#)
 show transaction-logging [3-237](#)
 show user [3-238](#)
 show users administrative [3-239](#)
 show version [3-241](#)
 show wccp [3-242](#)
 show windows-domain [3-248](#)
 shutdown [3-250](#)
 snmp trigger [3-253](#)
 ssh [3-256](#)
 tcpdump [3-257](#)
 telnet [3-259](#)
 terminal [3-260](#)
 tethereal [3-261](#)
 traceroute [3-263](#)
 transaction-log [3-264](#)
 type [3-265](#)
 type-tail [3-266](#)
 undebg [3-268](#)
 wafs [3-273](#)
 whoami [3-275](#)
 windows-domain [3-276](#)
 write [3-279](#)

Extended ACL Configuration Mode Commands

(config-ext-nacl) delete [3-499](#)
 (config-ext-nacl) deny [3-500](#)
 (config-ext-nacl) exit [3-505](#)
 (config-ext-nacl) list [3-506](#)
 (config-ext-nacl) move [3-507](#)
 (config-ext-nacl) permit [3-508](#)

Interface Configuration Mode Commands

(config-if) autosense [3-459](#)
 (config-if) bandwidth [3-460](#)
 (config-if) cdp [3-462](#)
 (config-if) exit [3-463](#)
 (config-if) failover timeout [3-464](#)
 (config-if) full-duplex [3-465](#)
 (config-if) half-duplex [3-467](#)
 (config-if) inline [3-469](#)
 (config-if) ip [3-471](#)
 (config-if) ip access-group [3-473](#)
 (config-if) mtu [3-475](#)
 (config-if) no [3-476](#)
 (config-if) shutdown [3-478](#)
 (config-if) standby [3-479](#)

Standard ACL Configuration Mode Commands

(config) ip access-list standard [3-485](#)
 (config-std-nacl) delete [3-488](#)
 (config-std-nacl) deny [3-489](#)
 (config-std-nacl) exit [3-491](#)
 (config-std-nacl) list [3-492](#)
 (config-std-nacl) move [3-493](#)
 (config-std-nacl) permit [3-494](#)