



## **Cisco Wide Area Application Services Command Reference**

Software Release 4.1.3

April 19, 2010

### **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

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, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flip Video, Flip Video (Design), Flipshare (Design), Flip Ultra, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0907R)

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*  
© 2006-2009 Cisco Systems, Inc. All rights reserved.



## CONTENTS

---

**CHAPTER 1****Preface** xvii**Using the WAAS Command-Line Interface** 1-1

|  |      |
|--|------|
| About the WAAS                             | 1-1  |
| Command Line Interface                     | 1-2  |
| Graphical User Interface                   | 1-2  |
| Using Command Modes                        | 1-2  |
| Organization of the WAAS CLI               | 1-3  |
| Using EXEC Mode                            | 1-4  |
| EXEC Mode Levels                           | 1-4  |
| EXEC Mode Command-Line Processing          | 1-4  |
| Using Global Configuration Mode            | 1-5  |
| Configuration Submodes                     | 1-5  |
| Exiting Configuration Mode                 | 1-5  |
| Using the Interface Configuration Mode     | 1-6  |
| Using ACL Configuration Modes              | 1-6  |
| Using the Preposition Configuration Mode   | 1-6  |
| Using the Virtual Blade Configuration Mode | 1-7  |
| Command Modes Summary                      | 1-7  |
| Device Mode                                | 1-8  |
| Changing the Device Mode                   | 1-8  |
| Displaying the Configured Device Mode      | 1-9  |
| Using Command-Line Processing              | 1-9  |
| Checking Command Syntax                    | 1-10 |
| Using the no Form of Commands              | 1-11 |
| Using System Help                          | 1-11 |
| Saving Configuration Changes               | 1-12 |
| WAAS Directories on a WAE                  | 1-12 |
| Navigating WAAS Directories                | 1-12 |
| Directory Descriptions                     | 1-13 |
| Managing WAAS Files Per Device             | 1-15 |

---

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

---

**CHAPTER 3 CLI Commands 3-1**

**EXEC Mode Commands 3-3**

- cd 3-4
- cifs 3-5
- clear arp-cache 3-7
- clear cache 3-8
- clear cdp 3-9
- clear ip 3-10
- clear license 3-11
- clear logging 3-12
- clear statistics 3-13
- clear statistics accelerator 3-15
- clear statistics connection 3-16
- clear transaction-log 3-18
- clear users 3-19
- clear windows-domain-log 3-21
- clock 3-22
- cms 3-23
- cms secure-store 3-26
- configure 3-29
- copy cdrom 3-30
- copy cdrom wow-recovery 3-31
- copy compactflash 3-32
- copy disk 3-33
- copy ftp 3-35
- copy http 3-39
- copy running-config 3-43
- copy startup-config 3-45
- copy sysreport 3-46
- copy system-status 3-48
- copy tech-support 3-49
- copy tftp 3-51
- copy virtual-blade 3-52

cpfile **3-53**  
crypto delete **3-54**  
crypto export **3-55**  
crypto generate **3-57**  
crypto import **3-59**  
crypto pki **3-61**  
debug aaa accounting **3-62**  
debug accelerator **3-64**  
debug all **3-67**  
debug authentication **3-69**  
debug buf **3-71**  
debug cdp **3-73**  
debug cli **3-75**  
debug cms **3-77**  
debug dataserver **3-79**  
debug dhcp **3-81**  
debug dre **3-83**  
debug egress-method **3-85**  
debug emdb **3-87**  
debug epm **3-89**  
debug flow **3-91**  
debug generic-gre **3-93**  
debug key-manager **3-95**  
debug logging **3-97**  
debug ntp **3-99**  
debug print-spooler **3-101**  
debug rbcpc **3-103**  
debug rpc **3-105**  
debug snmp **3-107**  
debug stats **3-109**  
debug tfo **3-111**  
debug translog **3-113**  
debug wafs **3-115**  
debug wccp **3-117**  
delfile **3-119**

deltree **3-120**  
dir **3-121**  
disable **3-123**  
disk **3-124**  
dnslookup **3-126**  
enable **3-127**  
exit **3-128**  
find-pattern **3-129**  
help **3-131**  
install **3-132**  
less **3-134**  
license add **3-135**  
lls **3-136**  
ls **3-138**  
mkdir **3-140**  
mkfile **3-141**  
ntpdate **3-142**  
ping **3-143**  
pwd **3-144**  
reload **3-145**  
rename **3-146**  
restore **3-147**  
rmdir **3-151**  
scp **3-152**  
script **3-154**  
setup **3-155**  
show aaa accounting **3-156**  
show accelerator **3-158**  
show alarms **3-160**  
show arp **3-163**  
show authentication **3-164**  
show auto-discovery **3-166**  
show auto-register **3-167**  
show banner **3-168**  
show bypass **3-169**

show cdp **3-170**  
show cifs **3-176**  
show clock **3-178**  
show cms **3-180**  
show cms secure-store **3-183**  
show crypto **3-184**  
show debugging **3-186**  
show device-mode **3-187**  
show directed-mode **3-189**  
show disks **3-190**  
show egress-methods **3-197**  
show filtering list **3-198**  
show flash **3-200**  
show hardware **3-201**  
show hosts **3-204**  
show inetd **3-205**  
show interface **3-206**  
show inventory **3-211**  
show ip access-list **3-212**  
show ip routes **3-214**  
show kdump **3-215**  
show kerberos **3-216**  
show license **3-217**  
show logging **3-218**  
show memory **3-219**  
show ntp **3-220**  
show policy-engine application **3-222**  
show policy-engine status **3-226**  
show print-services **3-228**  
show processes **3-230**  
show radius-server **3-232**  
show running-config **3-234**  
show services **3-236**  
show smb-conf **3-237**  
show snmp **3-239**

|   |              |
|---|--------------|
| show ssh                                  | <b>3-245</b> |
| show startup-config                       | <b>3-246</b> |
| show statistics accelerator               | <b>3-248</b> |
| show statistics aom                       | <b>3-275</b> |
| show statistics application               | <b>3-279</b> |
| show statistics authentication            | <b>3-282</b> |
| show statistics auto-discovery            | <b>3-283</b> |
| show statistics cifs                      | <b>3-286</b> |
| show statistics connection                | <b>3-288</b> |
| show statistics connection auto-discovery | <b>3-290</b> |
| show statistics connection closed         | <b>3-292</b> |
| show statistics connection conn-id        | <b>3-295</b> |
| show statistics connection egress-methods | <b>3-298</b> |
| show statistics connection optimized      | <b>3-302</b> |
| show statistics connection pass-through   | <b>3-305</b> |
| show statistics crypto ssl ciphers        | <b>3-307</b> |
| show statistics datamover                 | <b>3-308</b> |
| show statistics directed-mode             | <b>3-310</b> |
| show statistics dre                       | <b>3-311</b> |
| show statistics filtering                 | <b>3-313</b> |
| show statistics flow                      | <b>3-315</b> |
| show statistics generic-gre               | <b>3-318</b> |
| show statistics icmp                      | <b>3-319</b> |
| show statistics ip                        | <b>3-321</b> |
| show statistics netstat                   | <b>3-324</b> |
| show statistics pass-through              | <b>3-325</b> |
| show statistics peer                      | <b>3-327</b> |
| show statistics radius                    | <b>3-330</b> |
| show statistics services                  | <b>3-332</b> |
| show statistics snmp                      | <b>3-333</b> |
| show statistics synq                      | <b>3-335</b> |
| show statistics tacacs                    | <b>3-336</b> |
| show statistics tcp                       | <b>3-338</b> |
| show statistics tfo                       | <b>3-342</b> |
| show statistics udp                       | <b>3-346</b> |

show statistics wccp **3-347**  
show statistics windows-domain **3-351**  
show statistics windows-print requests **3-353**  
show synq list **3-355**  
show sysfs volumes **3-356**  
show tacacs **3-357**  
show tcp **3-359**  
show tech-support **3-361**  
show telnet **3-364**  
show tfo tcp **3-365**  
show transaction-logging **3-366**  
show user **3-368**  
show users administrative **3-369**  
show version **3-371**  
show virtual-blade **3-372**  
show wccp **3-375**  
show windows-domain **3-381**  
shutdown **3-383**  
snmp trigger **3-386**  
ssh **3-390**  
tcpdump **3-391**  
telnet **3-393**  
terminal **3-394**  
test **3-395**  
tethereal **3-398**  
traceroute **3-400**  
transaction-log **3-401**  
type **3-402**  
type-tail **3-403**  
virtual-blade **3-405**  
wafs **3-407**  
whoami **3-409**  
windows-domain **3-410**  
write **3-413**

|  |              |
|--|--------------|
| <b>Global Configuration Mode Commands</b>      | <b>3-414</b> |
| (config) aaa accounting                        | <b>3-415</b> |
| (config) accelerator cifs                      | <b>3-418</b> |
| (config) accelerator cifs preposition          | <b>3-420</b> |
| (config) accelerator epm                       | <b>3-421</b> |
| (config) accelerator http                      | <b>3-422</b> |
| (config) accelerator mapi                      | <b>3-423</b> |
| (config) accelerator nfs                       | <b>3-424</b> |
| (config) accelerator ssl                       | <b>3-425</b> |
| (config) accelerator video                     | <b>3-427</b> |
| (config) accelerator windows-print             | <b>3-429</b> |
| (config) alarm overload-detect                 | <b>3-430</b> |
| (config) asset                                 | <b>3-432</b> |
| (config) authentication configuration          | <b>3-433</b> |
| (config) authentication content-request        | <b>3-438</b> |
| (config) authentication fail-over              | <b>3-442</b> |
| (config) authentication login                  | <b>3-446</b> |
| (config) authentication strict-password-policy | <b>3-451</b> |
| (config) auto-discovery                        | <b>3-453</b> |
| (config) auto-register                         | <b>3-454</b> |
| (config) banner                                | <b>3-456</b> |
| (config) bypass                                | <b>3-459</b> |
| (config) cdp                                   | <b>3-461</b> |
| (config) central-manager                       | <b>3-462</b> |
| (config) clock                                 | <b>3-464</b> |
| (config) cms                                   | <b>3-468</b> |
| (config) crypto pki                            | <b>3-471</b> |
| (config) crypto ssl                            | <b>3-472</b> |
| (config) device mode                           | <b>3-473</b> |
| (config) directed-mode                         | <b>3-474</b> |
| (config) disk disk-name                        | <b>3-475</b> |
| (config) disk encrypt                          | <b>3-477</b> |
| (config) disk error-handling                   | <b>3-478</b> |
| (config) disk logical shutdown                 | <b>3-479</b> |
| (config) egress-method                         | <b>3-480</b> |

|   |              |
|---|--------------|
| (config) end  | <b>3-482</b> |
| (config) exec-timeout   | <b>3-483</b> |
| (config) exit   | <b>3-484</b> |
| (config) flow monitor   | <b>3-485</b> |
| (config) help   | <b>3-486</b> |
| (config) hostname   | <b>3-488</b> |
| (config) inetd  | <b>3-490</b> |
| (config) inline vlan-id-connection-check                      | <b>3-491</b> |
| (config) interface GigabitEthernet                            | <b>3-492</b> |
| (config) interface InlineGroup                                | <b>3-497</b> |
| (config) interface PortChannel                                | <b>3-499</b> |
| (config) interface standby                                    | <b>3-501</b> |
| (config) ip   | <b>3-502</b> |
| (config) ip access-list                                       | <b>3-504</b> |
| (config) kerberos   | <b>3-507</b> |
| (config) kernel kdb   | <b>3-509</b> |
| (config) kernel kdump   | <b>3-510</b> |
| (config) line   | <b>3-511</b> |
| (config) logging console                                      | <b>3-512</b> |
| (config) logging disk   | <b>3-514</b> |
| (config) logging facility                                     | <b>3-516</b> |
| (config) logging host   | <b>3-518</b> |
| (config) ntp  | <b>3-520</b> |
| (config) policy-engine application classifier                 | <b>3-522</b> |
| (config) policy-engine application map adaptor EPM            | <b>3-524</b> |
| (config) policy-engine application map adaptor WAFS transport | <b>3-526</b> |
| (config) policy-engine application map basic                  | <b>3-528</b> |
| (config) policy-engine application map other optimize DRE     | <b>3-531</b> |
| (config) policy-engine application map other optimize full    | <b>3-533</b> |
| (config) policy-engine application map other pass-through     | <b>3-534</b> |
| (config) policy-engine application name                       | <b>3-535</b> |
| (config) policy-engine application set-dscp                   | <b>3-537</b> |
| (config) policy-engine config                                 | <b>3-539</b> |
| (config) port-channel   | <b>3-541</b> |
| (config) primary-interface                                    | <b>3-542</b> |

|   |              |
|---|--------------|
| (config) print-services                   | <b>3-544</b> |
| (config) radius-server                    | <b>3-546</b> |
| (config) smb-conf                         | <b>3-548</b> |
| (config) snmp-server access-list          | <b>3-552</b> |
| (config) snmp-server community            | <b>3-553</b> |
| (config) snmp-server contact              | <b>3-555</b> |
| (config) snmp-server enable traps         | <b>3-556</b> |
| (config) snmp-server group                | <b>3-559</b> |
| (config) snmp-server host                 | <b>3-561</b> |
| (config) snmp-server location             | <b>3-563</b> |
| (config) snmp-server mib                  | <b>3-564</b> |
| (config) snmp-server notify inform        | <b>3-566</b> |
| (config) snmp-server trap-source          | <b>3-567</b> |
| (config) snmp-server user                 | <b>3-568</b> |
| (config) snmp-server view                 | <b>3-570</b> |
| (config) sshd                             | <b>3-571</b> |
| (config) ssh-key-generate                 | <b>3-574</b> |
| (config) tacacs                           | <b>3-575</b> |
| (config) tcp                              | <b>3-578</b> |
| (config) telnet enable                    | <b>3-580</b> |
| (config) tfo exception                    | <b>3-581</b> |
| (config) tfo optimize                     | <b>3-582</b> |
| (config) tfo tcp adaptive-buffer-sizing   | <b>3-583</b> |
| (config) tfo tcp keepalive                | <b>3-584</b> |
| (config) tfo tcp optimized-mss            | <b>3-585</b> |
| (config) tfo tcp optimized-receive-buffer | <b>3-586</b> |
| (config) tfo tcp optimized-send-buffer    | <b>3-587</b> |
| (config) tfo tcp original-mss             | <b>3-588</b> |
| (config) tfo tcp original-receive-buffer  | <b>3-589</b> |
| (config) tfo tcp original-send-buffer     | <b>3-590</b> |
| (config) transaction-logs                 | <b>3-591</b> |
| (config) username                         | <b>3-594</b> |
| (config) virtual-blade                    | <b>3-596</b> |
| (config) wccp access-list                 | <b>3-598</b> |
| (config) wccp flow-redirect               | <b>3-601</b> |

- (config) wccp router-list **3-602**
- (config) wccp shutdown **3-604**
- (config) wccp tcp-promiscuous mask **3-606**
- (config) wccp tcp-promiscuous router-list-num **3-607**
- (config) wccp version **3-609**
- (config) windows-domain **3-610**

### **Interface Configuration Mode Commands 3-613**

- (config-if) autosense **3-614**
- (config-if) bandwidth **3-615**
- (config-if) cdp **3-617**
- (config-if) encapsulation dot1Q **3-619**
- (config-if) exit **3-620**
- (config-if) failover timeout **3-621**
- (config-if) full-duplex **3-622**
- (config-if) half-duplex **3-624**
- (config-if) inline **3-626**
- (config-if) ip **3-628**
- (config-if) ip access-group **3-630**
- (config-if) mtu **3-631**
- (config-if) shutdown **3-632**
- (config-if) standby **3-633**

### **Standard ACL Configuration Mode Commands 3-635**

- (config-std-nacl) delete **3-638**
- (config-std-nacl) deny **3-639**
- (config-std-nacl) exit **3-641**
- (config-std-nacl) list **3-642**
- (config-std-nacl) move **3-643**
- (config-std-nacl) permit **3-644**

### **Extended ACL Configuration Mode Commands 3-646**

- (config-ext-nacl) delete **3-649**
- (config-ext-nacl) deny **3-650**
- (config-ext-nacl) exit **3-655**
- (config-ext-nacl) list **3-656**
- (config-ext-nacl) move **3-657**

|  |       |
|--|-------|
| (config-ext-nacl) permit   | 3-658 |
| <b>Preposition Configuration Mode Commands</b> 3-663               |       |
| (config-preposition) credentials                                   | 3-664 |
| (config-preposition) dscp  | 3-665 |
| (config-preposition) duration                                      | 3-666 |
| (config-preposition) enable  | 3-667 |
| (config-preposition) ignore-hidden-dir                             | 3-668 |
| (config-preposition) max-cache                                     | 3-669 |
| (config-preposition) max-file-size                                 | 3-670 |
| (config-preposition) min-file-size                                 | 3-671 |
| (config-preposition) name  | 3-672 |
| (config-preposition) pattern                                       | 3-673 |
| (config-preposition) recursive                                     | 3-674 |
| (config-preposition) root  | 3-675 |
| (config-preposition) scan-type                                     | 3-676 |
| (config-preposition) schedule                                      | 3-677 |
| (config-preposition) server  | 3-679 |
| <b>Virtual Blade Configuration Mode Commands</b> 3-681             |       |
| (config-vb) autostart  | 3-683 |
| (config-vb) boot   | 3-684 |
| (config-vb) description  | 3-686 |
| (config-vb) device   | 3-687 |
| (config-vb) disk   | 3-690 |
| (config-vb) interface  | 3-692 |
| (config-vb) memory   | 3-693 |
| (config-vb) vnc  | 3-694 |
| <b>PKI Certificate Authority Configuration Mode Commands</b> 3-695 |       |
| (config-ca) ca-certificate   | 3-697 |
| (config-ca) description  | 3-698 |
| (config-ca) revocation-check                                       | 3-699 |
| <b>PKI Global Settings Configuration Mode Commands</b> 3-701       |       |
| (config-pki-global-settings) ocsp                                  | 3-702 |
| (config-pki-global-settings) revocation-check                      | 3-703 |

**SSL Cipher List Configuration Mode Commands 3-705**

(config-cipher-list) cipher 3-706

**APPENDIX A****Acronyms and Abbreviations A-1****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 xvii](#)
- [Document Organization, page xvii](#)
- [Document Conventions, page xviii](#)
- [Related Documentation, page xix](#)
- [Obtaining Documentation and Submitting a Service Request, page xx](#)

## 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.

## Document Organization

This command reference includes the following chapters:

| Chapter  | Description  |
|--|--|
| <a href="#">Chapter 1, “Using the WAAS Command-Line Interface”</a> | Describes how to use the command-line interface.                     |
| <a href="#">Chapter 2, “Cisco WAAS Software Command Summary”</a>   | Lists WAAS software commands, providing a brief description of each. |

| Chapter  | Description  |
|--|--|
| <a href="#">Chapter 3, “CLI Commands”</a>                | <p>Provides detailed information for the following types of CLI commands for the WAAS software:</p> <ul style="list-style-type: none"> <li>• Commands you can enter after you log in to the WAAS device (EXEC mode).</li> <li>• 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.</li> </ul> <p>The description of each command includes the syntax of the command and any related commands, when appropriate.</p> |
| <a href="#">Appendix A, “Acronyms and Abbreviations”</a> | Defines the acronyms used in this publication.   |
| <a href="#">CLI Command Summary by Mode</a>              | Lists each command by command mode.  |

## Document Conventions

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

| Convention                  | Description  |
|-----------------------------|--|
| <b>boldface</b> font        | Commands, keywords, and button names are in <b>boldface</b> .  |
| <i>italic</i> font          | 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 screen font.  |
| <b>boldface screen</b> font | Information you must enter is in <b>boldface screen</b> font.  |
| <i>italic screen</i> font   | Variables you enter are printed in <i>italic screen</i> font.  |
| plain font                  | Enter one of a range of options as listed in the syntax description.   |
| <b>^D or Ctrl-D</b>         | Hold the <b>Ctrl</b> key while you press the <b>D</b> key.   |
| string                      | <p>Defined as a nonquoted set of characters.</p> <p>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.</p> |
| 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 Notes for Cisco Wide Area Application Services*  
[http://www.cisco.com/en/US/products/ps6870/prod\\_release\\_notes\\_list.html](http://www.cisco.com/en/US/products/ps6870/prod_release_notes_list.html)
- *Cisco Wide Area Application Services Configuration Guide*  
[http://www.cisco.com/en/US/products/ps6870/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps6870/products_installation_and_configuration_guides_list.html)
- *Cisco Wide Area Application Services Quick Configuration Guide*  
[http://www.cisco.com/en/US/products/ps6870/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps6870/products_installation_and_configuration_guides_list.html)
- *Cisco Wide Area Application Services API Reference*  
[http://www.cisco.com/en/US/products/ps6870/products\\_programming\\_reference\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps6870/products_programming_reference_guides_list.html)
- *Regulatory Compliance and Safety Information for the Cisco Content Networking Product Series*  
[http://www.cisco.com/en/US/docs/app\\_ntwk\\_services/waas/wae/regulatory/compliance/11564rcs.html](http://www.cisco.com/en/US/docs/app_ntwk_services/waas/wae/regulatory/compliance/11564rcs.html)
- *Cisco Wide Area Application Engine 511 and 611 Hardware Installation Guide*  
[http://www.cisco.com/en/US/products/ps6474/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps6474/prod_installation_guides_list.html)
- *Cisco Wide Area Application Engine 512 and 612 Hardware Installation Guide*  
[http://www.cisco.com/en/US/products/ps6474/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps6474/prod_installation_guides_list.html)
- *Cisco Wide Area Application Engine 7326 Hardware Installation Guide*  
[http://www.cisco.com/en/US/products/ps6474/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps6474/prod_installation_guides_list.html)
- *Cisco Wide Area Application Engine 7341, 7371, and 674 Hardware Installation Guide*  
[http://www.cisco.com/en/US/products/ps6474/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps6474/prod_installation_guides_list.html)
- *Cisco WAAS Enhanced Network Modules*  
<http://www.cisco.com/en/US/docs/routers/access/interfaces/nm/hardware/installation/guide/waasnme.html>
- *Using the Print Utilities to Troubleshoot and Fix Samba Driver Installation Problems*  
[http://www.cisco.com/en/US/products/ps6870/prod\\_troubleshooting\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps6870/prod_troubleshooting_guides_list.html)
- *Cisco Wide Area Virtualization Engine 574 Hardware Installation Guide*

[http://www.cisco.com/en/US/docs/app\\_ntwk\\_services/waas/wave/installation/574/guide/574inst.html](http://www.cisco.com/en/US/docs/app_ntwk_services/waas/wave/installation/574/guide/574inst.html)

- *Cisco Wide Area Virtualization Engine 274 and 474 Hardware Installation Guide*  
[http://www.cisco.com/en/US/docs/app\\_ntwk\\_services/waas/wave/installation/274-474/guide/wave274hig.html](http://www.cisco.com/en/US/docs/app_ntwk_services/waas/wave/installation/274-474/guide/wave274hig.html)
- *Regulatory Compliance and Safety Information for the Cisco Wide Area Virtualization Engines*  
[http://www.cisco.com/en/US/docs/app\\_ntwk\\_services/waas/wave/regulatory/compliance/wavercsi.html](http://www.cisco.com/en/US/docs/app_ntwk_services/waas/wave/regulatory/compliance/wavercsi.html)

## Obtaining Documentation and Submitting a Service Request

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

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

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



# CHAPTER 1

## Using the WAAS Command-Line Interface

---

This chapter describes 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:

- [About the WAAS, page 1-1](#)
- [Using Command Modes, page 1-2](#)
- [Using Command-Line Processing, page 1-9](#)
- [Checking Command Syntax, page 1-10](#)
- [Using the no Form of Commands, page 1-11](#)
- [Using System Help, page 1-11](#)
- [Saving Configuration Changes, page 1-12](#)
- [WAAS Directories on a WAE, page 1-12](#)
- [Managing WAAS Files Per Device, page 1-15](#)

## About the WAAS

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-674, WAE-7326, WAE-7341, WAE-7371, and on WAE-NME network modules that are connected to specific Cisco routers. You must deploy the WAAS Central Manager on a dedicated appliance.

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 on the WAAS software unless otherwise noted.

## Command Line Interface

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.

## Graphical User Interface

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.

## 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 1-3
- Using EXEC Mode, page 1-4
- Using Global Configuration Mode, page 1-5
- Using the Interface Configuration Mode, page 1-6
- Using ACL Configuration Modes, page 1-6
- Using the Preposition Configuration Mode, page 1-6
- Using the Virtual Blade Configuration Mode, page 1-7
- Command Modes Summary, page 1-7
- Device Mode, page 1-8

## Organization of the WAAS CLI

The WAAS software CLI is organized into multiple command modes. Each command mode has its own set of commands that allow you to configure, maintain, and monitor a WAAS Wide Area Application Engine (WAE). The commands available to you at any given time depend on the mode you are in. You can enter a question mark (?) at the system prompt to obtain a list of commands available for each command mode.

The WAAS command modes include the following:

- EXEC mode—Sets, views, and tests 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—Sets, views, and tests the configuration of WAAS software features for the entire device. To use this mode, enter the **configure** command from privileged EXEC mode.
- Interface configuration mode—Sets, views, and tests the configuration of a specific interface. To use this mode, enter the **interface** command from global configuration mode.
- Standard ACL configuration mode—Creates and modifies 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—Creates and modifies 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.
- Preposition configuration mode—Creates and modifies preposition directives on a WAAS device for prepositioning files for WAFS. To use this mode, enter the **accelerator cifs preposition** command.
- Virtual blade configuration mode—Configures virtual blades that reside in a WAE or WAVE device for additional services, including operating systems and applications, that work with the WAAS device. To use this mode, enter the **virtual-blade** command.

Modes are accessed in this order: user EXEC mode, privileged EXEC mode, then global configuration mode. From global configuration mode, you can access the configuration submodes (interface configuration mode, standard ACL configuration mode, extended ACL configuration mode, preposition configuration mode, and virtual blade mode).

## Using EXEC Mode

Use the EXEC mode to set, view, and test system operations. 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.

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.

### EXEC Mode Levels

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.

- User level—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.
- Privileged level—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. The following example shows how to access the privileged-level EXEC command line from the user level:

```
WAE> enable
WAE#
```

### EXEC Mode Command-Line Processing

Common functions you can use when entering commands in EXEC mode include the following:

- Edit—To edit commands, use the **Delete** or **Backspace** keys when you enter commands at the EXEC prompt.
- Abbreviate—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.
- Display multiple pages—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.

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

```
WAE# exit
WAE>
```

## Using Global Configuration Mode

Use global configuration mode to set, view, and test the 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 1-12. Once the configuration is saved, it is maintained across WAE reboots.

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.

You must be in global configuration mode to enter specific subordinate configuration modes.

## Configuration Submodes

Configuration submodes are used for the configuration of specific features within the scope of a given configuration mode. From global configuration mode, you can enter the following configuration submodes:

- Interface configuration mode
- Standard ACL configuration mode
- Extended ACL configuration mode
- Preposition configuration mode
- Virtual blade configuration mode

## Exiting Configuration Mode

Common functions used in configuration modes include the following:

- Exit current mode—To exit global configuration mode or any subordinate configuration mode, use the **exit** command or **Ctrl-Z**.
- Exit to privileged EXEC mode—To exit to privileged EXEC mode from global configuration mode or any subordinate configuration mode, use the **end** global configuration command:

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

## Using the Interface Configuration Mode

Use the interface configuration mode to set, view, and test 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 shows how to enter interface configuration mode:

```
WAE# configure
WAE(config)# interface ?
  GigabitEthernet Select a gigabit ethernet 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, use the **exit** command to return to global configuration mode:

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

```

## Using ACL Configuration Modes

Use the ACL configuration modes to create and modify standard and extended access list configuration on a WAAS device. From global configuration mode, you can enter the standard and extended ACL configuration modes.

- Standard—To work with a standard access list, use 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.
- Extended—To work with an extended access list, use 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, use the **exit** command to return to global configuration mode:

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

```

## Using the Preposition Configuration Mode

Use the preposition configuration mode to create and modify preposition directives on a WAAS device for prepositioning files for WAFS. To enter this mode, use the **accelerator cifs preposition** command in the global configuration mode.

To exit preposition configuration mode, use the **exit** command to return to global configuration mode:

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

```

## Using the Virtual Blade Configuration Mode

Use the virtual blade configuration mode to configure virtual blades within your WAE or WAVE device. A WAAS virtual blade acts as a computer emulator with its own virtualized CPU, memory, firmware, disk drive, CD drive, and network interface card. It works with your WAAS system to provide additional services for the users on your network.

To enter this mode, use the **virtual blade** command from the global configuration mode.

To exit virtual blade configuration mode, use the **exit** command to return to global configuration mode:

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

## 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>                   | To exit, use the <b>end</b> command.<br><br>To enter privileged EXEC mode, use the <b>enable</b> command.   |
| privileged EXEC            | From user EXEC mode, use the <b>enable</b> EXEC command.                        | WAE#                   | To return to user EXEC mode, use the <b>disable</b> command.<br><br>To enter global configuration mode, use the <b>configure</b> command.   |
| global configuration       | From privileged EXEC mode, use the <b>configure</b> command.                    | WAE(config) #          | To return to privileged EXEC mode, use the <b>exit</b> command or press <b>Ctrl-Z</b> .<br><br>To enter a configuration submode, use the specific command related to the submode. |
| interface configuration    | From global configuration mode, use the <b>interface</b> command.               | WAE(config-if) #       | To return to global configuration mode, use the <b>exit</b> command.<br><br>To return to privileged EXEC mode, use the <b>end</b> command or press <b>Ctrl-Z</b> .                |
| standard ACL configuration | From global configuration mode, use the <b>ip access-list standard</b> command. | WAE(config-std-nacl) # | To return to global configuration mode, use the <b>exit</b> command.<br><br>To return to privileged EXEC mode, use the <b>end</b> command or press <b>Ctrl-Z</b> .                |
| extended ACL configuration | From global configuration mode, use the <b>ip access-list extended</b> command. | WAE(config-ext-nacl) # | To return to global configuration mode, use the <b>exit</b> command.<br><br>To return to privileged EXEC mode, use the <b>end</b> command or press <b>Ctrl-Z</b> .                |

**Table 1-1** WAAS Command Modes Summary (continued)

| Command Mode                | Access Method  | Prompt                   | Exit Method  |
|-----------------------------|--|--------------------------|--|
| preposition configuration   | From global configuration mode, use the <b>accelerator cifs preposition</b> command. | WAE(config-preposition)# | To return to global configuration mode, use the <b>exit</b> command.<br>To return to privileged EXEC mode, use the <b>end</b> command or press <b>Ctrl-Z</b> . |
| virtual blade configuration | From global configuration mode, use the <b>virtual-blade</b> command.                | WAE(config-vb)#          | To return to global configuration mode, use the <b>exit</b> command.<br>To return to privileged EXEC mode, use the <b>end</b> command or press <b>Ctrl-Z</b> . |

## Device Mode

The WAAS software allows you 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 required by the WAAS Central Manager device.
- Application-accelerator mode—(Default) Mode for a WAAS Accelerator (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.



**Note** Because WAAS Central Manager must be deployed on a dedicated appliance, a WAAS device can operate only in one device mode: either in central-manager mode or application-accelerator mode.

The set of WAAS CLI commands that are available vary based on the device mode of the WAAS device.

## Changing the Device Mode

To change the device mode of a WAAS device, use the **device mode** global configuration command as follows:

```
waas-cm(config)# device mode ?
application-accelerator Configure device to function as a WAAS Engine.
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
```

## Displaying the Configured Device Mode

You can display the configured device mode for a change that has not taken effect by using the **show device-mode configured** EXEC command.

For example, if you changed the device mode to central-manager on a WAAS device (using the **device mode central-manager** global configuration command), but did not save the running configuration (using the **copy run start** EXEC command) then, even though the new device mode has not taken effect, the output for the **show device-mode configured** command would indicate that the configured device mode is central-manager:

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

# 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 <sup>1</sup> | 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 <sup>1</sup>  | Enters the next command line in the history buffer.                                  |
| Ctrl-P or the Up Arrow key <sup>1</sup>    | 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. |

**■ Checking Command Syntax****Table 1-2 Command-Line Processing Keystroke Combinations (continued)**

| Keystroke Combinations      | Function  |
|-----------------------------|---|
| 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; you must 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 caret symbol (^) indicates that you have entered an incorrect command, keyword, or argument at a specific point in the command string.

To set the clock, for example, you can 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. You can then 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 reenter 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# cl?
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.

# WAAS Directories on a WAE

This section describes how to navigate the WAAS directories on a WAE and provides directory descriptions useful for troubleshooting and monitoring the WAE.

## Navigating WAAS Directories

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  |
|-------------------------------|--|
| <b>cd</b> [directory-name]    | Change Directory—Moves you from the current directory to the specified directory in the WAAS tree. If no directory is specified, <b>cd</b> takes you up one directory.   |
| <b>deltree</b> directory-name | Remove Directory Tree—Deletes the specified directory and all subdirectories and files without displaying a warning message to you.  |
| <b>dir</b> [directory-name]   | 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 <b>lls</b> command.         |
| <b>ls</b> [directory-name]    | Show Directory Names—Lists the names of directories in the current directory path.   |
| <b>lls</b> [directory-name]   | 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 <b>dir</b> command. |
| <b>mkdir</b> directory-name   | Create Directory—Creates a directory of the specified name in the current directory path.  |

**Table 1-3** WAAS Navigation Commands (continued)

| Command                     | Description   |
|-----------------------------|---|
| <b>pwd</b>                  | Present Working Directory—Lists the complete path from where this command is entered.   |
| <b>rmdir directory-name</b> | 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   |
|---------------------|--|
| actona              | This directory contains the current software image installed on the WAAS device and any previous images that were installed.   |
| logs                | This directory contains application-specific logs used in troubleshooting. The <i>actona</i> subdirectory contains the commonly used Manager.log, Utilities.log, and Watchdog.log log files. See the <i>Cisco Wide Area Application Services Configuration Guide</i> for more details about how these log files are used.  |
| syslog.txt          | 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 <b>show tech-support</b> 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   |
|--|---|
| <b>copy {source   image}</b>   | Copy—Copies the selected source file, image, or configuration information: <ul style="list-style-type: none"> <li>• cdrom—Copies the file from the CDROM.</li> <li>• compactflash—Copies the file from the CompactFlash card.</li> <li>• disk—Copies the configuration or file from the disk.</li> <li>• ftp—Copies the file from the FTP server.</li> <li>• http—Copies the file from the HTTP server.</li> <li>• running-config—Copies information from the current system configuration.</li> <li>• startup-config—Copies information from the startup configuration.</li> <li>• sysreport—Copies system information.</li> <li>• system-status—Copies the system status for debugging reference.</li> <li>• tech-support—Copies system information for technical support.</li> <li>• tftp—Copies the software image from the TFTP server.</li> </ul> |
| <b>cpfile source-filename destination-filename</b>                                     | Copy File—Makes a copy of a source file, and puts it in the current directory.  |
| <b>delfile filename</b>  | Remove File—Deletes the specified file from the current directory path.   |
| <b>less filename</b>   | Display File Using LESS—Displays the specified file on the screen using the LESS program. The filename is case sensitive. Enter <b>q</b> to stop viewing the file and return to the directory.  |
| <b>mkfile filename</b>   | Create File—Creates a file of the specified name in the current directory path.   |
| <b>rename old-filename new-filename</b>  | Rename File—Renames the specified file with a new filename.   |
| <b>type filename</b>   | Display File—Displays the content of the specified file on the screen.  |
| <b>type-tail filename [line   follow   {begin LINE   exclude LINE   include LINE}]</b> | 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.   |
| <b>find-pattern pattern</b>  | 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 WAAS-specific configuration on a WAE, use the **wafs EXEC** command. To save the WAAS-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 4.1.1 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.

**Table 2-1      Command Summary**

| <b>Command</b>                        | <b>Description</b>   | <b>CLI Mode</b>      | <b>Device Mode</b>      |
|---------------------------------------|--|----------------------|-------------------------|
| (config) aaa accounting               | Configures AAA accounting.                                       | global configuration | All                     |
| (config) accelerator cifs             | Enables the CIFS application accelerator.                        | global configuration | application-accelerator |
| (config) accelerator cifs preposition | Configures a CIFS application accelerator preposition directive. | global configuration | application-accelerator |
| (config) accelerator epm              | Enables the EPM application accelerator.                         | global configuration | application-accelerator |
| (config) accelerator http             | Enables the HTTP application accelerator.                        | global configuration | application-accelerator |
| (config) accelerator mapi             | Enables the MAPI application accelerator.                        | global configuration | application-accelerator |
| (config) accelerator nfs              | Enables the NFS application accelerator.                         | global configuration | application-accelerator |
| (config) accelerator ssl              | Enables the SSL application accelerator.                         | global configuration | application-accelerator |
| (config) accelerator video            | Enables the video application accelerator.                       | global configuration | application-accelerator |
| (config) accelerator windows-print    | Enables the Windows print accelerator                            | global configuration | application-accelerator |
| (config) alarm overload-detect        | Configures the detection of an alarm overload.                   | global configuration | All                     |

**Table 2-1** Command Summary (continued)

| <b>Command</b>                                 | <b>Description</b>  | <b>CLI Mode</b>                           | <b>Device Mode</b>      |
|--|---|---|-------------------------|
| (config) asset                                 | Configures the tag name for the asset tag string.   | global configuration                      | All                     |
| (config) authentication configuration          | Configures administrative authentication and authorization parameters.  | global configuration                      | All                     |
| (config) authentication content-request        | Configures request for content authentication and authorization parameters.   | global configuration                      | All                     |
| (config) authentication fail-over              | Configures authentication failover if the primary authentication server is unreachable.   | global configuration                      | All                     |
| (config) authentication login                  | Configures administrative login authentication and authorization parameters.  | global configuration                      | All                     |
| (config) authentication strict-password-policy | Configures strong password policy parameters.   | global configuration                      | All                     |
| (config) 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 |
| (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                     |
| (config-vb) autostart                          | Sets a virtual blade to automatically start when the WAE is started.  | virtual blade configuration               | application-accelerator |
| (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-vb) boot                               | Configures the boot image location and source for a virtual blade.  | virtual blade configuration               | application-accelerator |
| (config) bypass                                | Configures the bypass functions on a WAE.   | global configuration                      | application-accelerator |
| (config-ca) ca-certificate                     | Sets the certification authority file.  | certification authority configuration     | All                     |
| 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                     |

**Table 2-1** *Command Summary (continued)*

| <b>Command</b>               | <b>Description</b>   | <b>CLI Mode</b>                           | <b>Device Mode</b>      |
|------------------------------|--|---|-------------------------|
| cifs                         | Controls CIFS adapter operations and run-time configurations.                                      | user-level EXEC and privileged-level EXEC | application-accelerator |
| (config-cipher-list) cipher  | Configures a cipher suite on the cipher list.  | cipher list configuration                 | All                     |
| clear arp-cache              | Resets the ARP cache.  | privileged-level EXEC                     | All                     |
| clear cache                  | Resets the cached objects.   | privileged-level EXEC                     | All                     |
| clear cdp                    | Resets Cisco Discovery Protocol statistics.  | privileged-level EXEC                     | All                     |
| clear ip                     | Resets IP access list statistics.  | privileged-level EXEC                     | All                     |
| clear license                | Resets licensing configuration.  | privileged-level EXEC                     | All                     |
| clear logging                | Resets the syslog messages saved in a disk file.   | privileged-level EXEC                     | All                     |
| clear statistics             | Resets statistics data.  | privileged-level EXEC                     | All                     |
| clear statistics accelerator | Resets all global statistics.  | privileged-level EXEC                     | All                     |
| clear statistics connection  | Resets connection statistics.  | privileged-level EXEC                     | All                     |
| clear transaction-log        | Archives the working transaction log file.   | privileged-level EXEC                     | All                     |
| clear users                  | Resets user connections or unlocks users that have been locked out.                                | privileged-level EXEC                     | All                     |
| clear windows-domain-log     | Clears user connections and unlocks users that have been locked out.                               | 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                     |
| cms secure-store             | Configures secure store encryption   | privileged-level EXEC                     | All                     |
| (config) cms                 | Schedules the maintenance and enables the Centralized Management System on a specific WAAS device. | global configuration                      | 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 cdrom wow-recovery      | Recovers Windows on a virtual blade without reloading the software.                                | 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)

| <b>Command</b>                                | <b>Description</b>  | <b>CLI Mode</b>           | <b>Device Mode</b>      |
|---|---|---------------------------|-------------------------|
| <code>copy startup-config</code>              | Copies information from the startup configuration.  | privileged-level EXEC     | All                     |
| <code>copy sysreport</code>                   | Copies system troubleshooting information.  | privileged-level EXEC     | All                     |
| <code>copy system-status</code>               | Copies the system status for debugging reference.   | privileged-level EXEC     | All                     |
| <code>copy tech-support</code>                | Copies system information for technical support.  | privileged-level EXEC     | All                     |
| <code>copy tftp</code>                        | Copies the software image from the TFTP server.   | privileged-level EXEC     | All                     |
| <code>copy virtual-blade</code>               | Copies software configuration or image data from a virtual blade disk image to an FTP server. | privileged-level EXEC     | All                     |
| <code>cfile</code>                            | Copies a file to the current directory.   | privileged-level EXEC     | All                     |
| <code>(config-preposition) credentials</code> | Sets the username and password credentials.   | preposition configuration | application-accelerator |
| <code>crypto delete</code>                    | Removes SSL certificate and key files.  | privileged-level EXEC     | application-accelerator |
| <code>crypto export</code>                    | Exports SSL certificate and key files.  | privileged-level EXEC     | application-accelerator |
| <code>crypto generate</code>                  | Generates a self-signed certificate or a certificate signing request.                         | privileged-level EXEC     | All                     |
| <code>crypto import</code>                    | Imports SSL certificate and key files.  | privileged-level EXEC     | application-accelerator |
| <code>crypto pki</code>                       | Initializes the PKI managed store.  | privileged-level EXEC     | All                     |
| <code>(config) crypto pki</code>              | Configures public key infrastructure (PKI) encryption parameters.                             | global configuration      | All                     |
| <code>(config) crypto ssl</code>              | Configures secure sockets layer (SSL) encryption parameters.                                  | global configuration      | All                     |
| <code>debug aaa accounting</code>             | Configures AAA accounting debugging.  | privileged-level EXEC     | All                     |
| <code>debug accelerator</code>                | Configures accelerator debugging.   | privileged-level EXEC     | All                     |
| <code>debug all</code>                        | Configures all debugging.   | privileged-level EXEC     | All                     |
| <code>debug authentication</code>             | Configures authentication debugging.  | privileged-level EXEC     | All                     |
| <code>debug buf</code>                        | Configures buffer manager debugging.  | privileged-level EXEC     | All                     |
| <code>debug cdp</code>                        | Configures CDP debugging.   | privileged-level EXEC     | All                     |
| <code>debug cli</code>                        | Configures CLI debugging.   | privileged-level EXEC     | All                     |
| <code>debug cms</code>                        | Configures CMS debugging.   | privileged-level EXEC     | All                     |
| <code>debug dataserver</code>                 | Configures data server debugging.   | privileged-level EXEC     | All                     |
| <code>debug dhcp</code>                       | Configures DHCP debugging.  | privileged-level EXEC     | All                     |
| <code>debug dre</code>                        | Configures DRE debugging.   | privileged-level EXEC     | application-accelerator |

**Table 2-1** **Command Summary (continued)**

| <b>Command</b>                        | <b>Description</b>   | <b>CLI Mode</b>                       | <b>Device Mode</b>      |
|---------------------------------------|--|---------------------------------------|-------------------------|
| <code>debug egress-method</code>      | Configures egress method debugging.  | privileged-level EXEC                 | application-accelerator |
| <code>debug emdb</code>               | Configures embedded database debugging.  | privileged-level EXEC                 | All                     |
| <code>debug epm</code>                | Configures DCE-RPC EPM debugging.  | privileged-level EXEC                 | application-accelerator |
| <code>debug flow</code>               | Configures network traffic flow debugging.   | privileged-level EXEC                 | All                     |
| <code>debug generic-gre</code>        | Configures generic GRE egress method debugging.  | privileged-level EXEC                 | All                     |
| <code>debug key-manager</code>        | Configures Central Manager key manager debugging.  | privileged-level EXEC                 | All                     |
| <code>debug logging</code>            | Configures logging debugging.  | privileged-level EXEC                 | All                     |
| <code>debug ntp</code>                | Configures NTP debugging.  | privileged-level EXEC                 | All                     |
| <code>debug print-spooler</code>      | Configures print spooler debugging.  | privileged-level EXEC                 | application-accelerator |
| <code>debug rbcpc</code>              | Configures RBCP debugging.   | privileged-level EXEC                 | All                     |
| <code>debug rpc</code>                | Configures record remote procedure calls debugging.  | privileged-level EXEC                 | All                     |
| <code>debug snmp</code>               | Configures SNMP debugging.   | privileged-level EXEC                 | All                     |
| <code>debug stats</code>              | Configures statistics debugging.   | privileged-level EXEC                 | All                     |
| <code>debug tfo</code>                | Configures TFO flow optimization debugging.  | privileged-level EXEC                 | application-accelerator |
| <code>debug translog</code>           | Configures transaction logging debugging.  | privileged-level EXEC                 | All                     |
| <code>debug wafs</code>               | Sets the log level of WAFS running components.   | privileged-level EXEC                 | application-accelerator |
| <code>debug wccp</code>               | Configures WCCP information debugging.   | privileged-level EXEC                 | application-accelerator |
| <code>(config-std-nacl) delete</code> | Deletes a line from the standard ACL.  | standard ACL configuration            | All                     |
| <code>(config-ext-nacl) delete</code> | Deletes a line from the extended ACL.  | extended ACL configuration            | All                     |
| <code>delfile</code>                  | Deletes a file.  | privileged-level EXEC                 | All                     |
| <code>deltree</code>                  | Deletes a directory and its subdirectories.  | privileged-level EXEC                 | All                     |
| <code>(config-std-nacl) deny</code>   | 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                     |
| <code>(config-ext-nacl) deny</code>   | 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                     |
| <code>(config-ca) description</code>  | Configures a description for the certification authority.  | certification authority configuration | All                     |

**Table 2-1** Command Summary (continued)

| <b>Command</b>                  | <b>Description</b>  | <b>CLI Mode</b>                           | <b>Device Mode</b>      |
|---------------------------------|---|---|-------------------------|
| (config-vb) description         | Configures a description for a virtual blade on your WAE.                           | virtual blade configuration               | application-accelerator |
| (config-vb) device              | Configures the device emulation parameters used by the virtual blade on your WAE.   | virtual blade configuration               | application-accelerator |
| (config) device mode            | Specifies the device mode of the WAAS device.                                       | global configuration                      | All                     |
| dir                             | Displays the files in a long list format.   | user-level EXEC and privileged-level EXEC | All                     |
| (config) directed-mode          | Configures the mode by which traffic is sent between two WAEs.                      | global configuration                      | application-accelerator |
| disable                         | Turns off the privileged EXEC commands.   | privileged-level EXEC                     | All                     |
| disk                            | Configures the disks on the WAAS device.  | privileged-level EXEC                     | All                     |
| (config-vb) disk                | Configures disk space for a virtual blade on the WAE hard drive.                    | virtual blade configuration               | application-accelerator |
| (config) disk disk-name         | Disables a RAID-1 disk for online removal.  | global configuration                      | All                     |
| (config) disk encrypt           | Enables disk encryption.  | global configuration                      | application-accelerator |
| (config) disk error-handling    | Configures how the disk errors should be handled.                                   | global configuration                      | All                     |
| (config) disk logical shutdown  | Shuts down the RAID-5 logical disk drive.   | global configuration                      | All                     |
| dnslookup                       | Resolves a DNS hostname.  | user-level EXEC and privileged-level EXEC | All                     |
| (config-preposition) dscp       | Sets the DSCP marking value for a preposition task.                                 | preposition configuration                 | application-accelerator |
| (config-preposition) duration   | Sets the maximum duration for a preposition task.                                   | preposition configuration                 | application-accelerator |
| (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-preposition) enable     | Enables or disables a preposition directive.  | preposition configuration                 | application-accelerator |
| (config-if) encapsulation dot1Q | Sets the VLAN ID of traffic leaving the Cisco WAE Inline Network Adapter interface. | interface configuration                   | application-accelerator |
| (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                     |

**Table 2-1** **Command Summary (continued)**

| <b>Command</b>                           | <b>Description</b>  | <b>CLI Mode</b>                           | <b>Device Mode</b>      |
|--|---|---|-------------------------|
| (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-if) failover timeout             | Configures the maximum time for the inline interface to transition traffic to another port after a failure event. | interface configuration                   | All                     |
| 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                     |
| 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-preposition) ignore-hidden-dir   | Configures to ignore hidden directories in the set of files to be prepositioned.                                  | preposition configuration                 | application-accelerator |
| (config) inetd                           | Enables FTP, RCP, and TFTP services.  | global configuration                      | All                     |
| (config-if) inline                       | Configures inline interception for an inlineGroup interface.  | interface configuration                   | All                     |
| (config) inline vlan-id-connection-check | Enables VLAN ID checking on intercepted traffic.  | global configuration                      | All                     |
| install                                  | Installs a new image into Flash memory.   | privileged-level EXEC                     | All                     |
| (config-vb) interface                    | Bridges a virtual blade interface to an interface on your WAE.  | virtual blade configuration               | application-accelerator |
| (config) interface GigabitEthernet*      | Configures a Gigabit Ethernet interface. Provides access to interface configuration mode.                         | global configuration                      | All                     |
| (config) interface InlineGroup*          | Configures a Inline Group channel, or standby interface. Provides access to interface configuration mode.         | global configuration                      | All                     |
| (config) interface PortChannel*          | Configures a port channel interface. Provides access to interface configuration mode.                             | global configuration                      | All                     |
| (config) interface standby*              | Configures a standby interface. Provides access to interface configuration mode.                                  | global configuration                      | All                     |

**Table 2-1** Command Summary (continued)

| <b>Command</b>                 | <b>Description</b>  | <b>CLI Mode</b>                           | <b>Device Mode</b>      |
|--------------------------------|---|---|-------------------------|
| (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 or Cisco WAE Inline Network Adapter. | 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                     |
| (config) kernel kdump          | Enables the kernel crash dump mechanism.  | global configuration                      | All                     |
| less                           | Displays the contents of a file using the LESS application.   | user-level EXEC and privileged-level EXEC | All                     |
| license add                    | Adds a software license.  | 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 console       | Configures system logging (syslog) to the console.  | global configuration                      | All                     |
| (config) logging disk          | Configures system logging (syslog) to a disk file.  | global configuration                      | All                     |
| (config) logging facility      | Sets the facility parameter for system logging (syslog).  | global configuration                      | All                     |
| (config) logging host          | Configures system logging (syslog) to a remote host.  | global configuration                      | All                     |
| ls                             | Lists the files and subdirectories in a directory.  | user-level EXEC and privileged-level EXEC | All                     |
| (config-preposition) max-cache | Sets the maximum cache percentage that prepositioned files can use.   | preposition configuration                 | application-accelerator |

**Table 2-1** **Command Summary (continued)**

| <b>Command</b>  | <b>Description</b>  | <b>CLI Mode</b>                           | <b>Device Mode</b>      |
|---|---|---|-------------------------|
| (config-preposition) max-file-size                            | Sets the maximum size of a prepositioned file.  | preposition configuration                 | application-accelerator |
| (config-vb) memory  | Configures memory for a virtual blade from the WAE system.  | virtual blade configuration               | application-accelerator |
| (config-preposition) min-file-size                            | Sets the minimum size of a prepositioned file.  | preposition configuration                 | application-accelerator |
| mkdir   | Makes a directory.  | privileged-level EXEC                     | All                     |
| mkfile  | Makes a file (for testing).   | 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-preposition) name                                     | Sets the name of a preposition directive.   | preposition configuration                 | application-accelerator |
| (config) ntp  | Configures the NTP server.  | global configuration                      | All                     |
| ntpdate   | Sets the NTP server name.   | privileged-level EXEC                     | All                     |
| (config-pki-global-settings) ocsp                             | Configures the URL to be used as the global settings for the Online Certificate Status Protocol (OCSP) protocol revocation status checking. | PKI global-settings configuration         | All                     |
| (config-preposition) pattern                                  | Sets a file filter for a preposition directive.   | preposition configuration                 | application-accelerator |
| (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 |

**Table 2-1** Command Summary (continued)

| Command  | Description   | CLI Mode                                  | Device Mode             |
|--|---|---|-------------------------|
| (config) policy-engine application map basic               | 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 other optimize DRE  | Configures the WAE's <b>optimize DRE</b> command action for nonclassified traffic.                                | global configuration                      | application-accelerator |
| (config) policy-engine application map other optimize full | Configures the application policy for nonclassified traffic with the <b>optimize full</b> command action.         | global configuration                      | application-accelerator |
| (config) policy-engine application map other pass-through  | Configures the application policy for nonclassified traffic with the <b>pass-through</b> 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 application set-dscp                | Sets the default DSCP marking value.  | 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                     |
| (config-preposition) recursive                             | Enables or disables recursion for a preposition directive.  | preposition configuration                 | application-accelerator |
| reload   | Halts a device and performs a cold restart.   | privileged-level EXEC                     | All                     |
| rename   | Renames a file.   | privileged-level EXEC                     | All                     |
| restore  | Restores a device to its manufactured default status.   | privileged-level EXEC                     | All                     |
| (config-ca) revocation-check                               | Configures the certification authority revocation checking method.  | certification authority configuration     | All                     |
| (config-pki-global-settings) revocation-check              | Configures the global settings revocation checking method.  | PKI global-settings configuration         | All                     |
| rmdir  | Removes a directory.  | privileged-level EXEC                     | All                     |

**Table 2-1** **Command Summary (continued)**

| <b>Command</b>                 | <b>Description</b>  | <b>CLI Mode</b>                           | <b>Device Mode</b>      |
|--------------------------------|---|---|-------------------------|
| (config-preposition) root      | Sets the root directory for a preposition directive.                                | preposition configuration                 | application-accelerator |
| (config-preposition) scan-type | Sets the file scanning type for a preposition directive.                            | preposition configuration                 | application-accelerator |
| (config-preposition) schedule  | Sets the schedule for a preposition directive.                                      | preposition configuration                 | application-accelerator |
| scp                            | Specifies the SCP client.   | privileged-level EXEC                     | All                     |
| script                         | Checks the errors in a script or executes a script.                                 | privileged-level EXEC                     | All                     |
| (config-preposition) server    | Sets the file server for a preposition directive.                                   | preposition configuration                 | application-accelerator |
| 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 accelerator               | Displays the status and configuration of the application accelerators.              | user-level EXEC and privileged-level EXEC | 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                     |
| show authentication            | Displays the authentication configuration.  | user-level EXEC and privileged-level EXEC | All                     |
| show auto-discovery            | Displays auto-discovery information for a WAE.                                      | user-level EXEC and privileged-level EXEC | application-accelerator |
| show auto-register             | Displays the status of the autoregistration feature for a WAE.                      | privileged-level EXEC                     | application-accelerator |
| show banner                    | Displays the message of the day, login, and EXEC banner settings.                   | privileged-level EXEC                     | All                     |
| 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 cms secure-store          | Displays the secure disk encryption status.   | privileged-level EXEC                     | All                     |
| show crypto                    | Displays crypto layer information.  | user-level EXEC and privileged-level EXEC | All                     |

**Table 2-1** Command Summary (continued)

| <b>Command</b>                              | <b>Description</b>   | <b>CLI Mode</b>                           | <b>Device Mode</b>      |
|---|--|---|-------------------------|
| <code>show debugging</code>                 | Displays the state of each debugging option.   | user-level EXEC and privileged-level EXEC | All                     |
| <code>show device-mode</code>               | Displays the device mode.  | user-level EXEC and privileged-level EXEC | All                     |
| <code>show directed-mode</code>             | Displays directed mode information.  | user-level EXEC and privileged-level EXEC | application-accelerator |
| <code>show disks</code>                     | Displays the disk configurations.  | user-level EXEC and privileged-level EXEC | All                     |
| <code>show egress-methods</code>            | 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 |
| <code>show filtering list</code>            | Displays TFO flow information for a WAE.   | user-level EXEC and privileged-level EXEC | application-accelerator |
| <code>show flash</code>                     | Displays the flash memory information.   | user-level EXEC and privileged-level EXEC | All                     |
| <code>show hardware</code>                  | Displays the system hardware information.  | user-level EXEC and privileged-level EXEC | All                     |
| <code>show hosts</code>                     | Displays the IP domain name, name servers, IP addresses, and host table.   | user-level EXEC and privileged-level EXEC | All                     |
| <code>show inetd</code>                     | Displays the status of TCP/IP services.  | user-level EXEC and privileged-level EXEC | All                     |
| <code>show interface</code>                 | Displays the hardware interface information.   | user-level EXEC and privileged-level EXEC | All                     |
| <code>show inventory</code>                 | Displays the system inventory information.   | user-level EXEC and privileged-level EXEC | All                     |
| <code>show ip access-list</code>            | Displays the information about access lists that are defined and applied to specific interfaces or applications. | user-level EXEC and privileged-level EXEC | All                     |
| <code>show ip routes</code>                 | Displays the IP routing table.   | user-level EXEC and privileged-level EXEC | All                     |
| <code>show kdump</code>                     | Displays the kernel crash dump information.  | privileged-level EXEC                     | All                     |
| <code>show kerberos</code>                  | Displays the Kerberos authentication configuration.  | user-level EXEC and privileged-level EXEC | All                     |
| <code>show license</code>                   | Displays the license information.  | user-level EXEC and privileged-level EXEC | All                     |
| <code>show logging</code>                   | Displays the system logging configuration.   | user-level EXEC and privileged-level EXEC | All                     |
| <code>show memory</code>                    | Displays the memory blocks and statistics.   | user-level EXEC and privileged-level EXEC | All                     |
| <code>show ntp</code>                       | Displays the NTP configuration status.   | user-level EXEC and privileged-level EXEC | All                     |
| <code>show policy-engine application</code> | Displays the display application policy information.   | user-level EXEC and privileged-level EXEC | application-accelerator |

**Table 2-1** **Command Summary (continued)**

| <b>Command</b>   | <b>Description</b>  | <b>CLI Mode</b>                           | <b>Device Mode</b>      |
|--|---|---|-------------------------|
| <code>show policy-engine status</code>                 | 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 |
| <code>show print-services</code>                       | Displays the print services administrator and process information.  | user-level EXEC and privileged-level EXEC | All                     |
| <code>show processes</code>                            | Displays the process status.  | user-level EXEC and privileged-level EXEC | All                     |
| <code>show radius-server</code>                        | Displays the RADIUS server information.   | user-level EXEC and privileged-level EXEC | All                     |
| <code>show running-config</code>                       | Displays the current operating configuration.   | user-level EXEC and privileged-level EXEC | All                     |
| <code>show services</code>                             | Displays information related to services.   | user-level EXEC and privileged-level EXEC | All                     |
| <code>show smb-conf</code>                             | Displays the smb-conf configurations.   | user-level EXEC and privileged-level EXEC | All                     |
| <code>show snmp</code>                                 | Displays the SNMP statistics.   | user-level EXEC and privileged-level EXEC | All                     |
| <code>show ssh</code>                                  | Displays the status and configuration of the Secure Shell (SSH) service.  | user-level EXEC and privileged-level EXEC | All                     |
| <code>show startup-config</code>                       | Displays the startup configuration.   | user-level EXEC and privileged-level EXEC | All                     |
| <code>show statistics accelerator</code>               | Displays the application accelerator statistics information.  | user-level EXEC and privileged-level EXEC | application-accelerator |
| <code>show statistics aoinm</code>                     | Displays AO (accelerator) Information Manager statistics.   | privileged-level EXEC                     | application-accelerator |
| <code>show statistics application</code>               | Displays the status of the application statistics.  | privileged-level EXEC                     | All                     |
| <code>show statistics authentication</code>            | Displays the authentication statistics.   | user-level EXEC and privileged-level EXEC | All                     |
| <code>show statistics auto-discovery</code>            | Displays TFO auto-discovery statistics for a WAE.   | user-level EXEC and privileged-level EXEC | application-accelerator |
| <code>show statistics cifs</code>                      | Displays the CIFS statistics information.   | user-level EXEC and privileged-level EXEC | application-accelerator |
| <code>show statistics connection</code>                | Displays the connection statistics for a WAE.   | user-level EXEC and privileged-level EXEC | application-accelerator |
| <code>show statistics connection auto-discovery</code> | Displays the auto-discovery connection statistics for a WAE.  | user-level EXEC and privileged-level EXEC | application-accelerator |
| <code>show statistics connection closed</code>         | Displays the closed connection statistics for a WAE.  | user-level EXEC and privileged-level EXEC | application-accelerator |

**Table 2-1** *Command Summary (continued)*

| <b>Command</b>   | <b>Description</b>   | <b>CLI Mode</b>                           | <b>Device Mode</b>      |
|--|--|---|-------------------------|
| <code>show statistics connection conn-id</code>        | Displays the connection ID statistics for a WAE.   | user-level EXEC and privileged-level EXEC | application-accelerator |
| <code>show statistics connection egress-methods</code> | Displays detailed egress method-related information about the connection segments for a WAE. | privileged-level EXEC                     | application-accelerator |
| <code>show statistics connection optimized</code>      | Displays optimized information about the connection segments for a WAE.                      | privileged-level EXEC                     | application-accelerator |
| <code>show statistics connection pass-through</code>   | Displays pass through information about the connection segments for a WAE.                   | privileged-level EXEC                     | application-accelerator |
| <code>show statistics crypto ssl ciphers</code>        | Displays crypto SSL cipher usage statistics.   | privileged-level EXEC                     | application-accelerator |
| <code>show statistics datamover</code>                 | Displays internal datamover information.   | user-level EXEC and privileged-level EXEC | application-accelerator |
| <code>show statistics directed-mode</code>             | Displays directed mode statistics.   | user-level EXEC and privileged-level EXEC | application-accelerator |
| <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 filtering</code>                 | Displays TFO flow statistics for a WAE.  | user-level EXEC and privileged-level EXEC | application-accelerator |
| <code>show statistics flow</code>                      | Displays the flow statistics.  | user-level EXEC and privileged-level EXEC | application-accelerator |
| <code>show statistics generic-gre</code>               | Displays the generic GRE tunnel 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 netstat</code>                   | Displays the Internet socket connection statistics.  | user-level EXEC and privileged-level EXEC | All                     |
| <code>show statistics pass-through</code>              | Displays the pass-through statistics.  | user-level EXEC and privileged-level EXEC | application-accelerator |
| <code>show statistics peer</code>                      | Displays the DRE peer statistics for a WAE.  | user-level EXEC and privileged-level EXEC | application-accelerator |
| <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 synq</code>                      | Displays statistics for the SynQ module.   | user-level EXEC and privileged-level EXEC | application-accelerator |

**Table 2-1** **Command Summary (continued)**

| <b>Command</b>                                      | <b>Description</b>   | <b>CLI Mode</b>                           | <b>Device Mode</b>      |
|---|--|---|-------------------------|
| <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 statistics windows-print requests</code> | Displays the Windows print accelerator statistics.                   | user-level EXEC and privileged-level EXEC | application-accelerator |
| <code>show synq list</code>                         | Displays connections for the SynQ module.                            | user-level EXEC and privileged-level EXEC | application-accelerator |
| <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                     |
| <code>show telnet</code>                            | Displays the Telnet services configuration.                          | user-level EXEC and privileged-level EXEC | All                     |
| <code>show tfo tcp</code>                           | Displays TFO TCP buffer information.                                 | user-level EXEC and privileged-level EXEC | application-accelerator |
| <code>show transaction-logging</code>               | Displays the transaction logging information for a WAE.              | user-level EXEC and privileged-level EXEC | application-accelerator |
| <code>show user</code>                              | Displays information about a particular user.                        | user-level EXEC and privileged-level EXEC | All                     |
| <code>show users administrative</code>              | Displays the administrative users.                                   | user-level EXEC and privileged-level EXEC | All                     |
| <code>show version</code>                           | Displays the software version.                                       | user-level EXEC and privileged-level EXEC | All                     |
| <code>show virtual-blade</code>                     | Displays virtual blade information on your WAE device.               | privileged-level EXEC                     | application-accelerator |
| <code>show wccp</code>                              | Displays the WCCP information for a WAE.                             | user-level EXEC and privileged-level EXEC | application-accelerator |
| <code>show windows-domain</code>                    | Displays the Windows domain configuration.                           | user-level EXEC and privileged-level EXEC | All                     |

**Table 2-1** Command Summary (continued)

| <b>Command</b>                     | <b>Description</b>  | <b>CLI Mode</b>                           | <b>Device Mode</b> |
|------------------------------------|---|---|--------------------|
| (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                |
| (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           | 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 trap-source   | Configures the SNMP trap source.  | 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                |

**Table 2-1** **Command Summary (continued)**

| <b>Command</b>   | <b>Description</b>  | <b>CLI Mode</b>                           | <b>Device Mode</b>      |
|--|---|---|-------------------------|
| <code>telnet</code>                                    | Starts the Telnet client.   | user-level EXEC and privileged-level EXEC | All                     |
| <code>(config) telnet enable</code>                    | Enables the Telnet services.  | global configuration                      | All                     |
| <code>terminal</code>                                  | Sets the terminal output commands.  | user-level EXEC and privileged-level EXEC | All                     |
| <code>test</code>                                      | Performs diagnostic tests and displays the results.                                       | user-level EXEC and privileged-level EXEC | All                     |
| <code>tethereal</code>                                 | Analyzes network traffic from the command line.   | privileged-level EXEC                     | All                     |
| <code>(config) tfo exception</code>                    | Configures TFO exception handling.  | global configuration                      | application-accelerator |
| <code>(config) tfo optimize</code>                     | Configures TFO optimization for DRE or full generic optimization on the WAE.              | global configuration                      | application-accelerator |
| <code>(config) tfo tcp adaptive-buffer-sizing</code>   | Configures TFO optimization with TCP adaptive buffer sizing.                              | global configuration                      | application-accelerator |
| <code>(config) tfo tcp keepalive</code>                | Configures TFO optimization with a TCP keepalive on a WAE.                                | global configuration                      | application-accelerator |
| <code>(config) tfo tcp optimized-mss</code>            | Configures TFO optimization with an optimized-side TCP maximum segment size on a WAE.     | global configuration                      | application-accelerator |
| <code>(config) tfo tcp optimized-receive-buffer</code> | Configures TFO optimization with an optimized-side receive buffer on a WAE.               | global configuration                      | application-accelerator |
| <code>(config) tfo tcp optimized-send-buffer</code>    | Configures TFO optimization with an optimized-side send buffer on a WAE.                  | global configuration                      | application-accelerator |
| <code>(config) tfo tcp original-mss</code>             | Configures TFO optimization with an unoptimized-side TCP maximum segment size on the WAE. | global configuration                      | application-accelerator |
| <code>(config) tfo tcp original-receive-buffer</code>  | Configures TFO optimization with an unoptimized-side receive buffer on a WAE.             | global configuration                      | application-accelerator |
| <code>(config) tfo tcp original-send-buffer</code>     | Configures TFO optimization with an unoptimized-side send buffer on a WAE.                | global configuration                      | application-accelerator |
| <code>traceroute</code>                                | Traces the route to a remote host.  | user-level EXEC and privileged-level EXEC | All                     |
| <code>transaction-log</code>                           | Forces the transaction logging for TFO and export on a WAE.                               | privileged-level EXEC                     | application-accelerator |
| <code>(config) transaction-logs</code>                 | Configures the transaction logging on a WAE.  | global configuration                      | application-accelerator |
| <code>type</code>                                      | Displays a file.  | user-level EXEC and privileged-level EXEC | All                     |
| <code>type-tail</code>                                 | Displays the last several lines of a file.  | user-level EXEC and privileged-level EXEC | All                     |
| <code>(config) username</code>                         | Establishes the username authentication.  | global configuration                      | All                     |

**Table 2-1** Command Summary (continued)

| <b>Command</b>   | <b>Description</b>  | <b>CLI Mode</b>                           | <b>Device Mode</b>      |
|--|---|---|-------------------------|
| <code>virtual-blade</code>                                 | Executes general operations on a virtual blade.   | privileged-level EXEC                     | application-accelerator |
| <code>(config) virtual-blade</code>                        | Configures virtual blades on your WAE device.   | global configuration                      | All                     |
| <code>(config-vb) vnc</code>                               | Enables or disables the VNC server for the virtual blade on your WAE.   | virtual blade configuration               | application-accelerator |
| <code>wafs</code>  | Performs a backup or restores system configuration, and creates a system report on a WAE.   | privileged-level EXEC                     | application-accelerator |
| <code>(config) wccp access-list</code>                     | Configures the IP access list for inbound Web Cache Coordination Protocol (WCCP) GRE-encapsulated traffic on a WAE.                 | global configuration                      | application-accelerator |
| <code>(config) wccp flow-redirect</code>                   | Enables the WCCP flow redirection on a WAE.   | global configuration                      | application-accelerator |
| <code>(config) wccp router-list</code>                     | Creates a router list on a WAE for use in the WCCP Version 2 services.  | global configuration                      | application-accelerator |
| <code>(config) wccp shutdown</code>                        | Sets the maximum time interval after which the WAE will perform a clean shut down.  | global configuration                      | application-accelerator |
| <code>(config) wccp tcp-promiscuous mask</code>            | Configures the TCP promiscuous mode service (WCCP Version 2 services 61 and 62) on a WAE.   | global configuration                      | application-accelerator |
| <code>(config) wccp tcp-promiscuous router-list-num</code> | Configures the TCP promiscuous mode service (WCCP Version 2 services 61 and 62) router list 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 that 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 “[Global Configuration Mode Commands](#)” section for a complete listing of commands.
- Interface configuration mode commands that you can enter after you access interface 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 the standard or extended ACL configuration modes. See the “[Standard ACL Configuration Mode Commands](#)” and “[Extended ACL Configuration Mode Commands](#)” sections for a complete listing of commands.
- Preposition configuration mode commands that you can enter after you access the preposition configuration mode. See the “[Preposition Configuration Mode Commands](#)” section for a complete listing of commands.
- Virtual blade configuration mode commands that you can enter after you access virtual blade configuration mode. See the “[Virtual Blade Configuration Mode Commands](#)” section for a complete listing of commands.
- PKI Certificate Authority configuration mode commands that you can enter after you access virtual blade configuration mode. See the “[PKI Certificate Authority Configuration Mode Commands](#)” section for a complete listing of commands.
- PKI Global Settings configuration mode commands that you can enter after you access virtual blade configuration mode. See the “[PKI Global Settings Configuration Mode Commands](#)” section for a complete listing of commands.
- SSL Cipher List configuration mode commands that you can enter after you access virtual blade configuration mode. See the “[SSL Cipher List Configuration Mode Commands](#)” section 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.

The following example shows how to access 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**

# cd

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

**cd** *directoryname*

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

|                 |                                |
|-----------------|--------------------------------|
| <b>Defaults</b> | No default behavior or values. |
|-----------------|--------------------------------|

|                      |      |
|----------------------|------|
| <b>Command Modes</b> | EXEC |
|----------------------|------|

|                     |  |
|---------------------|--|
| <b>Device Modes</b> | application-accelerator<br>central-manager |
|---------------------|--|

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

|                 |   |
|-----------------|---|
| <b>Examples</b> | 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
```

|                         |   |
|-------------------------|---|
| <b>Related Commands</b> | <a href="#">deltree</a><br><a href="#">dir</a><br><a href="#">lls</a><br><a href="#">ls</a><br><a href="#">mkdir</a><br><a href="#">pwd</a> |
|-------------------------|---|

# cifs

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

```
cifs auto-discovery {disable | enable | reset-log}

cifs mss value

cifs restart [core | edge]

cifs reverse-dns {active | disable | enable}

cifs session disconnect [client-ip ipaddress | server-ip ipaddress]
```

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

|          |                                |
|----------|--------------------------------|
| Defaults | No default behavior or values. |
|----------|--------------------------------|

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

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

|                  |   |
|------------------|---|
| Usage Guidelines | This command controls legacy mode WAFS. To control the transparent CIFS accelerator, use the <b>(config) accelerator cifs</b> command. These two modes are mutually exclusive. For more information on the two WAFS modes, see the chapter “Configuring Wide Area File Services” in the <i>Cisco Wide Area Application Services Configuration Guide</i> . |
|------------------|---|

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

**cifs****Examples**

The following example shows how to set the TCP maximum segment size (MSS) value to 512 for the CIFS adapter:

```
WAE# cifs mss 512
```

**Related Commands**

[show cifs](#)

[show statistics cifs](#)

# clear arp-cache

To clear the ARP cache, use the **clear arp-cache** EXEC command.

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

## Syntax Description

|                                 |   |
|---------------------------------|---|
| <b>arp-cache</b>                | Clears the ARP cache.                               |
| <i>ipaddress</i>                | (Optional) ARP entries for the IP address.          |
| <b>interface</b>                | (Optional) Clears all ARP entries on the interface. |
| <b>GigabitEthernet 1-2/port</b> | GigabitEthernet interface (slot/port).              |
| <b>PortChannel 1-2</b>          | PortChannel interface number. Values are 1 or 2     |
| <b>Standby 1-4</b>              | Standby interface number 1, 2, 3, or 4.             |

## Defaults

No default behavior or values.

## Command Modes

EXEC

## Device Modes

application-accelerator  
central-manager

## Examples

The following example shows how to clear the ARP cache on the WAAS device:

```
WAE# clear arp-cache
```

## Related Commands

[license add](#)  
[show interface](#)  
[show license](#)  
[show wccp](#)

**■ clear cache**

## clear cache

To clear cached objects, use the **clear cache** EXEC command.

```
clear cache {cifs | dre}
```

|                           |                        |
|---------------------------|------------------------|
| <b>Syntax Description</b> |                        |
| <b>cache</b>              | Clears cached objects. |
| <b>cifs</b>               | Clears the CIFS cache. |

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator  
central-manager

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

**Examples** The following example shows how to clear the CIFS cached objects on the WAAS device:

```
WAE# clear cache cifs
```

**Related Commands**

- [license add](#)
- [show interface](#)
- [show license](#)
- [show wecp](#)

# clear cdp

To clear Cisco Discovery Protocol statistics, use the **clear cdp** EXEC command.

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

| Syntax Description |   |
|--------------------|---|
| <b>cdp</b>         | Resets the Cisco Discovery Protocol (CDP) statistical data. |
| <b>counters</b>    | Clears the CDP counters.                                    |
| <b>table</b>       | Clears the CDP tables.                                      |

|          |                                |
|----------|--------------------------------|
| Defaults | No default behavior or values. |
|----------|--------------------------------|

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

|              |  |
|--------------|--|
| Device Modes | application-accelerator<br>central-manager |
|--------------|--|

|          |   |
|----------|---|
| Examples | The following example shows how to clear the CDP counter statistics on the WAAS device: |
|----------|---|

```
WAE# clear cdp counters
```

|                  |  |
|------------------|--|
| Related Commands | <a href="#">license add</a><br><a href="#">show interface</a><br><a href="#">show license</a><br><a href="#">show wccp</a> |
|------------------|--|

**clear ip**

# clear ip

To clear IP access list statistics, use the **clear ip** EXEC command.

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

---

## Syntax Description

|                    |  |
|--------------------|--|
| <b>ip</b>          | Clears the IP statistical information.   |
| <b>access-list</b> | Clears the access list statistical information.  |
| <b>counters</b>    | 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.       |

---



---

## Defaults

No default behavior or values.

---

## Command Modes

EXEC

---

## Device Modes

application-accelerator  
central-manager

---

## Examples

The following example shows how to clear the IP access list counters on the WAAS device:

```
WAE# clear ip access-list counters
```

---

## Related Commands

[license add](#)  
[show interface](#)  
[show license](#)  
[show wccp](#)

# clear license

To clear licensing configuration, use the **clear license** EXEC command.

**clear license [license-name]**

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | <b>license</b> Removes all installed software licenses, when specified without options.<br><b>license-name</b> Name of the software license to remove. The following license names are supported:  |
|                           | <ul style="list-style-type: none"> <li>• Transport—Enables basic DRE, TFO, and LZ optimization.</li> <li>• Enterprise—Enables the EPM, HTTP, MAPI, NFS, SSL, CIFS (WAFS), and Windows Print application accelerators, the WAAS Central Manager, and basic DRE, TFO, and LZ optimization. You cannot remove this license if the video or virtualization licenses are installed. You must remove both of those licenses first.</li> <li>• Video—Enables the video application accelerator.</li> <li>• Virtual-Blade—Enables the virtualization feature.</li> </ul> |
| <b>Defaults</b>           | No default behavior or values.   |
| <b>Command Modes</b>      | EXEC   |
| <b>Device Modes</b>       | application-accelerator<br>central-manager   |
| <b>Examples</b>           | <p>The following example shows how to clear the licensing configuration on the WAAS device:</p> <pre>WAE# clear license</pre>  |
| <b>Related Commands</b>   | <a href="#">license add</a><br><a href="#">show interface</a><br><a href="#">show license</a><br><a href="#">show wccp</a>   |

**clear logging**

# clear logging

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

**clear logging**

|                           |   |  |
|---------------------------|---|--|
| <b>Syntax Description</b> | <b>logging</b>  | Clears the syslog messages saved in the disk file. |
| <b>Defaults</b>           | No default behavior or values.  |  |
| <b>Command Modes</b>      | EXEC  |  |
| <b>Device Modes</b>       | application-accelerator<br>central-manager  |  |
| <b>Usage Guidelines</b>   | The <b>clear logging</b> command removes all current entries from the <i>syslog.txt</i> file but does not make an archive of the file. It puts a “Syslog cleared” message in the <i>syslog.txt</i> file to indicate that the syslog has been cleared. |  |
| <b>Examples</b>           | The following example shows how to clear all entries in the <i>syslog.txt</i> file on the WAAS device:<br><br>WAE# <b>clear logging</b><br><br>Feb 14 12:17:18 WAE# exec_clear_logging:Syslog cleared   |  |
| <b>Related Commands</b>   | <a href="#">license add</a><br><a href="#">show interface</a><br><a href="#">show license</a><br><a href="#">show wcep</a>  |  |

# clear statistics

To reset statistics data, use the **clear statistics** EXEC command.

```
clear statistics {all | aoim | authentication | auto-discovery {all | blacklist} | datamover |
    directed-mode | dre [global] | filtering | flow monitor tcpstat-v1 | generic-gre | icmp | inline |
    ip | pass-through | peer dre | radius | synq | tacacs | tcp | tfo | udp | wccp | windows-domain |
    windows-print}
```

| Syntax Description    |   |
|-----------------------|---|
| <b>all</b>            | Clears all statistics.  |
| <b>authentication</b> | Clears authentication statistics.   |
| <b>auto-discovery</b> | Clears the auto-discovery statistics.                                     |
| <b>all</b>            | Clears all of the auto-discovery statistics.                              |
| <b>aoim</b>           | Clears all of the application accelerator information manager statistics. |
| <b>blacklist</b>      | Clears the auto-discovery statistics for the blacklist.                   |
| <b>datamover</b>      | Clears all of the data mover statistics.                                  |
| <b>directed-mode</b>  | Clears the directed mode statistics.                                      |
| <b>dre</b>            | Clears the Data Redundancy Elimination (DRE) statistics.                  |
| <b>global</b>         | Clears the global DRE statistics.   |
| <b>filtering</b>      | Clears the filter table statistics.                                       |
| <b>flow</b>           | Clears the network traffic flow statistics.                               |
| <b>monitor</b>        | Clears the monitor flow performance statistics.                           |
| <b>tcpstat-v1</b>     | Clears the tcpstat-v1 collector statistics.                               |
| <b>generic-gre</b>    | Clears the generic GRE statistics.  |
| <b>icmp</b>           | Clears the ICMP statistics.   |
| <b>inline</b>         | Clears the inline interception statistics.                                |
| <b>ip</b>             | Clears the IP statistics.   |
| <b>pass-through</b>   | Clears all of the pass-through statistics.                                |
| <b>peer dre</b>       | Clears all peer DRE statistics.   |
| <b>radius</b>         | Clears the RADIUS statistics.   |
| <b>synq</b>           | Clears the SynQ module statistics.  |
| <b>tacacs</b>         | Clears the TACACS+ statistics.  |
| <b>tcp</b>            | Clears the TCP statistics.  |
| <b>tfo</b>            | Clears the TCP flow optimization (TFO) statistics.                        |
| <b>udp</b>            | Clears the UDP statistics.  |
| <b>wccp</b>           | Clears all of the WCCP statistics.  |
| <b>windows-domain</b> | Clears the Windows domain statistics.                                     |
| <b>windows-print</b>  | Clears all of the Windows print statistics.                               |

## Defaults

No default behavior or values.

**clear statistics****Command Modes** EXEC**Device Modes** application-accelerator  
central-manager**Usage Guidelines** The **clear statistics** command clears all statistical counters from the parameters given. Use this command to monitor fresh statistical data for some or all features without losing cached objects or configurations.

Not all command options are applicable for a device in central-manager mode.

**Examples** The following example shows how to clear all authentication, RADIUS and TACACS+ information on the WAAS device:

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

**Related Commands** [clear statistics accelerator](#)  
[clear statistics connection](#)

# clear statistics accelerator

To clear all global statistics, use the **clear statistics accelerator** EXEC command.

```
clear statistics accelerator {cifs | epm | generic | http | mapi | nfs | ssl | video}
```

| Syntax Description |  |
|--------------------|--|
| <b>cifs</b>        | Clears the statistics for the CIFS application accelerator.  |
| <b>epm</b>         | Clears the statistics for the EPM application accelerator.   |
| <b>generic</b>     | Clears the statistics for generic accelerator.               |
| <b>http</b>        | Clears the statistics for the HTTP application accelerator.  |
| <b>mapi</b>        | Clears the statistics for the MAPI application accelerator.  |
| <b>nfs</b>         | Clears the statistics for the NFS application accelerator.   |
| <b>ssl</b>         | Clears the statistics for the SSL application accelerator.   |
| <b>video</b>       | Clears the statistics for the video application accelerator. |

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator

**Examples** The following example shows how to clear the statistics for the CIFS application accelerator on the WAAS device:

```
WAE# clear statistics accelerator cifs
```

**Related Commands**
[clear statistics](#)  
[clear statistics connection](#)

---

 clear statistics connection

# clear statistics connection

To clear connection statistics, use the **clear statistics connection** EXEC command.

**clear statistics connection conn-id *connection\_id***

**clear statistics connection optimized [client-ip {*ip\_address* | *hostname*} | client-port *port* | {cifs | epm | http | mapi | nfs | ssl | tfo | video} dre | peer-id *peer\_id* | server-ip {*ip\_address* | *hostname*} | server-port *port*]**

| Syntax Description                  |   |
|-------------------------------------|---|
| <b>conn-id <i>connection_id</i></b> | Clears connection statistics for the connection with the specified number identifier.   |
| <b>optimized</b>                    | Clears connection statistics for optimized connections.   |
| <b>client-ip</b>                    | (Optional) Clears 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.   |
| <b>client-port <i>port</i></b>      | (Optional) Clears the connection statistics for the client with the specified port number. Port number 1–65535.                         |
| <b>cifs</b>                         | (Optional) Clears connection statistics for connections optimized by the CIFS application accelerator.                                  |
| <b>epm</b>                          | (Optional) Clears connection statistics for connections optimized by the EPM application accelerator.                                   |
| <b>http</b>                         | (Optional) Clears connection statistics for connections optimized by the HTTP application accelerator.                                  |
| <b>mapi</b>                         | (Optional) Clears connection statistics for connections optimized by the MAPI application accelerator.                                  |
| <b>nfs</b>                          | (Optional) Clears connection statistics for connections optimized by the NFS application accelerator.                                   |
| <b>ssl</b>                          | (Optional) Clears connection statistics for connections optimized by the SSL application accelerator.                                   |
| <b>tfo</b>                          | (Optional) Clears connection statistics for connections optimized by the TFO application accelerator.                                   |
| <b>video</b>                        | (Optional) Clears connection statistics for connections optimized by the video application accelerator.                                 |
| <b>dre</b>                          | (Optional) Clears connection statistics for connections optimized by the DRE feature.   |
| <b>peer-id <i>peer_id</i></b>       | (Optional) Clears the connection statistics for the peer with the specified identifier. Number from 0 to 4294967295 identifying a peer. |
| <b>server-ip</b>                    | (Optional) Clears the connection statistics for the server with the specified IP address or hostname.                                   |
| <b>server-port <i>port</i></b>      | (Optional) Clears the connection statistics for the server with the specified port number. Port number 1–65535.                         |

---

 Defaults

No default behavior or values.

---

**Command Modes** EXEC

---

**Device Modes** application-accelerator

---

**Examples** The following example shows how to clear the connection 1 statistics on the WAAS device:

```
WAE# clear statistics connection conn-id 1
```

---

**Related Commands**  
[clear statistics](#)  
[clear statistics accelerator](#)

**clear transaction-log**

# clear transaction-log

To archive working transaction log file, use the **clear transaction-log** EXEC command.

```
clear transaction-log {flow}
```

|                           |                        |                                 |
|---------------------------|------------------------|---------------------------------|
| <b>Syntax Description</b> | <b>transaction-log</b> | Clears the transaction log.     |
|                           | <b>flow</b>            | Clears the TFO transaction log. |

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator  
central-manager

**Examples** The following example shows how to archive the flow transaction log file on the WAAS device:

```
WAE# clear transaction-log flow
```

**Related Commands**

- [license add](#)
- [show interface](#)
- [show license](#)
- [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}]
```

|                                 |   |              |   |                       |  |                   |  |            |                              |                                 |                             |
|---------------------------------|---|--------------|---|-----------------------|--|-------------------|--|------------|------------------------------|---------------------------------|-----------------------------|
| <b>Syntax Description</b>       | <table border="0"> <tr> <td><b>users</b></td><td>Clears the connections (logins) of authenticated users.</td></tr> <tr> <td><b>administrative</b></td><td>(Optional) Clears the connections (logins) of administrative users authenticated through a remote login service.</td></tr> <tr> <td><b>locked-out</b></td><td>(Optional) Unlocks specified locked-out user accounts.</td></tr> <tr> <td><b>all</b></td><td>Specifies all user accounts.</td></tr> <tr> <td><b>username <i>username</i></b></td><td>Specifies account username.</td></tr> </table> | <b>users</b> | Clears the connections (logins) of authenticated users. | <b>administrative</b> | (Optional) Clears the connections (logins) of administrative users authenticated through a remote login service. | <b>locked-out</b> | (Optional) Unlocks specified locked-out user accounts. | <b>all</b> | Specifies all user accounts. | <b>username <i>username</i></b> | Specifies account username. |
| <b>users</b>                    | Clears the connections (logins) of authenticated users.   |              |   |                       |  |                   |  |            |                              |                                 |                             |
| <b>administrative</b>           | (Optional) Clears the connections (logins) of administrative users authenticated through a remote login service.  |              |   |                       |  |                   |  |            |                              |                                 |                             |
| <b>locked-out</b>               | (Optional) Unlocks specified locked-out user accounts.  |              |   |                       |  |                   |  |            |                              |                                 |                             |
| <b>all</b>                      | Specifies all user accounts.  |              |   |                       |  |                   |  |            |                              |                                 |                             |
| <b>username <i>username</i></b> | Specifies account username.   |              |   |                       |  |                   |  |            |                              |                                 |                             |

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-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 a strong password policy is enabled (see the **(config) authentication strict-password-policy** command) a user account will be locked out if the user fails three consecutive login attempts. (This restriction does not apply to the admin account.)

**Examples** The following example shows how to clear the connections of all authenticated users:

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

The following example shows how to clear 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 shows how to unlock all locked-out user accounts:

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

**■ clear users**

The following example shows how to unlock the account for username darcy:

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

**Related Commands**

[\*\*clear arp-cache\*\*](#)  
[\*\*\(config\) authentication strict-password-policy\*\*](#)

# clear windows-domain-log

To clear the Windows domain server log file, use the **clear windows-domain-log** EXEC command.

**clear windows-domain-log**

|                           |   |
|---------------------------|---|
| <b>Syntax Description</b> | <b>windows-domain-log</b><br>Clears the Samba, Kerberos, and Winbind log files.   |
| <b>Defaults</b>           | No default behavior or values.  |
| <b>Command Modes</b>      | EXEC  |
| <b>Device Modes</b>       | application-accelerator<br>central-manager  |
| <b>Examples</b>           | The following example shows how to clear all entries in the Windows domain log file on the WAAS device:<br><br><code>WAE# clear windows-domain-log</code> |
| <b>Related Commands</b>   | <a href="#">license add</a><br><a href="#">show interface</a><br><a href="#">show license</a><br><a href="#">show wccp</a>                                |

# clock

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

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

---

## Syntax Description

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

---

## Defaults

No default behavior or values.

---

## Command Modes

EXEC

---

## Device Modes

application-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 bootup to initialize the software clock.

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

---

## Examples

The following example shows how to set 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 | deregister [force] | lcm {enable | disable} | maintenance {full | regular} | recover {identity word} | restore filename | validate}
```

```
cms database {backup | create | delete | downgrade [script filename]}
```

| Syntax Description      |  |
|-------------------------|--|
| <b>config-sync</b>      | Sets the node to synchronize configuration with the WAAS Central Manager.  |
| <b>deregister</b>       | Removes the device registration record and its configuration on the WAAS Central Manager.  |
| <b>force</b>            | (Optional) Forces the removal of the node registration. This option is available only on WAEs and the standby Central Manager. If disk encryption is enabled, it is disabled and encrypted file systems are erased after a reload. |
| <b>lcm</b>              | Configures local/central management on a WAAS device that is registered with the WAAS Central Manager.   |
| <b>enable</b>           | Enables synchronization of the WAAS network configuration of the device with the local CLI configuration.  |
| <b>disable</b>          | Disables synchronization of the WAAS network configuration of the device with the local CLI configuration.   |
| <b>maintenance</b>      | Cleans and reindexes the embedded database tables.   |
| <b>full</b>             | Specifies a full maintenance routine for the embedded database tables.   |
| <b>regular</b>          | Specifies a regular maintenance routine for the embedded database tables.  |
| <b>recover</b>          | Recovers the identity of a WAAS device.  |
| <b>identity word</b>    | Specifies the identity of the recovered device (identification key set on the Central Manager)   |
| <b>restore filename</b> | Restores the database management tables using the backup local filename.   |
| <b>validate</b>         | Validates the database files.  |
| <b>database</b>         | Creates, backs up, deletes, restores, or validates the CMS-embedded database management tables or files.   |
| <b>backup</b>           | Backs up the database management tables.   |
| <b>create</b>           | Creates the embedded database management tables.   |
| <b>delete</b>           | Deletes the embedded database files.   |
| <b>downgrade</b>        | Downgrades the CMS database.   |
| <b>script filename</b>  | (Optional) Downgrades the CMS database by applying a downgrade script (filename).  |

### Defaults

No default behavior or values.

**Command Modes** EXEC**Device Modes** application-accelerator  
central-manager

**Usage Guidelines** 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 for a device that is already registered with the WAAS Central Manager. Then use the **cms enable** command to enable the CMS. For a device that is not registered with a WAAS Central Manager, use only the **cms enable** command to initialize the CMS database tables, register the node, and enable the CMS.

Before a node can join a WAAS network, it must first be registered and then activated. Activate the node by using the WAAS Central Manager GUI.

The **cms deregister** command removes the node from the WAAS network by deleting registration information and database tables.

The **cms deregister force** command forces the removal of the node from the WAAS network by deleting registration information and database tables. If disk encryption is enabled on the device, it is disabled after you confirm this action. All data in encrypted file systems and imported certificates and private keys for the SSL accelerator are lost after a reload.

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 and the WAAS version number.



**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*.



**Note** Do not run multiple instances of the **cms database backup** command simultaneously on a device. If a backup is in progress, you must wait for it to finish before using the command again.

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

# cms secure-store

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

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

|                           |   |  |
|---------------------------|---|--|
| <b>Syntax Description</b> | <b>init</b><br><b>open</b><br><b>change</b><br><b>clear</b><br><b>reset</b> | <p>Initializes secure store encryption on the WAAS device and opens the secure store.<br/>On the Central Manager, this command prompts you to enter the secure store encryption pass phrase.</p> <p>Activates secure store encryption (the WAAS device encrypts the stored data using secure store encryption). Secure store encryption must already be initialized using the <b>cms secure-store init</b> command.<br/>On the Central Manager, this command prompts you to enter the secure store encryption pass phrase.</p> <p>Changes the secure store encryption pass phrase and encryption key. On the Central Manager this command prompts you to enter the current pass phrase, new pass phrase, and confirm the new pass phrase. The WAAS device uses the pass phrase to generate the encryption key for secure disk encryption.</p> <p>Disables secure store encryption.</p> <p>Resets secure store to the uninitialized state. Secure store encryption must be initialized but not open to use this option. This option applies only to a Central Manager device.</p> |
|---------------------------|---|--|

**Defaults** The standard encryption and key management is the default.

**Command Modes** EXEC

**Device Modes** application-accelerator  
central-manager

**Usage Guidelines** Secure store encryption provides stronger encryption and key management for your WAAS system. The WAAS Central Manager and WAE devices use secure store 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 you enable secure store on Central Manager, the data is encrypted using a key encryption key generated from the pass phrase you enter with SHA-1 hashing and an AES 256-bit algorithm. When you enable secure store 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. The password must conform to the following rules:

- Be 8 to 64 characters in length
- Contain characters only from the allowed set ([A-Za-z0-9~%'!#\$^&\*()|;,:<>/]\*)
- Contain at least one digit
- Contain at least one lowercase and one uppercase letter

When you first initialize secure store encryption with the **cms secure-store init** command, this command also opens the secure store, so there is no need to use the **cms secure-store open** command. When you reboot the Central Manager, you must manually reopen secure store using the **cms secure-store open** command. Until you open the secure store, a critical alarm is displayed on the Central Manager.

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 user passwords, CIFS preposition and dynamic share credentials, and WAAS password credentials stored on the WAE. 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 the WAAS persistent storage. If key retrieval fails, an alarm is raised and secure store will be in the initialized but not open state. You must open secure store manually.

If you have made any other CLI configuration changes on a WAE within the datafeed poll rate time interval (5 minutes by default) before you entered the **cms secure-store** command, you will lose those prior configuration changes and you will need to redo them.

Use the **cms secure-store reset** command if you reload the Central Manager and forget the secure store password, so you cannot open the secure store. This command deletes all encrypted data, certificate and key files, and key manager keys. The secure store is left in the uninitialized state. For the complete procedure for resetting the secure store, see the “[Resetting Secure Store Encryption on a Central Manager](#)” section on page 9-15 in the *Cisco Wide Area Application Services Configuration Guide*.

## Examples

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

```
waas-cm# cms secure-store init
Stopping cms.

*****
* 1) Must be between 8 to 64 characters in length
* 2) Allowed character set is ([A-Za-z0-9~%'!#$^&*()|;,:<>/]*)
* 3) Must contain at least one digit
* 4) Must contain at least one lowercase and one uppercase letter *
*****


enter pass-phrase:
confirm pass-phrase:
Successfully migrated user passwords
Successfully migrated Cifs preposition password
Successfully migrated Cifs dynamic shares password
Successfully migrated key store
***** WARNING : REBOOTING CM REQUIRES RE-OPENING SECURE STORE MANUALLY. AFTER REBOOT, DISK
ENCRYPTION AND CIFS PREPOSITION FEATURES ON REMOTE WAE(S) WILL NOT OPERATE
PROPERLY UNTIL USER RE-OPENS SECURE STORE ON CM BY INPUTTING THE PASSPHRASE *****
successfully initialized and opened secure-store.
Starting cms.
```

**cms secure-store**

The following example shows how to deactivates secure store encryption:

```
waas-cm# cms secure-store clear
Secure store clear will result in deletion of CM pki store certificate/private key files
Do you want to continue(yes/no)?yes
Stopping cms.
Successfully migrated user passwords
Successfully migrated Cifs preposition password
Successfully migrated Cifs dynamic shares password
Successfully migrated key store
secure-store clear
Starting cms.
```

---

**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  
central-manager

**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**

## copy cdrom

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

```
copy cdrom install filedir filename
```

---

### Syntax Description

|  |   |
|--|---|
| <b>cdrom</b>                           | Copies a file from the CD-ROM.  |
| <b>install</b> <i>filedir filename</i> | Installs the software release from the directory location and filename specified. |

---

### Defaults

No default behavior or values.

---

### Command Modes

EXEC

---

### Device Modes

application-accelerator  
central-manager

---

### Examples

The following example shows how to copy a software release file from a CD-ROM:

```
WAE# copy cdrom install
```

---

### Related Commands

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

# copy cdrom wow-recovery

To recover Windows on a virtual blade without reloading the software, use the **copy cdrom wow-recovery** EXEC command.

```
copy cdrom wow-recovery install filedir filename
```

## Syntax Description

|  |  |
|--|--|
| <b>cdrom</b>                           | Copies the Windows system files from the CD-ROM.   |
| <b>wow-recovery</b>                    | Recovers the Windows operating system.   |
| <b>install</b> <i>filedir filename</i> | Installs the Windows operating system on the virtual blade from the directory location and Windows filename. |

## Defaults

No default behaviors or values.

## Command Modes

EXEC

## Device Modes

application-accelerator  
central-manager

## Usage Guidelines

Use the **copy cdrom wow-recovery** EXEC command to recover the Windows system files of a virtual blade. This command allows you to recover Windows on your virtual blade while the WAAS is running, without having to restart your WAE device.

## Examples

The following example shows how to recover Windows on a virtual blade:

```
WAE# copy cdrom wow-recovery install
```

## Related Commands

[copy ftp](#)  
[copy cdrom](#)  
[virtual-blade](#)  
[\(config\) virtual-blade](#)

---

copy compactflash

# copy compactflash

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

**copy compactflash install** *filename*

|                           |   |
|---------------------------|---|
| <b>Syntax Description</b> | <b>compactflash</b> Copies a file from the CompactFlash card.<br><b>install</b> <i>filename</i> Installs a software release from an image filename. |
|---------------------------|---|

---

**Defaults** No default behaviors or values.

---

**Command Modes** EXEC

---

**Device Modes** application-accelerator  
central-manager

---

**Examples** The following example shows how to copy a software release file from a CompactFlash card:

```
WAE# copy compactflash install
```

---

**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}
```

|                                       |  |
|---------------------------------------|--|
| <b>Syntax Description</b>             |  |
| <b>disk</b>                           | Copies a local disk file.  |
| <b>ftp</b>                            | Copies to a file on an FTP server.   |
| <i>hostname</i>                       | Hostname of the FTP server.  |
| <i>ip-address</i>                     | IP address of the FTP server.  |
| <i>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.   |
| <b>startup-config</b> <i>filename</i> | Copies the existing configuration file from the disk to the startup configuration (NVRAM). |

**Defaults** No default behaviors or values.

**Command Modes** EXEC

**Device Modes** application-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.

**Examples** The following example shows how to copy a startup-configuration file to NVRAM:

```
WAE# copy disk startup-config
```

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

copy disk

write

# copy ftp

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

```
copy ftp disk {hostname | ip-address} remotefiledir remotefilename localfilename
copy ftp install {hostname | ip-address} remotefiledir remotefilename
copy ftp virtual-blade vb_num disk vb_disk {hostname | ip-address} remotefiledir remotefilename
copy ftp wow-recovery {hostname | ip-address} remotefiledir remotefilename
```

|                                    |  |
|------------------------------------|--|
| <b>Syntax Description</b>          |  |
| <b>disk</b>                        | Copies a file to a local disk.   |
| <i>hostname</i>                    | Hostname of the specific server.   |
| <i>ip-address</i>                  | IP address of the specific server.   |
| <i>remotefiledir</i>               | Directory on the FTP server where the image file to be copied is located.                      |
| <i>remotefilename</i>              | Name of the file to be copied.   |
| <i>localfilename</i>               | Name of the copied file as it appears on the local disk.                                       |
| <b>install</b>                     | Copies the file from an FTP server and installs the software release file to the local device. |
| <b>virtual-blade</b> <i>vb_num</i> | Specifies the virtual blade number of the virtual blade disk image to copy to.                 |
| <b>disk</b> <i>vb_disk</i>         | Specifies the virtual blade disk number of the virtual blade disk image to copy to.            |
| <b>wow-recovery</b>                | Recovers the Windows operating system for use on a virtual blade.                              |

**Defaults** No default behaviors or values.

**Command Modes** EXEC

**Device Modes** application-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. To show progress, this command prints a number sign (#) for each 1 MB of data that is copied.

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 a disk and part goes to flash memory.

You can also use the **copy ftp install** EXEC command 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.

**copy ftp**

Use the **copy ftp wow-recovery** EXEC command to copy a Windows operating system image from an FTP server to a virtual blade partition on the WAAS device.

To show progress, this command prints a number sign (#) for each 1 MB of data that is copied.

### **Upgrading the BIOS**

You can remotely upgrade the BIOS on the WAE-511, WAE-512, WAE-611, WAE-612, and the WAE-7326.

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**


---

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

---

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 cisco/waas/4.1 WAAS-4.1.1-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-4.1.1-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-dependent 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 upgradeserver /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
```

**copy ftp**

```

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#

```

The following example shows how to copy a Windows image file from an FTP server and install the file on the virtual blade:

```

WAE# copy ftp wow-recovery 10.1.1.1 /cisco/waas/4.1 windows.iso
Enter username for remote ftp server:biff
Enter password for remote ftp server:*****
Initiating FTP download...

```

---

**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                |  |
|-----------------------------------|--|
| <b>http</b>                       | Copies the file from an HTTP server.   |
| <b>install</b>                    | 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.   |
| <b>port</b> <i>portnum</i>        | (Optional) Port number (1–65535) to connect to the HTTP server (the default is 80).                              |
| <b>proxy</b> <i>proxy_portnum</i> | (Optional) Allows the request to be redirected to an HTTP proxy server. HTTP proxy server port number (1–65535). |
| <b>username</b> <i>username</i>   | (Optional) Username and password to access the HTTP proxy server.  |
| <i>password</i>                   |  |

**Defaults** HTTP server port: 80

**Command Modes** EXEC

**Device Modes** application-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 a 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.

copy http

### 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 the software through an interface. The Basic Input Output System (BIOS) provides a 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, 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, and provides an interface between the hardware and the operating system in the form of a library of interrupt handlers.

Each time that 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. You can solve this problem 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**

---

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

---

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 (*/local1/bios\_upgrade.txt*) for traceability. The hardware-dependent 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 upgradeserver /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]
```

---

copy http

```

Erasing block 2f:280000 - 28ffff
Erasing block 30:290000 - 29ffff
Erasing block 31:2a0000 - 2a0000
Erasing block 32:2b0000 - 2b0000
Erasing block 33:2c0000 - 2c0000
Erasing block 34:2d0000 - 2d0000
Erasing block 35:2e0000 - 2e0000
Erasing block 36:2f0000 - 2f0000
Programming block 2f:280000 - 28ffff
Programming block 30:290000 - 29ffff
Programming block 31:2a0000 - 2a0000
Programming block 32:2b0000 - 2b0000
Programming block 33:2c0000 - 2c0000
Programming block 34:2d0000 - 2d0000
Programming block 35:2e0000 - 2e0000
Programming block 36:2f0000 - 2f0000
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}
```

|                           |   |
|---------------------------|---|
| <b>Syntax Description</b> |   |
| <b>running-config</b>     | Copies the current system configuration.  |
| <b>disk filename</b>      | Copies the current system configuration to a disk file. Specify the name of the file to be created on a disk. |
| <b>startup-config</b>     | Copies the running configuration to startup configuration (NVRAM).  |
| <b>tftp</b>               | 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.<br>Use the complete pathname.     |

**Defaults** No default behaviors or values.

**Command Modes** EXEC

**Device Modes** application-accelerator  
central-manager

**Usage Guidelines** Use the **copy running-config** EXEC command to copy the running system configuration of the WAAS device 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.

**Examples** The following example shows how to copy the current system configuration to startup configuration (NVRAM):

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

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

copy running-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}
```

|                              |   |
|------------------------------|---|
| <b>Syntax Description</b>    |   |
| <b>startup-config</b>        | Copies the startup configuration.   |
| <b>disk <i>filename</i></b>  | Copies the startup configuration to a disk file. Specify the name of the startup configuration file to be copied to the local disk. |
| <b>running-config</b>        | Copies the startup configuration to running configuration.  |
| <b>tftp</b>                  | Copies the startup configuration to a file on a TFTP server.  |
| <b><i>hostname</i></b>       | Hostname of the TFTP server.  |
| <b><i>ip-address</i></b>     | IP address of the TFTP server.  |
| <b><i>remotefilename</i></b> | 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  
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.

**Examples** The following example shows how to copy the startup configuration file to the running configuration:

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

**Related Commands**

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

**copy sysreport**

# copy sysreport

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

**copy sysreport disk filename**

**copy sysreport ftp {hostname | ip-address} remotedirectory remotefilename**

**copy sysreport tftp {hostname | ip-address} remotefilename} [start-date {day month | month day} year [end-date {day month | month day} year]]**

| Syntax Description | <b>sysreport</b>       | Generates and saves a report containing WAAS system information in a file.   |
|--------------------|------------------------|--|
|                    | <b>disk filename</b>   | Copies system information to a disk file. Specify the name of the file to be created on a disk. Note that .tar.gz is appended to the filename that you specify.  |
|                    | <b>ftp</b>             | Copies system information to a FTP server.   |
|                    | <i>hostname</i>        | Hostname of the server.  |
|                    | <i>ip-address</i>      | IP address of the 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.  |
|                    | <b>tftp</b>            | Copies system information to a TFTP server.  |
|                    | <i>remotefilename</i>  | Remote filename of the system information file to be created on the TFTP server. Use the complete pathname.  |
|                    | <b>start-date</b>      | (Optional) Start date of the 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).   |
|                    | <b>end-date</b>        | (Optional) End date of information in the generated system report. If omitted, this date defaults to today. 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 is used.

**Command Modes** EXEC

| Device Modes     | application-accelerator<br>central-manager   |
|------------------|--|
| Usage Guidelines | The <b>copy sysreport</b> command consumes significant CPU and disk resources and can adversely affect system performance while it is running.   |
| Examples         | <p>The following example shows how to copy system information to the file mysysinfo on the local WAAS device:</p> <pre>WAE# copy sysreport disk mysysinfo start-date 1 April 2006 end-date April 30 2006</pre> <p>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:</p> <pre>WAE# copy sysreport ftp myserver / foo start-date 1 April 2006 end-date April 30 2006</pre> |
| Related Commands | <a href="#">show running-config</a><br><a href="#">show startup-config</a><br><a href="#">wafs</a>   |

**copy system-status**

# copy system-status

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

**copy system-status disk *filename***

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

|                 |                                 |
|-----------------|---------------------------------|
| <b>Defaults</b> | No default behaviors or values. |
|-----------------|---------------------------------|

|                      |      |
|----------------------|------|
| <b>Command Modes</b> | EXEC |
|----------------------|------|

|                     |  |
|---------------------|--|
| <b>Device Modes</b> | application-accelerator<br>central-manager |
|---------------------|--|

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

|                 |   |
|-----------------|---|
| <b>Examples</b> | The following example shows how to copy the system status to a disk file: |
|-----------------|---|

```
WAE# copy system-status disk file1
```

|                         |  |
|-------------------------|--|
| <b>Related Commands</b> | <a href="#">install</a><br><a href="#">reload</a><br><a href="#">show running-config</a><br><a href="#">show startup-config</a><br><a href="#">wafs</a><br><a href="#">write</a> |
|-------------------------|--|

# 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 | ftp {hostname | ip-address} remotedirectory remotefilename |
    tftp {hostname | ip-address} remotefilename}
```

| Syntax Description     |   |
|------------------------|---|
| <b>tech-support</b>    | Copies system information for technical support.  |
| <b>disk filename</b>   | Copies system information for technical support to a disk file. Specify the name of the file to be created on disk. |
| <b>ftp</b>             | Copies system information for technical support to an FTP server.   |
| <i>hostname</i>        | Hostname of the FTP server.   |
| <i>ip-address</i>      | IP address of the FTP server.   |
| <b>remotedirectory</b> | Remote directory of the system information file to be created on the FTP server. Use the complete pathname.         |
| <b>remotefilename</b>  | Remote filename of the system information file to be created on the FTP server.                                     |
| <b>tftp</b>            | 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.  |
| <b>remotefilename</b>  | 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  
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.

**Examples** The following example shows how to copy system information for tech support to a disk file:

```
WAE# copy tech-support disk file1
```

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

```
copy tech-support
```

```
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**

**copy tftp running-config {hostname | ip-address} remotefilename**

**copy tftp startup-config {hostname | ip-address} remotefilename**

|                           |   |
|---------------------------|---|
| <b>Syntax Description</b> |   |
| <b>tftp</b>               | Copies an image from a TFTP server.   |
| <b>disk</b>               | 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.                                     |
| <b>running-config</b>     | Copies an image from a TFTP server to the running configuration.                            |
| <b>startup-config</b>     | Copies an image from a TFTP server to the startup configuration.                            |

|                 |                                 |
|-----------------|---------------------------------|
| <b>Defaults</b> | No default behaviors or values. |
|-----------------|---------------------------------|

|                      |      |
|----------------------|------|
| <b>Command Modes</b> | EXEC |
|----------------------|------|

|                     |  |
|---------------------|--|
| <b>Device Modes</b> | application-accelerator<br>central-manager |
|---------------------|--|

|                 |  |
|-----------------|--|
| <b>Examples</b> | The following example shows how to copy configuration or image data from a TFTP server to the running configuration: |
|                 | <b>WAE# copy tftp running-config</b>   |

|                         |  |
|-------------------------|--|
| <b>Related Commands</b> | <a href="#">install</a><br><a href="#">reload</a><br><a href="#">show running-config</a><br><a href="#">show startup-config</a><br><a href="#">wafs</a><br><a href="#">write</a> |
|-------------------------|--|

**copy virtual-blade**

# copy virtual-blade

To copy software configuration or image data from a virtual blade disk image to an FTP server, use the **copy virtual-blade** EXEC command.

```
copy virtual-blade vb_num disk vb_disk ftp {hostname | ip-address} remotefiledir remotefilename
```

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | <b>virtual-blade</b> <i>vb_num</i> Specifies the virtual blade number of the virtual blade disk image to copy to.<br><b>disk</b> <i>vb_disk</i> Specifies the virtual blade disk number of the virtual blade disk image to copy to.<br><b>ftp</b> Writes to an FTP server.<br><i>hostname</i> Hostname of the specific server.<br><i>ip-address</i> IP address of the specific server.<br><i>remotefiledir</i> Directory where the image file to be copied is located.<br><i>remotefilename</i> Name of the file to be copied. |
|---------------------------|--|

**Defaults**      No default behaviors or values.

**Command Modes**      EXEC

**Device Modes**      application-accelerator  
central-manager

**Examples**      The following example shows how to copy an image file from a virtual blade to an FTP server:

```
WAE# copy virtual-blade 1 disk 1 ftp 10.75.16.234 / file.img
```

**Related Commands**

- [copy ftp](#)
- [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*

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

|                 |                                |
|-----------------|--------------------------------|
| <b>Defaults</b> | No default behavior or values. |
|-----------------|--------------------------------|

|                      |      |
|----------------------|------|
| <b>Command Modes</b> | EXEC |
|----------------------|------|

|                     |  |
|---------------------|--|
| <b>Device Modes</b> | application-accelerator<br>central-manager |
|---------------------|--|

|                         |                                 |
|-------------------------|---------------------------------|
| <b>Usage Guidelines</b> | Only SYSFS files can be copied. |
|-------------------------|---------------------------------|

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

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

|                         |   |
|-------------------------|---|
| <b>Related Commands</b> | <a href="#">deltree</a><br><a href="#">dir</a><br><a href="#">lls</a><br><a href="#">ls</a><br><a href="#">mkdir</a><br><a href="#">pwd</a><br><a href="#">rename</a> |
|-------------------------|---|

**crypto delete**

# crypto delete

To remove SSL certificate and key files, use the **crypto delete** EXEC command.

```
crypto delete {ca-certificate filename | pkcs12 filename} }
```

Use the crypto delete EXEC command to remove a certificate from your WAE's secure store. If you only want to disassociate a certificate from an accelerated service, use **no server-cert-key** in crypto ssl services accelerated-service mode.

|                           |   |
|---------------------------|---|
| <b>Syntax Description</b> | <b>ca-certificate</b> <i>filename</i> Deletes a certificate authority certificate file.<br><b>pkcs12</b> <i>filename</i> Deletes a PKCS12 format file. (PKCS12 files contain both the private encryption key and the public key certificate.) |
|---------------------------|---|

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator

**Examples** The following example shows how to delete the CA certificate file mycert.ca:

```
WAE# crypto delete ca-certificate mycert.ca
```

**Related Commands**

- [crypto export](#)
- [crypto generate](#)
- [crypto import](#)

# crypto export

To export SSL certificate and key files, use the **crypto export** EXEC command.

```
crypto export {ca-certificate filename | pkcs12 {factory-self-signed | filename} {pem-cert-key | pem-cert-only | pem-key-only | pkcs12}}{disk pathname | ftp address | sftp address | terminal | tftp address}
```

| Syntax Description | <b>ca-certificate</b> <i>filename</i> | Export a certificate authority certificate file.  |
|--------------------|---------------------------------------|---|
|                    | <b>pkcs12</b>                         | Export a PKCS12 format file. (PKCS12 files contain both the private encryption key and the public key certificate.) |
|                    | <b>factory-self-signed</b>            | Specifies that the SSL PKCS file is to be self-signed.  |
|                    | <i>filename</i>                       | The name of the PKCS12 file to be exported.   |
|                    | <b>pem-cert-key</b>                   | Export both the certificate and key in PEM format.  |
|                    | <b>pem-cert-only</b>                  | Export only the certificate in PEM format.  |
|                    | <b>pem-key-only</b>                   | Export only the key in PEM format.  |
|                    | <b>pkcs12</b>                         | Export both the certificate and key in PKCS12 format.   |
|                    | <b>disk</b> <i>pathname</i>           | Export to a disk. Type the disk filename including the full path.   |
|                    | <b>ftp</b> <i>address</i>             | Export to FTP. Type the FTP server's IP address or hostname.  |
|                    | <b>sftp</b> <i>address</i>            | Export to secure FTP. Type the secure FTP server's IP address or hostname.  |
|                    | <b>terminal</b>                       | Export to a terminal.(Not available for <b>crypto export pkcs12</b> .)  |
|                    | <b>tftp</b> <i>address</i>            | Export to TFTP. Type the TFTP server's IP address or hostname.  |

**Defaults** No default behavior or values.

---

## Command Modes

## Device Modes

The following example shows how to export a CA certificate file named mycert.ca to an FTP server:

WAE#\_cryptos expert ss certificate mycert ss ftp 1 2 3 4 dir1 mycert ss

The following example shows how to export the certificate and private key from a PKCS12 file named myfile.p12 to a PEM file on the local1 directory on the hard drive:

```
WAF# cryptos expert phcs13 myfile.p13 phcs13 disk <local1/myfile.p13>
```

---

|                         |  |
|-------------------------|--|
| <b>Related Commands</b> | <a href="#">crypto delete</a><br><a href="#">crypto generate</a> |
|-------------------------|--|

■ **crypto export**

**crypto import**

# crypto generate

To generate a self-signed certificate or a certificate signing request, use the **crypt generate** EXEC command.

```
crypto generate {csr rsa modulus {1024 | 1536 | 2048 | 512 | 768} {disk pathname | ftp address |
sftp address | terminal | tftp address} | self-signed-cert filename [exportable] rsa modulus
{1024 | 1536 | 2048 | 512 | 768}}
```

| Syntax Description | csr                                   | Generate a certificate signing request (CSR).   |
|--------------------|---------------------------------------|---|
|                    | <b>rsa modulus</b>                    | Specify the size of the RSA modulus to be used for the CSR.   |
|                    | <b>1024   1536   2048   512   768</b> | The size (number of bits) used for the RSA modulus.   |
|                    | <b>disk pathname</b>                  | Generate the file to a disk. Type the disk filename including the full path.  |
|                    | <b>ftp address</b>                    | Generate the file to FTP. Type the FTP server's IP address or hostname.   |
|                    | <b>sftp address</b>                   | Generate the file to secure FTP. Type the secure FTP server's IP address or hostname.   |
|                    | <b>terminal</b>                       | Generate the file to a terminal.  |
|                    | <b>tftp address</b>                   | Generate the file to TFTP. Type the TFTP server's IP address or hostname.   |
|                    | <b>self-signed-cert</b>               | Generate a self-signed SSL encryption certificate. The filename of the self-signed certificate to be generated must have the .p12 file extension. |
|                    | <b>filename</b>                       |   |
|                    | <b>exportable</b>                     | Allows the self-signed certificate to be exported.  |
|                    | <b>rsa modulus</b>                    | Specify the size of the RSA modulus to be used when generating the self-signed certificate.   |

|          |                                |
|----------|--------------------------------|
| Defaults | No default behavior or values. |
|----------|--------------------------------|

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

|              |  |
|--------------|--|
| Device Modes | application-accelerator<br>central-manager |
|--------------|--|

|          |   |
|----------|---|
| Examples | The following example shows how to create an exportable self-signed certificate. The certificate file is named myfile.p12 and is created using a 512-bit RSA modulus. |
|----------|---|

```
WAE# crypto generate self-signed-cert myfile.p12 exportable rsa modulus 512
Generating a 512 bit RSA private key
```

```
.....+++++++
....+++++++
----
```

You are about to be asked to enter information that will be incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank

**crypto generate**

For some fields there will be a default value,  
If you enter '.', the field will be left blank.

-----  
Country Name (2 letter code) [US]:**us**  
State or Province Name (full name) [California]:<cr> (Press Enter to accept the default.)  
Locality Name (eg, city) [San Jose]:San Jose  
Organization Name (eg, company) [Cisco Systems]:  
Organizational Unit Name (eg, section) [ADBU]:  
Common Name (eg, YOUR name) [www.cisco.com]:  
Email Address [tac@cisco.com]:

WAE#

**Related Commands**

[crypto delete](#)

[crypto export](#)

[crypto import](#)

# crypto import

To import SSL certificates and key files, use the **crypto export** EXEC command.

```
crypto import {ca-certificate filename | pkcs12 filename [exportable]}{pem-cert-key | pkcs12} }{disk pathname | ftp address | sftp address | terminal | tftp address}
```

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | <b>ca-certificate <i>filename</i></b> Import a certificate authority certificate file. The name of the CA certificate file to be imported (PEM format) must have .ca extension.<br><b>pkcs12 <i>filename</i></b> Specifies a certificate intended for the management or an accelerated service (PKCS12 format). A PKCS12 file contains both the private encryption key and the public key certificate. The name of the PKCS12 file to be imported must have a .p12 extension.<br><i>Note:</i> DSA-encoded certificates are not supported and will not be imported.<br><b>pem-cert-key</b> Import both the certificate and key in PEM format.<br><i>When you use pem-cert-key, you must specify the pathname and filename or the address and filename for both the certificate file and the key file for disk, ftp, sftp, and tftp.</i><br><b>exportable</b> Configures the imported certificate to be exportable.<br><b>pkcs12</b> Import both the certificate and key in PKCS12 format.<br><b>disk <i>pathname</i></b> Import from a disk. Type the disk filename including the full path.<br><b>ftp <i>address</i></b> Import from FTP. Type the FTP server's IP address or hostname.<br><b>sftp <i>address</i></b> Import from secure FTP. Type the secure FTP server's IP address or hostname.<br><b>terminal</b> Import from a terminal.<br><b>tftp <i>address</i></b> Import from TFTP. Type the TFTP server's IP address or hostname. |
|---------------------------|--|

|                 |                                |
|-----------------|--------------------------------|
| <b>Defaults</b> | No default behavior or values. |
|-----------------|--------------------------------|

|                      |      |
|----------------------|------|
| <b>Command Modes</b> | EXEC |
|----------------------|------|

|                     |                         |
|---------------------|-------------------------|
| <b>Device Modes</b> | application-accelerator |
|---------------------|-------------------------|

|                 |  |
|-----------------|--|
| <b>Examples</b> | The following example shows how to import a CA certificate file named mycert.ca from a TFTP server:<br><pre>WAE# crypto import ca-certificate mycert.ca tftp 00.00.00.00</pre> |
|-----------------|--|

|                         |  |
|-------------------------|--|
| <b>Related Commands</b> | <a href="#">crypto delete</a><br><a href="#">crypto export</a> |
|-------------------------|--|

■ **crypto import**

**crypto generate**

# crypto pki

To initialize the PKI managed store, use the **crypto pki** EXEC command.

**crypto pki managed-store initialize**

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | <b>managed-store</b> Specifies managed store commands.<br><b>initialize</b> Initializes the PKI managed store. |
|---------------------------|--|

|                 |                                |
|-----------------|--------------------------------|
| <b>Defaults</b> | No default behavior or values. |
|-----------------|--------------------------------|

|                      |      |
|----------------------|------|
| <b>Command Modes</b> | EXEC |
|----------------------|------|

|                     |  |
|---------------------|--|
| <b>Device Modes</b> | application-accelerator<br>central-manager |
|---------------------|--|

|                 |  |
|-----------------|--|
| <b>Examples</b> | The following example shows how to initialize the PKI managed store: |
|-----------------|--|

```
WAE# crypto pki managed-store initialize
```

|                         |   |
|-------------------------|---|
| <b>Related Commands</b> | <a href="#">crypto export</a><br><a href="#">crypto generate</a><br><a href="#">crypto import</a> |
|-------------------------|---|

---

```
debug aaa accounting
```

# debug aaa accounting

To monitor and record AAA accounting debugging, use the **debug aaa accounting** EXEC command. To disable debugging, use the **undebbug** form of this command.

```
debug aaa accounting
undebbug aaa accounting
```

|                           |   |
|---------------------------|---|
| <b>Syntax Description</b> | <b>aaa accounting</b><br><br>(Optional) Enables AAA accounting actions.   |
| <b>Defaults</b>           | No default behavior or values.  |
| <b>Command Modes</b>      | EXEC  |
| <b>Device Modes</b>       | application-accelerator<br>central-manager  |
| <b>Usage Guidelines</b>   | <p>Because the performance of the WAAS device degrades when you use the <b>debug</b> command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the “<a href="#">Obtaining Documentation and Submitting a Service Request</a>” section on page xx.</p> <p>If the watchdog utility is not running, the message “WAAS is not running” appears.</p> <p>Use the <b>show debugging</b> command to display enabled <b>debug</b> options.</p> <p>The output associated with the <b>debug</b> command is written to either the syslog file in <code>/local1/syslog.txt</code> or the debug log associated with the module in the file <code>/local1/errorlog/module_name-errorlog.current</code>.</p> <p>The debug log file associated with a module will be rotated to a backup file when the current file reaches its maximum size. The backup files are named as follows: <code>name-errorlog.#</code>, where # is the backup file number.</p> <p>For any <b>debug</b> command, system logging must be enabled. The command to enable logging is the <b>logging disk enable</b> global configuration command, which is enabled by default.</p> <p>If a <b>debug</b> command module uses the syslog for debug output, then you must use the <b>logging disk priority debug</b> global configuration command (the default is <b>logging disk priority notice</b>).</p> <p>If a <b>debug</b> command module uses the debug log for output, then the output can be filtered based on the priority level configuration for the four different levels of debug log output, as follows:</p> <ul style="list-style-type: none"> <li>• For filtering on critical debug messages only, use the <b>logging disk priority critical</b> global configuration command.</li> <li>• For filtering on critical and error level debug messages, use the <b>logging disk priority error</b> global configuration command.</li> <li>• For filtering on critical, error, and trace debug level debug messages, use the <b>logging disk priority debug</b> global configuration command.</li> </ul> |

- For seeing all debug log messages, which include critical, error, trace and detail messages, use the **logging disk priority detail** global configuration command.

Regardless of the priority level configuration, any syslog messages at the LOG\_ERROR or higher priority will be automatically written to the debug log associated with a module.

We recommend that you use the **debug** and **undebbug** commands only at the direction of Cisco Systems technical support personnel.

---

**Examples**

The following example shows how to enable AAA accounting debug monitoring:

```
WAE# debug aaa accounting
```

---

**Related Commands**

[show debugging](#)

■ debug accelerator

# debug accelerator

To monitor and record accelerator debugging, use the **debug accelerator** EXEC command. To disable debugging, use the **undebug** form of this command.

**debug accelerator cifs [shell | all]**

**undebug accelerator cifs [shell | all]**

**debug accelerator generic [connection | misc | shell | stats | all]**

**undebug accelerator generic [connection | misc | shell | stats | all]**

**debug accelerator http [cli | connection | shell | all]**

**undebug accelerator http [cli | connection | shell | all]**

**debug accelerator mapi [all | Common-flow | DCERPC-layer | EMSMDB-layer | IO | ROP-layer | ROP-parser | RCP-parser | shell | Transport | Utilities]**

**undebug accelerator mapi [all | Common-flow | DCERPC-layer | EMSMDB-layer | IO | ROP-layer | ROP-parser | RCP-parser | shell | Transport | Utilities]**

**debug accelerator nfs [async-write | attributes-cache | nfs-v3 | read-ahead | rpc | shell | utils | all]**

**undebug accelerator nfs [async-write | attributes-cache | nfs-v3 | read-ahead | rpc | shell | utils | all]**

**debug accelerator video [all | gateway | shell | windows-media  
[client-ip ip-addr | server-ip ip-addr]]**

**undebug accelerator video [all | gateway | shell | windows-media  
[client-ip ip-addr | server-ip ip-addr]]**

## Syntax Description

|                    |  |
|--------------------|--|
| <b>accelerator</b> | Enables accelerator debugging.                         |
| <b>cifs</b>        | (Optional) Enables CIFS accelerator debugging.         |
| <b>shell</b>       | Enables accelerator shell debugging.                   |
| <b>all</b>         | Enables all accelerator debugging of a specified type. |
| <b>generic</b>     | Enables generic accelerator debugging.                 |
| <b>connection</b>  | Enables accelerator connection debugging.              |
| <b>misc</b>        | Enables generic accelerator miscellaneous debugging.   |
| <b>stats</b>       | Enables generic accelerator statistics debugging.      |
| <b>http</b>        | Enables HTTP accelerator debugging.                    |
| <b>cli</b>         | Enables configuration CLI debugging.                   |
| <b>mapi</b>        | Enables MAPI accelerator debugging.                    |

|                          |   |
|--------------------------|---|
| <b>Common-flow</b>       | Enables MAPI common flow debugging.   |
| <b>DCERPC-layer</b>      | Enables MAPI DCERPC layer flow debugging.   |
| <b>EMSMDB-layer</b>      | Enables MAPI EMSMDB layer flow debugging.   |
| <b>IO</b>                | Enables MAPI IO flow debugging.   |
| <b>ROP-layer</b>         | Enables MAPI ROP layer flow debugging.  |
| <b>ROP-parser</b>        | Enables MAPI ROP parser flow debugging.   |
| <b>RCP-parser</b>        | Enables MAPI RCP parser flow debugging.   |
| <b>shell</b>             | Enables MAPI shell flow debugging.  |
| <b>Transport</b>         | Enables MAPI transport flow debugging.  |
| <b>Utilities</b>         | Enables MAPI utilities flow debugging.  |
| <b>nfs</b>               | Enables NFS accelerator debugging.  |
| <b>async-write</b>       | Enables NFS asynchronous write optimization debugging.                              |
| <b>attributes-cache</b>  | Enables NFS attributes cache debugging.   |
| <b>nfs-v3</b>            | Enables NFS version 3 layer debugging.  |
| <b>read-ahead</b>        | Enables NFS read ahead optimization debugging.                                      |
| <b>rpc</b>               | Enables NFS RPC layer debugging.  |
| <b>shell</b>             | Enables NFS shell debugging.  |
| <b>utils</b>             | Enables NFS utilities debugging.  |
| <b>video</b>             | Enables video accelerator debugging.  |
| <b>gateway</b>           | Enables debugging of the media independent gateway module of the video accelerator. |
| <b>windows-media</b>     | Enables debugging of the Windows Media module of the video accelerator.             |
| <b>client-ip ip-addr</b> | Specifies the client IP address.  |
| <b>server-ip ip-addr</b> | Specifies the server IP address.  |

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator  
central-manager

**Usage Guidelines** The output associated with the **debug accelerator name module** command for an application accelerator is written to the file *nameao-errorlog.current*, where *name* is the accelerator name. The accelerator information manager debug output is written to the file *aoim-errorlog.current*.

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 xx.

**debug accelerator**

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

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

The output associated with the **debug** command is written to either the syslog file in /local1/syslog.txt or the debug log associated with the module in the file /local1/errorlog/module\_name-errorlog.current.

The debug log file associated with a module will be rotated to a backup file when the current file reaches its maximum size. The backup files are named as follows: *name*-errorlog.#, where # is the backup file number.

For any **debug** command, system logging must be enabled. The command to enable logging is the **logging disk enable** global configuration command, which is enabled by default.

If a **debug** command module uses the syslog for debug output, then you must use the **logging disk priority debug** global configuration command (the default is **logging disk priority notice**).

If a **debug** command module uses the debug log for output, then the output can be filtered based on the priority level configuration for the four different levels of debug log output, as follows:

- For filtering on critical debug messages only, use the **logging disk priority critical** global configuration command.
- For filtering on critical and error level debug messages, use the **logging disk priority error** global configuration command.
- For filtering on critical, error, and trace debug level debug messages, use the **logging disk priority debug** global configuration command.
- For seeing all debug log messages, which include critical, error, trace and detail messages, use the **logging disk priority detail** global configuration command.

Regardless of the priority level configuration, any syslog messages at the LOG\_ERROR or higher priority will be automatically written to the debug log associated with a module.

We recommend that you use the **debug** and **undebbug** commands only at the direction of Cisco Systems technical support personnel.

**Examples**

The following example shows how to enable all accelerator debug monitoring:

```
WAE# debug accelerator all
```

**Related Commands**

[show debugging](#)

# debug all

To monitor and record all debugging, use the **debug all** EXEC command. To disable debugging, use the **undebug** form of this command.

**debug all**

**undebug all**

|                           |   |                        |
|---------------------------|---|------------------------|
| <b>Syntax Description</b> | <b>all</b>  | Enables all debugging. |
| <b>Defaults</b>           | No default behavior or values.  |                        |
| <b>Command Modes</b>      | EXEC  |                        |
| <b>Device Modes</b>       | application-accelerator<br>central-manager  |                        |
| <b>Usage Guidelines</b>   | <p>Because the performance of the WAAS device degrades when you use the <b>debug</b> command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the “<a href="#">Obtaining Documentation and Submitting a Service Request</a>” section on page xx.</p> <p>If the watchdog utility is not running, the message “WAAS is not running” appears.</p> <p>Use the <b>show debugging</b> command to display enabled <b>debug</b> options.</p> <p>The output associated with the <b>debug</b> command is written to either the syslog file in <code>/local1/syslog.txt</code> or the debug log associated with the module in the file <code>/local1/errorlog/module_name-errorlog.current</code>.</p> <p>The debug log file associated with a module will be rotated to a backup file when the current file reaches its maximum size. The backup files are named as follows: <code>name-errorlog.#</code>, where # is the backup file number.</p> <p>For any <b>debug</b> command, system logging must be enabled. The command to enable logging is the <b>logging disk enable</b> global configuration command, which is enabled by default.</p> <p>If a <b>debug</b> command module uses the syslog for debug output, then you must use the <b>logging disk priority debug</b> global configuration command (the default is <b>logging disk priority notice</b>).</p> <p>If a <b>debug</b> command module uses the debug log for output, then the output can be filtered based on the priority level configuration for the four different levels of debug log output, as follows:</p> <ul style="list-style-type: none"> <li>• For filtering on critical debug messages only, use the <b>logging disk priority critical</b> global configuration command.</li> <li>• For filtering on critical and error level debug messages, use the <b>logging disk priority error</b> global configuration command.</li> <li>• For filtering on critical, error, and trace debug level debug messages, use the <b>logging disk priority debug</b> global configuration command.</li> </ul> |                        |

**debug all**

- For seeing all debug log messages, which include critical, error, trace and detail messages, use the **logging disk priority detail** global configuration command.

Regardless of the priority level configuration, any syslog messages at the LOG\_ERROR or higher priority will be automatically written to the debug log associated with a module.

We recommend that you use the **debug** and **undebbug** commands only at the direction of Cisco Systems technical support personnel.

---

**Examples**

The following example shows how to enable all debug monitoring:

```
WAE# debug all
```

---

**Related Commands**

[show debugging](#)

# debug authentication

To monitor and record authentication debugging, use the **debug authentication** EXEC command. To disable debugging, use the **undebug** form of this command.

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

**undebug authentication {content-request | user | windows-domain}**

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> |  |
| <b>authentication</b>     | (Optional) Enables authentication debugging.                           |
| <b>content-request</b>    | Enables content request authentication debugging.                      |
| <b>user</b>               | Enables debugging of the user login against the system authentication. |
| <b>windows-domain</b>     | Enables Windows domain authentication debugging.                       |

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-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 xx.

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

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

The output associated with the **debug** command is written to either the syslog file in /local1/syslog.txt or the debug log associated with the module in the file /local1/errorlog/module\_name-errorlog.current.

The debug log file associated with a module will be rotated to a backup file when the current file reaches its maximum size. The backup files are named as follows: *name*-errorlog.#, where # is the backup file number.

For any **debug** command, system logging must be enabled. The command to enable logging is the **logging disk enable** global configuration command, which is enabled by default.

If a **debug** command module uses the syslog for debug output, then you must use the **logging disk priority debug** global configuration command (the default is **logging disk priority notice**).

If a **debug** command module uses the debug log for output, then the output can be filtered based on the priority level configuration for the four different levels of debug log output, as follows:

- For filtering on critical debug messages only, use the **logging disk priority critical** global configuration command.

**debug authentication**

- For filtering on critical and error level debug messages, use the **logging disk priority error** global configuration command.
- For filtering on critical, error, and trace debug level debug messages, use the **logging disk priority debug** global configuration command.
- For seeing all debug log messages, which include critical, error, trace and detail messages, use the **logging disk priority detail** global configuration command.

Regardless of the priority level configuration, any syslog messages at the LOG\_ERROR or higher priority will be automatically written to the debug log associated with a module.

We recommend that you use the **debug** and **undebbug** commands only at the direction of Cisco Systems technical support personnel.

---

**Examples**

The following example shows how to enable user authentication debug monitoring, verify that 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
```

---

**Related Commands**

[show debugging](#)

# debug buf

To monitor and record buffer manager debugging, use the **debug buf** EXEC command. To disable debugging, use the **undebuf** form of this command.

**debug buf {all | dmbuf | dmsg}**

**undebuf {all | dmbuf | dmsg}**

| Syntax Description |  |
|--------------------|--|
| <b>buf</b>         | (Optional) Enables buffer manager debugging. |
| <b>all</b>         | Enables all buffer manager debugging.        |
| <b>dmbuf</b>       | Enables only dmbuf debugging.                |
| <b>dmsg</b>        | Enables only dmsg debugging.                 |

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-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 xx.

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

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

The output associated with the **debug** command is written to either the syslog file in /local1/syslog.txt or the debug log associated with the module in the file /local1/errorlog/module\_name-errorlog.current.

The debug log file associated with a module will be rotated to a backup file when the current file reaches its maximum size. The backup files are named as follows: *name*-errorlog.*#*, where *#* is the backup file number.

For any **debug** command, system logging must be enabled. The command to enable logging is the **logging disk enable** global configuration command, which is enabled by default.

If a **debug** command module uses the syslog for debug output, then you must use the **logging disk priority debug** global configuration command (the default is **logging disk priority notice**).

If a **debug** command module uses the debug log for output, then the output can be filtered based on the priority level configuration for the four different levels of debug log output, as follows:

- For filtering on critical debug messages only, use the **logging disk priority critical** global configuration command.

**debug buf**

- For filtering on critical and error level debug messages, use the **logging disk priority error** global configuration command.
- For filtering on critical, error, and trace debug level debug messages, use the **logging disk priority debug** global configuration command.
- For seeing all debug log messages, which include critical, error, trace and detail messages, use the **logging disk priority detail** global configuration command.

Regardless of the priority level configuration, any syslog messages at the LOG\_ERROR or higher priority will be automatically written to the debug log associated with a module.

We recommend that you use the **debug** and **undebug** commands only at the direction of Cisco Systems technical support personnel.

---

**Examples**

The following example shows how to enable all buffer manager debug monitoring:

```
WAE# debug buff all
```

---

**Related Commands**

[show debugging](#)

# debug cdp

To monitor and record CDP debugging, use the **debug cdp** EXEC command. To disable debugging, use the **undebug** form of this command.

**debug cdp {adjacency | events | ip | packets}**

**undebug cdp {adjacency | events | ip | packets}**

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | <b>cdp</b> (Optional) Enables CDP debugging.<br><b>adjacency</b> Enables CDP neighbor information debugging.<br><b>events</b> Enables CDP events debugging.<br><b>ip</b> Enables CDP IP debugging.<br><b>packets</b> Enables packet-related CDP debugging. |
|---------------------------|--|

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-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 xx.

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

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

The output associated with the **debug** command is written to either the syslog file in /local1/syslog.txt or the debug log associated with the module in the file /local1/errorlog/module\_name-errorlog.current.

The debug log file associated with a module will be rotated to a backup file when the current file reaches its maximum size. The backup files are named as follows: *name*-errorlog.#, where # is the backup file number.

For any **debug** command, system logging must be enabled. The command to enable logging is the **logging disk enable** global configuration command, which is enabled by default.

If a **debug** command module uses the syslog for debug output, then you must use the **logging disk priority debug** global configuration command (the default is **logging disk priority notice**).

If a **debug** command module uses the debug log for output, then the output can be filtered based on the priority level configuration for the four different levels of debug log output, as follows:

- For filtering on critical debug messages only, use the **logging disk priority critical** global configuration command.

**debug cdp**

- For filtering on critical and error level debug messages, use the **logging disk priority error** global configuration command.
- For filtering on critical, error, and trace debug level debug messages, use the **logging disk priority debug** global configuration command.
- For seeing all debug log messages, which include critical, error, trace and detail messages, use the **logging disk priority detail** global configuration command.

Regardless of the priority level configuration, any syslog messages at the LOG\_ERROR or higher priority will be automatically written to the debug log associated with a module.

We recommend that you use the **debug** and **undebug** commands only at the direction of Cisco Systems technical support personnel.

---

**Examples**

The following example shows how to enable CDP events debug monitoring:

```
WAE# debug cdp events
```

---

**Related Commands**

[show debugging](#)

# debug cli

To monitor and record CLI debugging, use the **debug cli** EXEC command. To disable debugging, use the **undebug** form of this command.

**debug cli {all | bin | parser}**

**undebug cli {all | bin | parser}**

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | <b>cli</b> (Optional) Enables CLI debugging.<br><b>all</b> Enables all CLI debugging.<br><b>bin</b> Enables CLI command binary program debugging.<br><b>parser</b> Enables CLI command parser debugging. |
|---------------------------|--|

|                 |                                |
|-----------------|--------------------------------|
| <b>Defaults</b> | No default behavior or values. |
|-----------------|--------------------------------|

|                      |      |
|----------------------|------|
| <b>Command Modes</b> | EXEC |
|----------------------|------|

|                     |  |
|---------------------|--|
| <b>Device Modes</b> | application-accelerator<br>central-manager |
|---------------------|--|

|                         |  |
|-------------------------|--|
| <b>Usage Guidelines</b> | Because the performance of the WAAS device degrades when you use the <b>debug</b> command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the “ <a href="#">Obtaining Documentation and Submitting a Service Request</a> ” section on page xx. |
|-------------------------|--|

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

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

The output associated with the **debug** command is written to either the syslog file in /local1/syslog.txt or the debug log associated with the module in the file /local1/errorlog/module\_name-errorlog.current.

The debug log file associated with a module will be rotated to a backup file when the current file reaches its maximum size. The backup files are named as follows: *name*-errorlog.#, where # is the backup file number.

For any **debug** command, system logging must be enabled. The command to enable logging is the **logging disk enable** global configuration command, which is enabled by default.

If a **debug** command module uses the syslog for debug output, then you must use the **logging disk priority debug** global configuration command (the default is **logging disk priority notice**).

If a **debug** command module uses the debug log for output, then the output can be filtered based on the priority level configuration for the four different levels of debug log output, as follows:

- For filtering on critical debug messages only, use the **logging disk priority critical** global configuration command.

**debug cli**

- For filtering on critical and error level debug messages, use the **logging disk priority error** global configuration command.
- For filtering on critical, error, and trace debug level debug messages, use the **logging disk priority debug** global configuration command.
- For seeing all debug log messages, which include critical, error, trace and detail messages, use the **logging disk priority detail** global configuration command.

Regardless of the priority level configuration, any syslog messages at the LOG\_ERROR or higher priority will be automatically written to the debug log associated with a module.

We recommend that you use the **debug** and **undebug** commands only at the direction of Cisco Systems technical support personnel.

---

**Examples**

The following example shows how to enable all CLI debug monitoring:

```
WAE# debug cli all
```

---

**Related Commands**

[show debugging](#)

# debug cms

To monitor and record CMS debugging, use the **debug cms** EXEC command. To disable debugging, use the **undebbug cms** form of this command.

**debug cms**

**undebbug cms**

|                           |   |
|---------------------------|---|
| <b>Syntax Description</b> | <b>cms</b><br><br>(Optional) Enables CMS debugging.   |
| <b>Defaults</b>           | No default behavior or values.  |
| <b>Command Modes</b>      | EXEC  |
| <b>Device Modes</b>       | application-accelerator<br>central-manager  |
| <b>Usage Guidelines</b>   | <p>Because the performance of the WAAS device degrades when you use the <b>debug</b> command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the “<a href="#">Obtaining Documentation and Submitting a Service Request</a>” section on page xx.</p> <p>If the watchdog utility is not running, the message “WAAS is not running” appears.</p> <p>Use the <b>show debugging</b> command to display enabled <b>debug</b> options.</p> <p>The output associated with the <b>debug</b> command is written to either the syslog file in /local1/syslog.txt or the debug log associated with the module in the file /local1/errorlog/module_name-errorlog.current.</p> <p>The debug log file associated with a module will be rotated to a backup file when the current file reaches its maximum size. The backup files are named as follows: <i>name</i>-errorlog.#, where # is the backup file number.</p> <p>For any <b>debug</b> command, system logging must be enabled. The command to enable logging is the <b>logging disk enable</b> global configuration command, which is enabled by default.</p> <p>If a <b>debug</b> command module uses the syslog for debug output, then you must use the <b>logging disk priority debug</b> global configuration command (the default is <b>logging disk priority notice</b>).</p> <p>If a <b>debug</b> command module uses the debug log for output, then the output can be filtered based on the priority level configuration for the four different levels of debug log output, as follows:</p> <ul style="list-style-type: none"> <li>• For filtering on critical debug messages only, use the <b>logging disk priority critical</b> global configuration command.</li> <li>• For filtering on critical and error level debug messages, use the <b>logging disk priority error</b> global configuration command.</li> <li>• For filtering on critical, error, and trace debug level debug messages, use the <b>logging disk priority debug</b> global configuration command.</li> </ul> |

**debug cms**

- For seeing all debug log messages, which include critical, error, trace and detail messages, use the **logging disk priority detail** global configuration command.

Regardless of the priority level configuration, any syslog messages at the LOG\_ERROR or higher priority will be automatically written to the debug log associated with a module.

We recommend that you use the **debug** and **undebbug** commands only at the direction of Cisco Systems technical support personnel.

---

**Examples**

The following example shows how to enable CMS debug monitoring:

```
WAE# debug cms
```

---

**Related Commands**

[show debugging](#)

# debug dataserver

To monitor and record data server debugging, use the **debug dataserver** EXEC command. To disable debugging, use the **undebug** form of this command.

**debug dataserver {all | clientlib | server}**

**undebug dataserver {all | clientlib | server}**

| Syntax Description | <b>dataserver</b> (Optional) Enables data server debugging.<br><b>all</b> Enables all data server debugging.<br><b>clientlib</b> Enables data server client library module debugging.<br><b>server</b> Enables data server module debugging. |
|--------------------|--|
|--------------------|--|

|          |                                |
|----------|--------------------------------|
| Defaults | No default behavior or values. |
|----------|--------------------------------|

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

|              |  |
|--------------|--|
| Device Modes | application-accelerator<br>central-manager |
|--------------|--|

|                  |  |
|------------------|--|
| Usage Guidelines | Because the performance of the WAAS device degrades when you use the <b>debug</b> command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the “ <a href="#">Obtaining Documentation and Submitting a Service Request</a> ” section on page xx. |
|------------------|--|

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

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

The output associated with the **debug** command is written to either the syslog file in /local1/syslog.txt or the debug log associated with the module in the file /local1/errorlog/module\_name-errorlog.current.

The debug log file associated with a module will be rotated to a backup file when the current file reaches its maximum size. The backup files are named as follows: *name*-errorlog.#, where # is the backup file number.

For any **debug** command, system logging must be enabled. The command to enable logging is the **logging disk enable** global configuration command, which is enabled by default.

If a **debug** command module uses the syslog for debug output, then you must use the **logging disk priority debug** global configuration command (the default is **logging disk priority notice**).

If a **debug** command module uses the debug log for output, then the output can be filtered based on the priority level configuration for the four different levels of debug log output, as follows:

- For filtering on critical debug messages only, use the **logging disk priority critical** global configuration command.

**debug dataserver**

- For filtering on critical and error level debug messages, use the **logging disk priority error** global configuration command.
- For filtering on critical, error, and trace debug level debug messages, use the **logging disk priority debug** global configuration command.
- For seeing all debug log messages, which include critical, error, trace and detail messages, use the **logging disk priority detail** global configuration command.

Regardless of the priority level configuration, any syslog messages at the LOG\_ERROR or higher priority will be automatically written to the debug log associated with a module.

We recommend that you use the **debug** and **undebug** commands only at the direction of Cisco Systems technical support personnel.

---

**Examples**

The following example shows how to enable all data server debug monitoring:

```
WAE# debug dataserver all
```

---

**Related Commands**

[show debugging](#)

# debug dhcp

To monitor and record DHCP debugging, use the **debug dhcp** EXEC command. To disable debugging, use the **undebug** form of this command.

**debug dhcp**

**undebug dhcp**

|                           |   |
|---------------------------|---|
| <b>Syntax Description</b> | <b>dhcp</b> (Optional) Enables DHCP debugging.  |
| <b>Defaults</b>           | No default behavior or values.  |
| <b>Command Modes</b>      | EXEC  |
| <b>Device Modes</b>       | application-accelerator<br>central-manager  |
| <b>Usage Guidelines</b>   | <p>Because the performance of the WAAS device degrades when you use the <b>debug</b> command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the “<a href="#">Obtaining Documentation and Submitting a Service Request</a>” section on page xx.</p> <p>If the watchdog utility is not running, the message “WAAS is not running” appears.</p> <p>Use the <b>show debugging</b> command to display enabled <b>debug</b> options.</p> <p>The output associated with the <b>debug</b> command is written to either the syslog file in <code>/local1/syslog.txt</code> or the debug log associated with the module in the file <code>/local1/errorlog/module_name-errorlog.current</code>.</p> <p>The debug log file associated with a module will be rotated to a backup file when the current file reaches its maximum size. The backup files are named as follows: <code>name-errorlog.#</code>, where # is the backup file number.</p> <p>For any <b>debug</b> command, system logging must be enabled. The command to enable logging is the <b>logging disk enable</b> global configuration command, which is enabled by default.</p> <p>If a <b>debug</b> command module uses the syslog for debug output, then you must use the <b>logging disk priority debug</b> global configuration command (the default is <b>logging disk priority notice</b>).</p> <p>If a <b>debug</b> command module uses the debug log for output, then the output can be filtered based on the priority level configuration for the four different levels of debug log output, as follows:</p> <ul style="list-style-type: none"> <li>• For filtering on critical debug messages only, use the <b>logging disk priority critical</b> global configuration command.</li> <li>• For filtering on critical and error level debug messages, use the <b>logging disk priority error</b> global configuration command.</li> <li>• For filtering on critical, error, and trace debug level debug messages, use the <b>logging disk priority debug</b> global configuration command.</li> </ul> |

**debug dhcp**

- For seeing all debug log messages, which include critical, error, trace and detail messages, use the **logging disk priority detail** global configuration command.

Regardless of the priority level configuration, any syslog messages at the LOG\_ERROR or higher priority will be automatically written to the debug log associated with a module.

We recommend that you use the **debug** and **undebbug** commands only at the direction of Cisco Systems technical support personnel.

---

**Examples**

The following example shows how to enable DHCP debug monitoring:

```
WAE# debug dhcp
```

---

**Related Commands**

[show debugging](#)

## debug dre

To monitor and record DRE debugging, use the **debug dre** EXEC command. To disable debugging, use the **undebug** form of this command.

```
debug dre {aggregation | all | cache | connection {aggregation [acl] | cache [acl] | core [acl] | message [acl] | misc [acl] | acl} | core | lz | message | misc}
```

```
undebug dre {aggregation | all | cache | connection {aggregation [acl] | cache [acl] | core [acl] | message [acl] | misc [acl] | acl} | core | lz | message | misc}
```

| Syntax Description |   |
|--------------------|---|
| <b>dre</b>         | (Optional) Enables DRE debugging.                         |
| <b>aggregation</b> | Enables DRE chunk-aggregation debugging.                  |
| <b>all</b>         | Enables the debugging of all DRE commands.                |
| <b>cache</b>       | Enables DRE cache debugging.                              |
| <b>connection</b>  | Enables DRE connection debugging.                         |
| <b>acl</b>         | ACL to limit connections traced.                          |
| <b>message</b>     | Enables DRE message debugging for a specified connection. |
| <b>misc</b>        | Enables DRE other debugging for a specified connection.   |
| <b>core</b>        | Enables DRE core debugging.                               |
| <b>lz</b>          | Enables DRE lz debugging.                                 |

|          |                                |
|----------|--------------------------------|
| Defaults | No default behavior or values. |
|----------|--------------------------------|

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

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

|                  |  |
|------------------|--|
| Usage Guidelines | Because the performance of the WAAS device degrades when you use the <b>debug</b> command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the “ <a href="#">Obtaining Documentation and Submitting a Service Request</a> ” section on page xx. |
|------------------|--|

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

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

The output associated with the **debug** command is written to either the syslog file in /local1/syslog.txt or the debug log associated with the module in the file /local1/errorlog/module\_name-errorlog.current.

The debug log file associated with a module will be rotated to a backup file when the current file reaches its maximum size. The backup files are named as follows: *name*-errorlog.#, where # is the backup file number.

For any **debug** command, system logging must be enabled. The command to enable logging is the **logging disk enable** global configuration command, which is enabled by default.

**debug dre**

If a **debug** command module uses the syslog for debug output, then you must use the **logging disk priority debug** global configuration command (the default is **logging disk priority notice**).

If a **debug** command module uses the debug log for output, then the output can be filtered based on the priority level configuration for the four different levels of debug log output, as follows:

- For filtering on critical debug messages only, use the **logging disk priority critical** global configuration command.
- For filtering on critical and error level debug messages, use the **logging disk priority error** global configuration command.
- For filtering on critical, error, and trace debug level debug messages, use the **logging disk priority debug** global configuration command.
- For seeing all debug log messages, which include critical, error, trace and detail messages, use the **logging disk priority detail** global configuration command.

Regardless of the priority level configuration, any syslog messages at the LOG\_ERROR or higher priority will be automatically written to the debug log associated with a module.

We recommend that you use the **debug** and **undebug** commands only at the direction of Cisco Systems technical support personnel.

---

**Examples**

The following example shows how to enable all DRE debug monitoring:

```
WAE# debug dre all
```

---

**Related Commands**

[show debugging](#)

# debug egress-method

To monitor and record egress method debugging, use the **debug egress-method** EXEC command. To disable debugging, use the **undebug** form of this command.

**debug egress-method connection**

**undebug egress-method connection**

|                           |   |
|---------------------------|---|
| <b>Syntax Description</b> | <b>egress-method connection</b> (Optional) Enables egress method connection debugging.  |
| <b>Defaults</b>           | No default behavior or values.  |
| <b>Command Modes</b>      | EXEC  |
| <b>Device Modes</b>       | application-accelerator   |
| <b>Usage Guidelines</b>   | <p>Because the performance of the WAAS device degrades when you use the <b>debug</b> command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the <a href="#">“Obtaining Documentation and Submitting a Service Request” section on page xx</a>.</p> <p>If the watchdog utility is not running, the message “WAAS is not running” appears.</p> <p>Use the <b>show debugging</b> command to display enabled <b>debug</b> options.</p> <p>The output associated with the <b>debug</b> command is written to either the syslog file in /local1/syslog.txt or the debug log associated with the module in the file /local1/errorlog/module_name-errorlog.current.</p> <p>The debug log file associated with a module will be rotated to a backup file when the current file reaches its maximum size. The backup files are named as follows: <i>name</i>-errorlog.<i>#</i>, where <i>#</i> is the backup file number.</p> <p>For any <b>debug</b> command, system logging must be enabled. The command to enable logging is the <b>logging disk enable</b> global configuration command, which is enabled by default.</p> <p>If a <b>debug</b> command module uses the syslog for debug output, then you must use the <b>logging disk priority debug</b> global configuration command (the default is <b>logging disk priority notice</b>).</p> <p>If a <b>debug</b> command module uses the debug log for output, then the output can be filtered based on the priority level configuration for the four different levels of debug log output, as follows:</p> <ul style="list-style-type: none"> <li>• For filtering on critical debug messages only, use the <b>logging disk priority critical</b> global configuration command.</li> <li>• For filtering on critical and error level debug messages, use the <b>logging disk priority error</b> global configuration command.</li> <li>• For filtering on critical, error, and trace debug level debug messages, use the <b>logging disk priority debug</b> global configuration command.</li> </ul> |

**debug egress-method**

- For seeing all debug log messages, which include critical, error, trace and detail messages, use the **logging disk priority detail** global configuration command.

Regardless of the priority level configuration, any syslog messages at the LOG\_ERROR or higher priority will be automatically written to the debug log associated with a module.

We recommend that you use the **debug** and **undebbug** commands only at the direction of Cisco Systems technical support personnel.

---

**Examples**

The following example shows how to enable all egress method debug monitoring:

```
WAE# debug egress-method connection
```

---

**Related Commands**

[show debugging](#)

# debug emdb

To monitor and record embedded database debugging, use the **debug emdb** EXEC command. To disable debugging, use the **undebbug** form of this command.

**debug emdb [level [levelnum]]**

**undebbug emdb [level [levelnum]]**

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | <b>emdb</b> (Optional) Enables embedded database debugging.<br><b>level</b> (Optional) Enables the specified debug level for EMDB service.<br><b>levelnum</b> (Optional) Debug level to disable. Level 0 disables debugging. |
|---------------------------|--|

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** 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 xx.

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

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

The output associated with the **debug** command is written to either the syslog file in /local1/syslog.txt or the debug log associated with the module in the file /local1/errorlog/module\_name-errorlog.current.

The debug log file associated with a module will be rotated to a backup file when the current file reaches its maximum size. The backup files are named as follows: *name*-errorlog.#, where # is the backup file number.

For any **debug** command, system logging must be enabled. The command to enable logging is the **logging disk enable** global configuration command, which is enabled by default.

If a **debug** command module uses the syslog for debug output, then you must use the **logging disk priority debug** global configuration command (the default is **logging disk priority notice**).

If a **debug** command module uses the debug log for output, then the output can be filtered based on the priority level configuration for the four different levels of debug log output, as follows:

- For filtering on critical debug messages only, use the **logging disk priority critical** global configuration command.
- For filtering on critical and error level debug messages, use the **logging disk priority error** global configuration command.

**debug emdb**

- For filtering on critical, error, and trace debug level debug messages, use the **logging disk priority debug** global configuration command.
- For seeing all debug log messages, which include critical, error, trace and detail messages, use the **logging disk priority detail** global configuration command.

Regardless of the priority level configuration, any syslog messages at the LOG\_ERROR or higher priority will be automatically written to the debug log associated with a module.

We recommend that you use the **debug** and **undebug** commands only at the direction of Cisco Systems technical support personnel.

---

**Examples**

The following example shows how to enable all embedded database debug monitoring:

```
WAE# debug emdb all
```

---

**Related Commands**[show debugging](#)

# debug epm

To monitor and record DCE-RPC EPM debugging, use the **debug epm** EXEC command. To disable debugging, use the **undebbug** form of this command.

**debug** **epm**

**undeb**bug epm

|                           |  |   |
|---------------------------|--|---|
| <b>Syntax Description</b> | <b>epm</b>   | (Optional) Enables DCE-RPC EPM debugging. |
| <b>Defaults</b>           | No default behavior or values.   |   |
| <b>Command Modes</b>      | EXEC   |   |
| <b>Device Modes</b>       | application-accelerator  |   |
| <b>Usage Guidelines</b>   | <p>Because the performance of the WAAS device degrades when you use the <b>debug</b> command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the “<a href="#">Obtaining Documentation and Submitting a Service Request</a>” section on page <a href="#">xx</a>.</p> <p>If the watchdog utility is not running, the message “WAAS is not running” appears.</p> <p>Use the <b>show debugging</b> command to display enabled <b>debug</b> options.</p> <p>The output associated with the <b>debug</b> command is written to either the syslog file in <code>/local1/syslog.txt</code> or the debug log associated with the module in the file <code>/local1/errorlog/module_name-errorlog.current</code>.</p> <p>The debug log file associated with a module will be rotated to a backup file when the current file reaches its maximum size. The backup files are named as follows: <code>name-errorlog.#</code>, where <code>#</code> is the backup file number.</p> <p>For any <b>debug</b> command, system logging must be enabled. The command to enable logging is the <b>logging disk enable</b> global configuration command, which is enabled by default.</p> <p>If a <b>debug</b> command module uses the syslog for debug output, then you must use the <b>logging disk priority debug</b> global configuration command (the default is <b>logging disk priority notice</b>).</p> <p>If a <b>debug</b> command module uses the debug log for output, then the output can be filtered based on the priority level configuration for the four different levels of debug log output, as follows:</p> <ul style="list-style-type: none"> <li>• For filtering on critical debug messages only, use the <b>logging disk priority critical</b> global configuration command.</li> <li>• For filtering on critical and error level debug messages, use the <b>logging disk priority error</b> global configuration command.</li> <li>• For filtering on critical, error, and trace debug level debug messages, use the <b>logging disk priority debug</b> global configuration command.</li> </ul> |   |

**debug epm**

- For seeing all debug log messages, which include critical, error, trace and detail messages, use the **logging disk priority detail** global configuration command.

Regardless of the priority level configuration, any syslog messages at the LOG\_ERROR or higher priority will be automatically written to the debug log associated with a module.

We recommend that you use the **debug** and **undebug** commands only at the direction of Cisco Systems technical support personnel.

---

**Examples**

The following example shows how to enable EPM debug monitoring:

```
WAE# debug epm
```

---

**Related Commands**

[show debugging](#)

# debug flow

To monitor and record network traffic flow debugging, use the **debug flow** EXEC command. To disable debugging, use the **undebbug** form of this command.

**debug flow monitor tcpstat-v1**

**undebbug flow monitor tcpstat-v1**

|                           |   |             |  |                |  |                   |                               |
|---------------------------|---|-------------|--|----------------|--|-------------------|-------------------------------|
| <b>Syntax Description</b> | <table border="1"> <tr> <td><b>flow</b></td><td>(Optional) Enables network traffic flow debugging.</td></tr> <tr> <td><b>monitor</b></td><td>Enables monitor flow performance debugging commands.</td></tr> <tr> <td><b>tcpstat-v1</b></td><td>Enables tcpstat-v1 debugging.</td></tr> </table> | <b>flow</b> | (Optional) Enables network traffic flow debugging. | <b>monitor</b> | Enables monitor flow performance debugging commands. | <b>tcpstat-v1</b> | Enables tcpstat-v1 debugging. |
| <b>flow</b>               | (Optional) Enables network traffic flow debugging.  |             |  |                |  |                   |                               |
| <b>monitor</b>            | Enables monitor flow performance debugging commands.  |             |  |                |  |                   |                               |
| <b>tcpstat-v1</b>         | Enables tcpstat-v1 debugging.   |             |  |                |  |                   |                               |

|                 |                                |
|-----------------|--------------------------------|
| <b>Defaults</b> | No default behavior or values. |
|-----------------|--------------------------------|

|                      |      |
|----------------------|------|
| <b>Command Modes</b> | EXEC |
|----------------------|------|

|                     |                         |
|---------------------|-------------------------|
| <b>Device Modes</b> | application-accelerator |
|---------------------|-------------------------|

|                         |  |
|-------------------------|--|
| <b>Usage Guidelines</b> | Because the performance of the WAAS device degrades when you use the <b>debug</b> command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the “ <a href="#">Obtaining Documentation and Submitting a Service Request</a> ” section on page xx. |
|-------------------------|--|

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

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

The output associated with the **debug** command is written to either the syslog file in /local1/syslog.txt or the debug log associated with the module in the file /local1/errorlog/module\_name-errorlog.current.

The debug log file associated with a module will be rotated to a backup file when the current file reaches its maximum size. The backup files are named as follows: *name*-errorlog.#, where # is the backup file number.

For any **debug** command, system logging must be enabled. The command to enable logging is the **logging disk enable** global configuration command, which is enabled by default.

If a **debug** command module uses the syslog for debug output, then you must use the **logging disk priority debug** global configuration command (the default is **logging disk priority notice**).

If a **debug** command module uses the debug log for output, then the output can be filtered based on the priority level configuration for the four different levels of debug log output, as follows:

- For filtering on critical debug messages only, use the **logging disk priority critical** global configuration command.
- For filtering on critical and error level debug messages, use the **logging disk priority error** global configuration command.

**debug flow**

- For filtering on critical, error, and trace debug level debug messages, use the **logging disk priority debug** global configuration command.
- For seeing all debug log messages, which include critical, error, trace and detail messages, use the **logging disk priority detail** global configuration command.

Regardless of the priority level configuration, any syslog messages at the LOG\_ERROR or higher priority will be automatically written to the debug log associated with a module.

We recommend that you use the **debug** and **undebug** commands only at the direction of Cisco Systems technical support personnel.

---

**Examples**

The following example shows how to enable network traffic flow debug monitoring:

```
WAE# debug flow monitor tcpstat-v1
```

---

**Related Commands**

[show debugging](#)

# debug generic-gre

To monitor and record generic GRE egress method debugging, use the **debug generic-gre** EXEC command. To disable debugging, use the **undebbug** form of this command.

**debug generic-gre**

**undebbug generic-gre**

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | generic-gre<br><br>(Optional) Enables generic GRE egress method debugging.   |
| <b>Defaults</b>           | No default behavior or values.   |
| <b>Command Modes</b>      | EXEC   |
| <b>Device Modes</b>       | application-accelerator<br>central-manager   |
| <b>Usage Guidelines</b>   | <p>Because the performance of the WAAS device degrades when you use the <b>debug</b> command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the “<a href="#">Obtaining Documentation and Submitting a Service Request</a>” section on page xx.</p> <p>If the watchdog utility is not running, the message “WAAS is not running” appears.</p> <p>Use the <b>show debugging</b> command to display enabled <b>debug</b> options.</p> <p>The output associated with the <b>debug</b> command is written to either the syslog file in /local1/syslog.txt or the debug log associated with the module in the file /local1/errorlog/module_name-errorlog.current. The debug log file associated with a module will be rotated to a backup file when the current file reaches its maximum size. The backup files are named as follows: <i>name</i>-errorlog.#, where # is the backup file number.</p> <p>For any <b>debug</b> command, system logging must be enabled. The command to enable logging is the <b>logging disk enable</b> global configuration command, which is enabled by default.</p> <p>If a <b>debug</b> command module uses the syslog for debug output, then you must use the <b>logging disk priority debug</b> global configuration command (the default is <b>logging disk priority notice</b>).</p> <p>If a <b>debug</b> command module uses the debug log for output, then the output can be filtered based on the priority level configuration for the four different levels of debug log output, as follows:</p> <ul style="list-style-type: none"> <li>• For filtering on critical debug messages only, use the <b>logging disk priority critical</b> global configuration command.</li> <li>• For filtering on critical and error level debug messages, use the <b>logging disk priority error</b> global configuration command.</li> <li>• For filtering on critical, error, and trace debug level debug messages, use the <b>logging disk priority debug</b> global configuration command.</li> </ul> |

```
■ debug generic-gre
```

- For seeing all debug log messages, which include critical, error, trace and detail messages, use the **logging disk priority detail** global configuration command.

Regardless of the priority level configuration, any syslog messages at the LOG\_ERROR or higher priority will be automatically written to the debug log associated with a module.

We recommend that you use the **debug** and **undebbug** commands only at the direction of Cisco Systems technical support personnel.

---

**Examples**

The following example shows how to enable generic GRE egress method debug monitoring:

```
WAE# debug generic-gre
```

---

**Related Commands**

[show debugging](#)

# debug key-manager

To monitor and record Central Manager key manager debugging, use the **debug key-manager** EXEC command. To disable debugging, use the **undebbug** form of this command.

## debug key-manager

## **undebug key-manager**

| Syntax Description | key-manager  | (Optional) Enables the Central Manager key manager debugging. |
|--------------------|--|---|
| Defaults           | No default behavior or values.   |   |
| Command Modes      | EXEC   |   |
| Device Modes       | application-accelerator<br>central-manager   |   |
| Usage Guidelines   | <p>Because the performance of the WAAS device degrades when you use the <b>debug</b> command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the “<a href="#">Obtaining Documentation and Submitting a Service Request</a>” section on page xx.</p> <p>If the watchdog utility is not running, the message “WAAS is not running” appears.</p> <p>Use the <b>show debugging</b> command to display enabled <b>debug</b> options.</p> <p>The output associated with the <b>debug</b> command is written to either the syslog file in /local1/syslog.txt or the debug log associated with the module in the file /local1/errorlog/module_name-errorlog.current. The debug log file associated with a module will be rotated to a backup file when the current file reaches its maximum size. The backup files are named as follows: <i>name-errorlog.#</i>, where # is the backup file number.</p> <p>For any <b>debug</b> command, system logging must be enabled. The command to enable logging is the <b>logging disk enable</b> global configuration command, which is enabled by default.</p> <p>If a <b>debug</b> command module uses the syslog for debug output, then you must use the <b>logging disk priority debug</b> global configuration command (the default is <b>logging disk priority notice</b>).</p> <p>If a <b>debug</b> command module uses the debug log for output, then the output can be filtered based on the priority level configuration for the four different levels of debug log output, as follows:</p> <ul style="list-style-type: none"> <li>• For filtering on critical debug messages only, use the <b>logging disk priority critical</b> global configuration command.</li> <li>• For filtering on critical and error level debug messages, use the <b>logging disk priority error</b> global configuration command.</li> <li>• For filtering on critical, error, and trace debug level debug messages, use the <b>logging disk priority debug</b> global configuration command.</li> </ul> |   |

**debug key-manager**

- For seeing all debug log messages, which include critical, error, trace and detail messages, use the **logging disk priority detail** global configuration command.

Regardless of the priority level configuration, any syslog messages at the LOG\_ERROR or higher priority will be automatically written to the debug log associated with a module.

We recommend that you use the **debug** and **undebbug** commands only at the direction of Cisco Systems technical support personnel.

---

**Examples**

The following example shows how to enable Central Manager key manager debug monitoring:

```
WAE# debug key-manager
```

---

**Related Commands**

[show debugging](#)

# debug logging

To monitor and record logging debugging, use the **debug logging** EXEC command. To disable debugging, use the **undebbug** form of this command.

**debug logging all**

**undebbug logging all**

|                           |   |
|---------------------------|---|
| <b>Syntax Description</b> | <b>logging</b> (Optional) Enables logging debugging.<br><b>all</b> Enables all logging debugging.   |
| <b>Defaults</b>           | No default behavior or values.  |
| <b>Command Modes</b>      | EXEC  |
| <b>Device Modes</b>       | application-accelerator<br>central-manager  |
| <b>Usage Guidelines</b>   | <p>Because the performance of the WAAS device degrades when you use the <b>debug</b> command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the <a href="#">“Obtaining Documentation and Submitting a Service Request” section on page xx</a>.</p> <p>If the watchdog utility is not running, the message “WAAS is not running” appears.</p> <p>Use the <b>show debugging</b> command to display enabled <b>debug</b> options.</p> <p>The output associated with the <b>debug</b> command is written to either the syslog file in /local1/syslog.txt or the debug log associated with the module in the file /local1/errorlog/module_name-errorlog.current.</p> <p>The debug log file associated with a module will be rotated to a backup file when the current file reaches its maximum size. The backup files are named as follows: <i>name</i>-errorlog.#, where # is the backup file number.</p> <p>For any <b>debug</b> command, system logging must be enabled. The command to enable logging is the <b>logging disk enable</b> global configuration command, which is enabled by default.</p> <p>If a <b>debug</b> command module uses the syslog for debug output, then you must use the <b>logging disk priority debug</b> global configuration command (the default is <b>logging disk priority notice</b>).</p> <p>If a <b>debug</b> command module uses the debug log for output, then the output can be filtered based on the priority level configuration for the four different levels of debug log output, as follows:</p> <ul style="list-style-type: none"> <li>• For filtering on critical debug messages only, use the <b>logging disk priority critical</b> global configuration command.</li> <li>• For filtering on critical and error level debug messages, use the <b>logging disk priority error</b> global configuration command.</li> </ul> |

**debug logging**

- For filtering on critical, error, and trace debug level debug messages, use the **logging disk priority debug** global configuration command.
- For seeing all debug log messages, which include critical, error, trace and detail messages, use the **logging disk priority detail** global configuration command.

Regardless of the priority level configuration, any syslog messages at the LOG\_ERROR or higher priority will be automatically written to the debug log associated with a module.

We recommend that you use the **debug** and **undebug** commands only at the direction of Cisco Systems technical support personnel.

---

**Examples**

The following example shows how to enable all logging debug monitoring:

```
WAE# debug logging all
```

---

**Related Commands**

[show debugging](#)

# debug ntp

To monitor and record NTP debugging, use the **debug ntp** EXEC command. To disable debugging, use the **undebbug** form of this command.(

**debug ntp**

**undebbug ntp**

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | <b>ntp</b> (Optional) Enables NTP debugging.   |
| <b>Defaults</b>           | No default behavior or values.   |
| <b>Command Modes</b>      | EXEC   |
| <b>Device Modes</b>       | application-accelerator<br>central-manager   |
| <b>Usage Guidelines</b>   | <p>Because the performance of the WAAS device degrades when you use the <b>debug</b> command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the “<a href="#">Obtaining Documentation and Submitting a Service Request</a>” section on page xx.</p> <p>If the watchdog utility is not running, the message “WAAS is not running” appears.</p> <p>Use the <b>show debugging</b> command to display enabled <b>debug</b> options.</p> <p>The output associated with the <b>debug</b> command is written to either the syslog file in /local1/syslog.txt or the debug log associated with the module in the file /local1/errorlog/module_name-errorlog.current. The debug log file associated with a module will be rotated to a backup file when the current file reaches its maximum size. The backup files are named as follows: <i>name</i>-errorlog.#, where # is the backup file number.</p> <p>For any <b>debug</b> command, system logging must be enabled. The command to enable logging is the <b>logging disk enable</b> global configuration command, which is enabled by default.</p> <p>If a <b>debug</b> command module uses the syslog for debug output, then you must use the <b>logging disk priority debug</b> global configuration command (the default is <b>logging disk priority notice</b>).</p> <p>If a <b>debug</b> command module uses the debug log for output, then the output can be filtered based on the priority level configuration for the four different levels of debug log output, as follows:</p> <ul style="list-style-type: none"> <li>• For filtering on critical debug messages only, use the <b>logging disk priority critical</b> global configuration command.</li> <li>• For filtering on critical and error level debug messages, use the <b>logging disk priority error</b> global configuration command.</li> <li>• For filtering on critical, error, and trace debug level debug messages, use the <b>logging disk priority debug</b> global configuration command.</li> </ul> |

**debug ntp**

- For seeing all debug log messages, which include critical, error, trace and detail messages, use the **logging disk priority detail** global configuration command.

Regardless of the priority level configuration, any syslog messages at the LOG\_ERROR or higher priority will be automatically written to the debug log associated with a module.

We recommend that you use the **debug** and **undebbug** commands only at the direction of Cisco Systems technical support personnel.

---

**Examples**

The following example shows how to enable NTP debug monitoring:

```
WAE# debug ntp
```

---

**Related Commands**

[show debugging](#)

# debug print-spooler

To monitor and record print spooler debugging, use the **debug print-spooler** EXEC command. To disable debugging, use the **undebug** form of this command.

**debug print-spooler {all | brief | errors | warnings}**

**undebug print-spooler {all | brief | errors | warnings}**

| Syntax Description   |  |
|----------------------|--|
| <b>print-spooler</b> | (Optional) Enables print spooler debugging.                        |
| <b>all</b>           | Enables print spooler debugging using all debug features.          |
| <b>brief</b>         | Enables print spooler debugging using only brief debug messages.   |
| <b>errors</b>        | Enables print spooler debugging using only the error conditions.   |
| <b>warnings</b>      | Enables print spooler debugging using only the warning conditions. |

|          |                                |
|----------|--------------------------------|
| Defaults | No default behavior or values. |
|----------|--------------------------------|

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

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

|                  |   |
|------------------|---|
| Usage Guidelines | Because the performance of the WAAS device degrades when you use the <b>debug</b> command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the <a href="#">“Obtaining Documentation and Submitting a Service Request” section on page xx</a> . |
|------------------|---|

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

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

The output associated with the **debug** command is written to either the syslog file in /local1/syslog.txt or the debug log associated with the module in the file /local1/errorlog/module\_name-errorlog.current.

The debug log file associated with a module will be rotated to a backup file when the current file reaches its maximum size. The backup files are named as follows: *name*-errorlog.*#*, where *#* is the backup file number.

For any **debug** command, system logging must be enabled. The command to enable logging is the **logging disk enable** global configuration command, which is enabled by default.

If a **debug** command module uses the syslog for debug output, then you must use the **logging disk priority debug** global configuration command (the default is **logging disk priority notice**).

If a **debug** command module uses the debug log for output, then the output can be filtered based on the priority level configuration for the four different levels of debug log output, as follows:

- For filtering on critical debug messages only, use the **logging disk priority critical** global configuration command.

**debug print-spooler**

- For filtering on critical and error level debug messages, use the **logging disk priority error** global configuration command.
- For filtering on critical, error, and trace debug level debug messages, use the **logging disk priority debug** global configuration command.
- For seeing all debug log messages, which include critical, error, trace and detail messages, use the **logging disk priority detail** global configuration command.

Regardless of the priority level configuration, any syslog messages at the LOG\_ERROR or higher priority will be automatically written to the debug log associated with a module.

We recommend that you use the **debug** and **undebug** commands only at the direction of Cisco Systems technical support personnel.

---

**Examples**

The following example shows how to enable all print spooler debug monitoring:

```
WAE# debug print-spooler all
```

---

**Related Commands**

[show debugging](#)

# debug rbcpc

To monitor and record RBCP debugging, use the **debug rbcpc** EXEC command. To disable debugging, use the **undebbug** form of this command.

**debug rbcpc**

**undebbug rbcpc**

|                           |   |
|---------------------------|---|
| <b>Syntax Description</b> | <b>rbcpc</b> (Optional) Enables RBCP debugging.   |
| <b>Defaults</b>           | No default behavior or values.  |
| <b>Command Modes</b>      | EXEC  |
| <b>Device Modes</b>       | application-accelerator   |
| <b>Usage Guidelines</b>   | <p>Because the performance of the WAAS device degrades when you use the <b>debug</b> command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the <a href="#">“Obtaining Documentation and Submitting a Service Request” section on page xx</a>.</p> <p>If the watchdog utility is not running, the message “WAAS is not running” appears.</p> <p>Use the <b>show debugging</b> command to display enabled <b>debug</b> options.</p> <p>The output associated with the <b>debug</b> command is written to either the syslog file in /local1/syslog.txt or the debug log associated with the module in the file /local1/errorlog/module_name-errorlog.current.</p> <p>The debug log file associated with a module will be rotated to a backup file when the current file reaches its maximum size. The backup files are named as follows: <i>name</i>-errorlog.<i>#</i>, where <i>#</i> is the backup file number.</p> <p>For any <b>debug</b> command, system logging must be enabled. The command to enable logging is the <b>logging disk enable</b> global configuration command, which is enabled by default.</p> <p>If a <b>debug</b> command module uses the syslog for debug output, then you must use the <b>logging disk priority debug</b> global configuration command (the default is <b>logging disk priority notice</b>).</p> <p>If a <b>debug</b> command module uses the debug log for output, then the output can be filtered based on the priority level configuration for the four different levels of debug log output, as follows:</p> <ul style="list-style-type: none"> <li>• For filtering on critical debug messages only, use the <b>logging disk priority critical</b> global configuration command.</li> <li>• For filtering on critical and error level debug messages, use the <b>logging disk priority error</b> global configuration command.</li> <li>• For filtering on critical, error, and trace debug level debug messages, use the <b>logging disk priority debug</b> global configuration command.</li> </ul> |

**debug rbcpc**

- For seeing all debug log messages, which include critical, error, trace and detail messages, use the **logging disk priority detail** global configuration command.

Regardless of the priority level configuration, any syslog messages at the LOG\_ERROR or higher priority will be automatically written to the debug log associated with a module.

We recommend that you use the **debug** and **undebbug** commands only at the direction of Cisco Systems technical support personnel.

---

**Examples**

The following example shows how to enable RBCP debug monitoring:

```
WAE# debug rbcpc
```

---

**Related Commands**

[show debugging](#)

# debug rpc

To monitor and record remote procedure calls (RPC) debugging, use the **debug rpc EXEC** command. To disable debugging, use the **undebbug** form of this command.

## debug rpc

**undeb**ug rpc {detail | trace}

| Syntax Description | rpc   | (Optional) Enables the remote procedure calls (RPC) debugging. |
|--------------------|---|--|
| Defaults           | No default behavior or values.  |  |
| Command Modes      | EXEC  |  |
| Device Modes       | central-manager   |  |
| Usage Guidelines   | <p>Because the performance of the WAAS device degrades when you use the <b>debug</b> command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the <a href="#">“Obtaining Documentation and Submitting a Service Request” section on page xx</a>.</p> <p>If the watchdog utility is not running, the message “WAAS is not running” appears.</p> <p>Use the <b>show debugging</b> command to display enabled <b>debug</b> options.</p> <p>The output associated with the <b>debug</b> command is written to either the syslog file in <code>/local1/syslog.txt</code> or the debug log associated with the module in the file <code>/local1/errorlog/module_name-errorlog.current</code>.</p> <p>The debug log file associated with a module will be rotated to a backup file when the current file reaches its maximum size. The backup files are named as follows: <code>name-errorlog.#</code>, where # is the backup file number.</p> <p>For any <b>debug</b> command, system logging must be enabled. The command to enable logging is the <b>logging disk enable</b> global configuration command, which is enabled by default.</p> <p>If a <b>debug</b> command module uses the syslog for debug output, then you must use the <b>logging disk priority debug</b> global configuration command (the default is <b>logging disk priority notice</b>).</p> <p>If a <b>debug</b> command module uses the debug log for output, then the output can be filtered based on the priority level configuration for the four different levels of debug log output, as follows:</p> <ul style="list-style-type: none"> <li>• For filtering on critical debug messages only, use the <b>logging disk priority critical</b> global configuration command.</li> <li>• For filtering on critical and error level debug messages, use the <b>logging disk priority error</b> global configuration command.</li> <li>• For filtering on critical, error, and trace debug level debug messages, use the <b>logging disk priority debug</b> global configuration command.</li> </ul> |  |

**debug rpc**

- For seeing all debug log messages, which include critical, error, trace and detail messages, use the **logging disk priority detail** global configuration command.

Regardless of the priority level configuration, any syslog messages at the LOG\_ERROR or higher priority will be automatically written to the debug log associated with a module.

We recommend that you use the **debug** and **undebbug** commands only at the direction of Cisco Systems technical support personnel.

---

**Examples**

The following example shows how to enable RPC detail debug monitoring:

```
WAE# debug rpd detail
```

---

**Related Commands**

[show debugging](#)

# debug snmp

To monitor and record SNMP debugging , use the **debug snmp** EXEC command. To disable debugging, use the **undebug** form of this command.

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

**undebug snmp {all | cli | main | mib | traps}**

| Syntax Description      | <b>snmp</b> (Optional) Enables SNMP debugging.<br><b>all</b> Enables all SNMP debug commands.<br><b>cli</b> Enables SNMP CLI debugging.<br><b>main</b> Enables SNMP main debugging.<br><b>mib</b> Enables SNMP MIB debugging.<br><b>traps</b> Enables SNMP trap debugging.   |
|-------------------------|--|
| <b>Defaults</b>         | No default behavior or values.   |
| <b>Command Modes</b>    | EXEC   |
| <b>Device Modes</b>     | application-accelerator<br>central-manager   |
| <b>Usage Guidelines</b> | <p>Because the performance of the WAAS device degrades when you use the <b>debug</b> command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the “<a href="#">Obtaining Documentation and Submitting a Service Request</a>” section on page xx.</p> <p>If the watchdog utility is not running, the message “WAAS is not running” appears.</p> <p>Use the <b>show debugging</b> command to display enabled <b>debug</b> options.</p> <p>The output associated with the <b>debug</b> command is written to either the syslog file in /local1/syslog.txt or the debug log associated with the module in the file /local1/errorlog/module_name-errorlog.current.</p> <p>The debug log file associated with a module will be rotated to a backup file when the current file reaches its maximum size. The backup files are named as follows: <i>name-errorlog.#</i>, where # is the backup file number.</p> <p>For any <b>debug</b> command, system logging must be enabled. The command to enable logging is the <b>logging disk enable</b> global configuration command, which is enabled by default.</p> <p>If a <b>debug</b> command module uses the syslog for debug output, then you must use the <b>logging disk priority debug</b> global configuration command (the default is <b>logging disk priority notice</b>).</p> <p>If a <b>debug</b> command module uses the debug log for output, then the output can be filtered based on the priority level configuration for the four different levels of debug log output, as follows:</p> |

**debug snmp**

- For filtering on critical debug messages only, use the **logging disk priority critical** global configuration command.
- For filtering on critical and error level debug messages, use the **logging disk priority error** global configuration command.
- For filtering on critical, error, and trace debug level debug messages, use the **logging disk priority debug** global configuration command.
- For seeing all debug log messages, which include critical, error, trace and detail messages, use the **logging disk priority detail** global configuration command.

Regardless of the priority level configuration, any syslog messages at the LOG\_ERROR or higher priority will be automatically written to the debug log associated with a module.

We recommend that you use the **debug** and **undebug** commands only at the direction of Cisco Systems technical support personnel.

---

**Examples**

The following example shows how to enable all SNMP debug monitoring:

```
WAE# debug snmp all
```

---

**Related Commands**[show debugging](#)

# debug stats

To monitor and record statistics debugging, use the **debug stats** EXEC command. To disable debugging, use the **undebug** form of this command.

**debug stats {all | collections | computation | history}**

**undebug stats {all | collections | computation | history}**

| Syntax Description |   |
|--------------------|---|
| <b>stats</b>       | (Optional) Enables statistics debugging.  |
| <b>all</b>         | Enables all statistics debug commands.    |
| <b>collection</b>  | Enables collection statistics debugging.  |
| <b>computation</b> | Enables computation statistics debugging. |
| <b>history</b>     | Enables history statistics debugging.     |

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-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 xx.

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

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

The output associated with the **debug** command is written to either the syslog file in /local1/syslog.txt or the debug log associated with the module in the file /local1/errorlog/module\_name-errorlog.current.

The debug log file associated with a module will be rotated to a backup file when the current file reaches its maximum size. The backup files are named as follows: *name*-errorlog.#, where # is the backup file number.

For any **debug** command, system logging must be enabled. The command to enable logging is the **logging disk enable** global configuration command, which is enabled by default.

If a **debug** command module uses the syslog for debug output, then you must use the **logging disk priority debug** global configuration command (the default is **logging disk priority notice**).

If a **debug** command module uses the debug log for output, then the output can be filtered based on the priority level configuration for the four different levels of debug log output, as follows:

- For filtering on critical debug messages only, use the **logging disk priority critical** global configuration command.

**debug stats**

- For filtering on critical and error level debug messages, use the **logging disk priority error** global configuration command.
- For filtering on critical, error, and trace debug level debug messages, use the **logging disk priority debug** global configuration command.
- For seeing all debug log messages, which include critical, error, trace and detail messages, use the **logging disk priority detail** global configuration command.

Regardless of the priority level configuration, any syslog messages at the LOG\_ERROR or higher priority will be automatically written to the debug log associated with a module.

We recommend that you use the **debug** and **undebug** commands only at the direction of Cisco Systems technical support personnel.

---

**Examples**

The following example shows how to enable all statistics debug monitoring:

```
WAE# debug stat all
```

---

**Related Commands**

[show debugging](#)

## debug tfo

To monitor and record TFO flow optimization debugging, use the **debug tfo** EXEC command. To disable debugging, use the **undebug** form of this command.

```
debug tfo {buffer-mgr | connection [auto-discovery | comp-mgr [acl] | conn-mgr [acl] |
    egress-method [acl] | filtering [acl] | netio-engine [acl] | policy-engine [acl] |
    synq [acl] | acl] | stat-mgr | translog}

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}
```

### Syntax Description

|                       |  |
|-----------------------|--|
| <b>buffer-mgr</b>     | Enables TFO flow optimization debugging.                                   |
| <b>connection</b>     | Enables TFO connection debugging.  |
| <b>auto-discovery</b> | (Optional) Enables TFO connection debugging for the auto-discovery module. |
| <i>acl</i>            | (Optional) ACL to limit TFO connections.                                   |
| <b>comp-mgr</b>       | Enables TFO connection debugging for the compression module.               |
| <b>conn-mgr</b>       | Enables TFO connection debugging for the connection manager.               |
| <b>egress-method</b>  | Enables TFO connection debugging for the connection egress method.         |
| <b>filtering</b>      | Enables TFO connection debugging for the filtering module.                 |
| <b>netio-engine</b>   | Enables TFO connection debugging for the network input/output module.      |
| <b>policy-engine</b>  | Enables TFO connection debugging of application policies.                  |
| <b>synq</b>           | Enables TFO connection debugging for the SynQ module.                      |
| <b>stat-mgr</b>       | Enables TFO statistics manager debugging.                                  |
| <b>translog</b>       | Enables TFO transaction log debugging.                                     |

### Defaults

No default behavior or values.

### Command Modes

EXEC

### Device Modes

application-accelerator

### 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 xx.

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

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

---

```
debug tfo
```

The output associated with the **debug** command is written to either the syslog file in /local1/syslog.txt or the debug log associated with the module in the file /local1/errorlog/module\_name-errorlog.current.

The debug log file associated with a module will be rotated to a backup file when the current file reaches its maximum size. The backup files are named as follows: *name-errorlog.#*, where # is the backup file number.

For any **debug** command, system logging must be enabled. The command to enable logging is the **logging disk enable** global configuration command, which is enabled by default.

If a **debug** command module uses the syslog for debug output, then you must use the **logging disk priority debug** global configuration command (the default is **logging disk priority notice**).

If a **debug** command module uses the debug log for output, then the output can be filtered based on the priority level configuration for the four different levels of debug log output, as follows:

- For filtering on critical debug messages only, use the **logging disk priority critical** global configuration command.
- For filtering on critical and error level debug messages, use the **logging disk priority error** global configuration command.
- For filtering on critical, error, and trace debug level debug messages, use the **logging disk priority debug** global configuration command.
- For seeing all debug log messages, which include critical, error, trace and detail messages, use the **logging disk priority detail** global configuration command.

Regardless of the priority level configuration, any syslog messages at the LOG\_ERROR or higher priority will be automatically written to the debug log associated with a module.

We recommend that you use the **debug** and **undebbug** commands only at the direction of Cisco Systems technical support personnel.

---

## Examples

The following example shows how to enable all TFO flow optimization debug monitoring:

```
WAE# debug tfo all
```

---

## Related Commands

[show debugging](#)

# debug translog

To monitor and record transaction logging debugging, use the **debug translog** EXEC command. To disable debugging, use the **undebbug** form of this command.

**debug translog {detail | export | info}**

**undebbug translog export**

|                           |   |                 |   |               |   |               |   |             |   |
|---------------------------|---|-----------------|---|---------------|---|---------------|---|-------------|---|
| <b>Syntax Description</b> | <table border="1"> <tr> <td><b>translog</b></td><td>(Optional) Enables transaction logging debugging.</td></tr> <tr> <td><b>detail</b></td><td>Enables transaction log detailed debugging.</td></tr> <tr> <td><b>export</b></td><td>Enables transaction log FTP export debugging.</td></tr> <tr> <td><b>info</b></td><td>Enables transaction log high level debugging.</td></tr> </table> | <b>translog</b> | (Optional) Enables transaction logging debugging. | <b>detail</b> | Enables transaction log detailed debugging. | <b>export</b> | Enables transaction log FTP export debugging. | <b>info</b> | Enables transaction log high level debugging. |
| <b>translog</b>           | (Optional) Enables transaction logging debugging.   |                 |   |               |   |               |   |             |   |
| <b>detail</b>             | Enables transaction log detailed debugging.   |                 |   |               |   |               |   |             |   |
| <b>export</b>             | Enables transaction log FTP export debugging.   |                 |   |               |   |               |   |             |   |
| <b>info</b>               | Enables transaction log high level debugging.   |                 |   |               |   |               |   |             |   |

|                 |                                |
|-----------------|--------------------------------|
| <b>Defaults</b> | No default behavior or values. |
|-----------------|--------------------------------|

|                      |      |
|----------------------|------|
| <b>Command Modes</b> | EXEC |
|----------------------|------|

|                     |                         |
|---------------------|-------------------------|
| <b>Device Modes</b> | application-accelerator |
|---------------------|-------------------------|

|                         |  |
|-------------------------|--|
| <b>Usage Guidelines</b> | Because the performance of the WAAS device degrades when you use the <b>debug</b> command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the “ <a href="#">Obtaining Documentation and Submitting a Service Request</a> ” section on page xx. |
|-------------------------|--|

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

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

The output associated with the **debug** command is written to either the syslog file in /local1/syslog.txt or the debug log associated with the module in the file /local1/errorlog/module\_name-errorlog.current.

The debug log file associated with a module will be rotated to a backup file when the current file reaches its maximum size. The backup files are named as follows: *name*-errorlog.#, where # is the backup file number.

For any **debug** command, system logging must be enabled. The command to enable logging is the **logging disk enable** global configuration command, which is enabled by default.

If a **debug** command module uses the syslog for debug output, then you must use the **logging disk priority debug** global configuration command (the default is **logging disk priority notice**).

If a **debug** command module uses the debug log for output, then the output can be filtered based on the priority level configuration for the four different levels of debug log output, as follows:

- For filtering on critical debug messages only, use the **logging disk priority critical** global configuration command.
- For filtering on critical and error level debug messages, use the **logging disk priority error** global configuration command.

**debug translog**

- For filtering on critical, error, and trace debug level debug messages, use the **logging disk priority debug** global configuration command.
- For seeing all debug log messages, which include critical, error, trace and detail messages, use the **logging disk priority detail** global configuration command.

Regardless of the priority level configuration, any syslog messages at the LOG\_ERROR or higher priority will be automatically written to the debug log associated with a module.

We recommend that you use the **debug** and **undebug** commands only at the direction of Cisco Systems technical support personnel.

---

**Examples**

The following example shows how to enable transaction logging detail debug monitoring:

```
WAE# debug translog detail
```

---

**Related Commands**

[show debugging](#)

# debug wafs

To set the log level of WAFS running components, use the **debug wafs** EXEC command. To disable debugging, use the **undebug** form of this command.

```
debug wafs {{all | core-fe | edge-fe | manager | utilities} {debug | error | info | warn}}
```

```
undebug wafs {{all | core-fe | edge-fe | manager | utilities} {debug | error | info | warn}}
```

| Syntax Description | 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.   |
|                    | debug  | Specifies debug.   |
|                    | error  | Specifies error.   |
|                    | info   | Specifies info.  |
|                    | warn   | Specifies warn.  |
| Defaults           | No default behavior or values.   |  |
| Command Modes      | EXEC   |  |
| Device Modes       | application-accelerator  |  |
| Usage Guidelines   | <p>Because the performance of the WAAS device degrades when you use the <b>debug</b> command, we recommend that you use this command only at the direction of Cisco TAC. For more information, see the “<a href="#">Obtaining Documentation and Submitting a Service Request</a>” section on page xx.</p> <p>If the watchdog utility is not running, the message “WAAS is not running” appears.</p> <p>Use the <b>show debugging</b> command to display enabled <b>debug</b> options.</p> <p>The output associated with the <b>debug</b> command is written to either the syslog file in /local1/syslog.txt or the debug log associated with the module in the file /local1/errorlog/module_name-errorlog.current.</p> <p>The debug log file associated with a module will be rotated to a backup file when the current file reaches its maximum size. The backup files are named as follows: <i>name</i>-errorlog.#, where # is the backup file number.</p> |  |

**debug wafs**

For any **debug** command, system logging must be enabled. The command to enable logging is the **logging disk enable** global configuration command, which is enabled by default.

If a **debug** command module uses the syslog for debug output, then you must use the **logging disk priority debug** global configuration command (the default is **logging disk priority notice**).

If a **debug** command module uses the debug log for output, then the output can be filtered based on the priority level configuration for the four different levels of debug log output, as follows:

- For filtering on critical debug messages only, use the **logging disk priority critical** global configuration command.
- For filtering on critical and error level debug messages, use the **logging disk priority error** global configuration command.
- For filtering on critical, error, and trace debug level debug messages, use the **logging disk priority debug** global configuration command.
- For seeing all debug log messages, which include critical, error, trace and detail messages, use the **logging disk priority detail** global configuration command.

Regardless of the priority level configuration, any syslog messages at the LOG\_ERROR or higher priority will be automatically written to the debug log associated with a module.

We recommend that you use the **debug** and **undebbug** commands only at the direction of Cisco Systems technical support personnel.

---

**Examples**

The following example shows how to set the log level for all WAFS components to error level:

```
WAE# debug wafs all error
```

---

**Related Commands**

[show debugging](#)

# debug wccp

To monitor and record WCCP information debugging, use the **debug wccp** EXEC command. To disable debugging, use the **undebbug** form of this command.

```
debug wccp { all | detail | error | events | keepalive | packets | slowstart }
```

```
undebbug wccp { all | detail | error | events | keepalive | packets | slowstart }
```

| Syntax Description |  |
|--------------------|--|
| 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.                                       |

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator

**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 xx.

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

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

The output associated with the **debug** command is written to either the syslog file in /local1/syslog.txt or the debug log associated with the module in the file /local1/errorlog/module\_name-errorlog.current.

The debug log file associated with a module will be rotated to a backup file when the current file reaches its maximum size. The backup files are named as follows: *name*-errorlog.#, where # is the backup file number.

For any **debug** command, system logging must be enabled. The command to enable logging is the **logging disk enable** global configuration command, which is enabled by default.

If a **debug** command module uses the syslog for debug output, then you must use the **logging disk priority debug** global configuration command (the default is **logging disk priority notice**).

**debug wccp**

If a **debug** command module uses the debug log for output, then the output can be filtered based on the priority level configuration for the four different levels of debug log output, as follows:

- For filtering on critical debug messages only, use the **logging disk priority critical** global configuration command.
- For filtering on critical and error level debug messages, use the **logging disk priority error** global configuration command.
- For filtering on critical, error, and trace debug level debug messages, use the **logging disk priority debug** global configuration command.
- For seeing all debug log messages, which include critical, error, trace and detail messages, use the **logging disk priority detail** global configuration command.

Regardless of the priority level configuration, any syslog messages at the LOG\_ERROR or higher priority will be automatically written to the debug log associated with a module.

We recommend that you use the **debug** and **undebbug** commands only at the direction of Cisco Systems technical support personnel.

---

**Examples**

The following example shows how to enable WCCP information debug monitoring:

```
WAE# debug wccp all
```

---

**Related Commands**

[show debugging](#)

# delfile

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

**delfile** *filename*

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | <i>filename</i> Name of the file to delete.  |
| <b>Defaults</b>           | No default behavior or values.   |
| <b>Command Modes</b>      | EXEC   |
| <b>Device Modes</b>       | application-accelerator<br>central-manager   |
| <b>Usage Guidelines</b>   | Use the <b>delfile</b> EXEC command to remove a file from a SYSFS partition on the disk drive of the WAAS device.  |
| <b>Examples</b>           | The following example shows how to delete a temporary file from the <i>/local1</i> directory using an absolute path:<br><br><code>WAE# delfile /local1/tempfile</code> |
| <b>Related Commands</b>   | <a href="#">cpfile</a><br><a href="#">dir</a><br><a href="#">lls</a><br><a href="#">ls</a><br><a href="#">mkdir</a><br><a href="#">pwd</a><br><a href="#">rename</a>   |

**deltree**

# deltree

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

**deltree** *directory*

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

|                 |                                |
|-----------------|--------------------------------|
| <b>Defaults</b> | No default behavior or values. |
|-----------------|--------------------------------|

|                      |      |
|----------------------|------|
| <b>Command Modes</b> | EXEC |
|----------------------|------|

|                     |  |
|---------------------|--|
| <b>Device Modes</b> | application-accelerator<br>central-manager |
|---------------------|--|

|                         |   |
|-------------------------|---|
| <b>Usage Guidelines</b> | Use the <b>deltree</b> 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** Make sure that you do not remove files or directories required for the WAAS device to function properly.

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

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

|                         |  |
|-------------------------|--|
| <b>Related Commands</b> | <a href="#">cpfile</a><br><a href="#">dir</a><br><a href="#">lls</a><br><a href="#">ls</a><br><a href="#">mkdir</a><br><a href="#">pwd</a><br><a href="#">rename</a> |
|-------------------------|--|

# dir

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

**dir [directory]**

|                           |   |
|---------------------------|---|
| <b>Syntax Description</b> | <i>directory</i><br>(Optional) Name of the directory to list.   |
| <b>Defaults</b>           | No default behavior or values.  |
| <b>Command Modes</b>      | EXEC  |
| <b>Device Modes</b>       | application-accelerator<br>central-manager  |
| <b>Usage Guidelines</b>   | Use the <b>dir</b> EXEC command to view a detailed list of files contained within the working directory, including information about the file name, size, and time created. The <b>lls</b> EXEC command produces the same output. |

**Examples** The following example shows how to create 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 how to display the detailed information for only the *logs* directory:

```
WAE# dir logs
size          time of last change           name
-----
-----
```

**dir**

```
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  
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 shows how to enter 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 scan-errors *diskname***

| Syntax Description | <b>delete-partitions</b><br><i>diskname</i> | 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.<br><br>Specify the 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. |
|--------------------|---|---|
|                    | <b>disk-name diskxx</b><br><b>replace</b>   | Shuts down the physical disk with the name diskxx (disk00, disk01, etc.) so that it can be replaced in the RAID-5 array.<br><br><b>Note</b> This option is available only on RAID-5 systems.  |
|                    | <b>insert</b><br><i>diskname</i>            | Instructs the SCSI host to rescan the bus to detect and mount the newly inserted disk. Specify the name of the disk to be inserted (disk00, disk01).<br><br><b>Note</b> This option is available only on WAE-612 and WAE-7326 models.   |
|                    | <b>recreate-raid</b>                        | Recreates the RAID-5 array.<br><br><b>Note</b> This option is available only on RAID-5 systems.   |
|                    | <b>scan-errors</b><br><i>diskname</i>       | Scans SCSI or IDE disks for errors and remaps the bad sectors if they are unused. Specify the name of the disk to be scanned (disk00, disk01).<br><br>For RAID-5 systems, this command scans the logical RAID device for errors. On these systems, there is no <i>diskname</i> option.  |

|                 |                                |
|-----------------|--------------------------------|
| <b>Defaults</b> | No default behavior or values. |
|-----------------|--------------------------------|

|                      |      |
|----------------------|------|
| <b>Command Modes</b> | EXEC |
|----------------------|------|

|                     |  |
|---------------------|--|
| <b>Device Modes</b> | application-accelerator<br>central-manager |
|---------------------|--|

**Usage Guidelines**

The WAAS software 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.)

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**.

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** EXEC command to bring the disk back into service. For all other models, see the **(config) disk disk-name** command section.

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

**Caution**

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.

**Note**

Be careful when using the **disk delete-partitions** EXEC command because the WAAS software treats the specified disk drive as blank. All previous data on the drive will become inaccessible.

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.

**Examples**

The following example shows how to recreate the RAID-5 array:

```
WAE# disk recreate-raid
```

**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}**

|                           |  |                 |                                    |                   |                 |
|---------------------------|--|-----------------|------------------------------------|-------------------|-----------------|
| <b>Syntax Description</b> | <table border="0"> <tr> <td><i>hostname</i></td><td>Name of DNS server on the network.</td></tr> <tr> <td><i>domainname</i></td><td>Name of domain.</td></tr> </table> | <i>hostname</i> | Name of DNS server on the network. | <i>domainname</i> | Name of domain. |
| <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  
central-manager

**Examples** The following 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
```

**Related Commands**

# 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  
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 for each 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:



The above behavior occurs 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**

# 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  
central-manager

**Usage Guidelines** The **exit** EXEC command is equivalent to pressing **Ctrl-Z** or entering the **end** command. Entering the **exit** command 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>
```

**Related Commands** [\(config\) exit](#)

# 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 | count reg-express filename | lineno reg-express
filename | match reg-express filename | nomatch reg-express filename | recursive reg-express
filename}

find-pattern 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}
```

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

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator  
central-manager

**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/
```

**find-pattern**

```
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  
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 how to display 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.

**Related Commands**

[\(config\) help](#)

# 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***

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

|                 |                                |
|-----------------|--------------------------------|
| <b>Defaults</b> | No default behavior or values. |
|-----------------|--------------------------------|

|                      |      |
|----------------------|------|
| <b>Command Modes</b> | EXEC |
|----------------------|------|

|                     |  |
|---------------------|--|
| <b>Device Modes</b> | application-accelerator<br>central-manager |
|---------------------|--|

|                         |  |
|-------------------------|--|
| <b>Usage Guidelines</b> | The <b>install</b> command loads the system image into flash memory and copies components of the optional software to the software file system (swfs) partition. |
|-------------------------|--|



|             |  |
|-------------|--|
| <b>Note</b> | 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*. 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.

Close your browser and restart the browser session to the WAAS Central Manager, if you installed a new software image to the primary WAAS Central Manager.

|                 |   |
|-----------------|---|
| <b>Examples</b> | The following example shows how to load the system image contained in the <i>wae511-cache-300.bin</i> 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*

---

|                           |                  |                                   |
|---------------------------|------------------|-----------------------------------|
| <b>Syntax Description</b> | <i>file_name</i> | Name of the file to be displayed. |
|---------------------------|------------------|-----------------------------------|

---

|                 |                                |
|-----------------|--------------------------------|
| <b>Defaults</b> | No default behavior or values. |
|-----------------|--------------------------------|

|                      |      |
|----------------------|------|
| <b>Command Modes</b> | EXEC |
|----------------------|------|

|                     |  |
|---------------------|--|
| <b>Device Modes</b> | application-accelerator<br>central-manager |
|---------------------|--|

|                         |   |
|-------------------------|---|
| <b>Usage Guidelines</b> | Less is a pager application that displays text files one 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 include the following: |
|-------------------------|---|

- Backward movement—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—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—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.

|                 |   |
|-----------------|---|
| <b>Examples</b> | The following example shows how to display the text of the <i>syslog.txt</i> file using the Less application: |
|-----------------|---|

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

|                         |                      |
|-------------------------|----------------------|
| <b>Related Commands</b> | <a href="#">type</a> |
|-------------------------|----------------------|

# license add

To add a software license to a device, use the **license add** EXEC command.

**license add *license-name***

|                           |                     |   |
|---------------------------|---------------------|---|
| <b>Syntax Description</b> | <i>license-name</i> | Name of the software license to add. The following license names are supported: <ul style="list-style-type: none"><li>• Transport—Enables basic DRE, TFO, and LZ optimization.</li><li>• Enterprise—Enables the EPM, HTTP, MAPI, NFS, SSL, CIFS (WAFS), and Windows Print application accelerators, the WAAS Central Manager, and basic DRE, TFO, and LZ optimization.</li><li>• Video—Enables the video application accelerator. Requires the Enterprise license to be configured first.</li><li>• Virtual-Blade—Enables the virtualization feature. Requires the Enterprise license to be configured first.</li></ul> |
| <b>Defaults</b>           |                     | No default behavior or values.  |
| <b>Command Modes</b>      |                     | EXEC  |
| <b>Device Modes</b>       |                     | application-accelerator<br>central-manager  |
| <b>Examples</b>           |                     | The following example shows how to install the enterprise license:<br><pre>WAE# license add Enterprise</pre>  |
| <b>Related Commands</b>   |                     | <a href="#">clear arp-cache license</a><br><a href="#">show license</a>   |

**lls**

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

**lls [directory]**

---

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

---

|                 |                                |
|-----------------|--------------------------------|
| <b>Defaults</b> | No default behavior or values. |
|-----------------|--------------------------------|

---

|                      |      |
|----------------------|------|
| <b>Command Modes</b> | EXEC |
|----------------------|------|

---

|                     |  |
|---------------------|--|
| <b>Device Modes</b> | application-accelerator<br>central-manager |
|---------------------|--|

---

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

---

|                 |   |
|-----------------|---|
| <b>Examples</b> | The following example shows how to display 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 |                     |
|------------------|---------------------|
|                  | <a href="#">dir</a> |
|                  | <a href="#">lls</a> |
|                  | <a href="#">ls</a>  |

**ls****ls**

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

**ls** [*directory*]

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | <i>directory</i><br>(Optional) Name of the directory for which you want a list of files.   |
| <b>Defaults</b>           | No default behavior or values.   |
| <b>Command Modes</b>      | EXEC   |
| <b>Device Modes</b>       | application-accelerator<br>central-manager   |
| <b>Usage Guidelines</b>   | <p>Use the <b>ls</b> <i>directory</i> command to list the filenames and subdirectories within a particular directory.</p> <p>Use the <b>ls</b> command to list the filenames and subdirectories of the current working directory.</p> <p>Use the <b>pwd</b> command to view the present working directory.</p> |
| <b>Examples</b>           | The following example shows how to display the files and subdirectories that are listed within the root directory:   |
|                           | <pre>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 var wdd.sh.signed</pre>  |
| <b>Related Commands</b>   | <a href="#">dir</a><br><a href="#">lls</a>   |

pwd

**mkdir**

# mkdir

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

**mkdir** *directory*

|                           |  |                                  |
|---------------------------|--|----------------------------------|
| <b>Syntax Description</b> | <i>directory</i>   | Name of the directory to create. |
| <b>Defaults</b>           | No default behavior or values.   |                                  |
| <b>Command Modes</b>      | EXEC   |                                  |
| <b>Device Modes</b>       | application-accelerator<br>central-manager   |                                  |
| <b>Examples</b>           | The following example shows how to create a new directory, <i>oldpaxfiles</i> :  |                                  |
|                           | WAE# <b>mkdir /oldpaxfiles</b>   |                                  |
| <b>Related Commands</b>   | <a href="#">cpfile</a><br><a href="#">dir</a><br><a href="#">lls</a><br><a href="#">ls</a><br><a href="#">pwd</a><br><a href="#">rename</a><br><a href="#">rmdir</a> |                                  |

# mkfile

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

**mkfile** *filename*

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | <i>filename</i> Name of the file that you want to create.  |
| <b>Defaults</b>           | No default behavior or values.   |
| <b>Command Modes</b>      | EXEC   |
| <b>Device Modes</b>       | application-accelerator<br>central-manager   |
| <b>Usage Guidelines</b>   | Use the <b>mkfile</b> EXEC command to create a new file in any directory of the WAAS device.   |
| <b>Examples</b>           | The following example shows how to create a new file, <i>traceinfo</i> , in the root directory:<br><pre>WAE# mkfile traceinfo</pre>                                  |
| <b>Related Commands</b>   | <a href="#">cpfile</a><br><a href="#">dir</a><br><a href="#">lls</a><br><a href="#">ls</a><br><a href="#">mkdir</a><br><a href="#">pwd</a><br><a href="#">rename</a> |

# ntpdate

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

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

---

## Syntax Description

|                           |   |
|---------------------------|---|
| <b>hostname</b>           | NTP hostname.   |
| <b>ip-address</b>         | NTP server IP address.  |
| <b>key</b>                | (Optional) Specifies to use authentication with the NTP server.   |
| <b>authentication-key</b> | 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  
central-manager

---

## Usage Guidelines

Use the **ntpdate** command to find the current time of day and set the current time on the WAAS device to match. You must save the time to the hardware clock using the **clock save** command if you want to restore the time after a reload.

---

## Examples

The following example shows how to set the software clock on the WAAS device using a 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  
central-manager

## Usage Guidelines

To use the **ping** command with the *hostname* argument, make sure that DNS functionality is configured on 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**

## 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  
central-manager

---

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

```
WAE# pwd  
/local1
```

---

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

# reload

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

**reload [force | in *m* | cancel]**

## Syntax Description

|                    |   |
|--------------------|---|
| <b>force</b>       | (Optional) Forces a reboot without further prompting.                       |
| <b>in <i>m</i></b> | (Optional) Schedules a reboot after a specified interval (1-10080 minutes). |
| <b>cancel</b>      | (Optional) Cancels a scheduled reboot.                                      |

## Defaults

No default behavior or values.

## Command Modes

EXEC

## Device Modes

application-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 a restart. Any open connections are dropped after you enter the **reload** command, and the file system is reformatted upon restart.

The **reload** command can include the option to schedule a reload of the software to take effect in a specified number of minutes. After entering this command, you are asked to confirm the reload by typing **y** and then confirm WCCP shutdown by typing **y** again (if WCCP is active).

You can use the **cancel** option to cancel a scheduled reload.

## Examples

The following example shows how to halt the operation of the WAAS device and reboot with the configuration saved in flash memory. You are not prompted for confirmations during the process.

```
WAE# reload force
```

## Related Commands

[write](#)

rename

## 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  
central-manager

---

### Usage Guidelines

Use the **rename** 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 by removing the user data from the disk and flash memory, use the **restore** EXEC command.

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

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

|          |                                |
|----------|--------------------------------|
| Defaults | No default behavior or values. |
|----------|--------------------------------|

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

|              |  |
|--------------|--|
| Device Modes | application-accelerator<br>central-manager |
|--------------|--|

|                  |   |
|------------------|---|
| Usage Guidelines | Use the <b>restore</b> EXEC command to restore data on a 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, make sure that you back up the WAAS Central Manager database and copy the backup file to a safe location that is separate from the WAAS Central Manager. You must halt the operation of the WAAS Central Manager before you enter the **backup** and **restore** commands.



### Caution

The **restore** command erases user-specified configuration information stored in the flash image and removes data from a 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 that is removed includes the starting configuration of the device.

**restore**

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 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 the 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**


---

WAFS to WAAS migration is supported. Rollback from WAAS to WAFS is not supported.

---



---

**Examples**

The following 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 the IP address, hostname, and name server) at this point, or you can enter these parameters later through entries in the command-line interface.

---

The following example shows how to verify that the **restore** command has removed data from the SYSFS, WAAS, and PRINTSPOOLFS partitioned file systems:

```

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-filesystems 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 example, 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 how to roll back the software to version X (using the **restore rollback** command), and reload the software:

```

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 2
006)
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

```

**■ restore**

```
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*

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | <i>directory</i> Name of the directory that you want to delete.  |
| <b>Defaults</b>           | No default behavior or values.   |
| <b>Command Modes</b>      | EXEC   |
| <b>Device Modes</b>       | application-accelerator<br>central-manager   |
| <b>Usage Guidelines</b>   | Use the <b>rmdir</b> EXEC command to remove any directory from the WAAS file system. The <b>rmdir</b> command only removes empty directories.                        |
| <b>Examples</b>           | The following example shows how to delete the <i>oldfiles</i> directory from the <i>local1</i> directory:<br><br><pre>WAE# rmdir /local1/oldfiles</pre>              |
| <b>Related Commands</b>   | <a href="#">cpfile</a><br><a href="#">dir</a><br><a href="#">lls</a><br><a href="#">ls</a><br><a href="#">mkdir</a><br><a href="#">pwd</a><br><a href="#">rename</a> |

# scp

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

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

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

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

|              |  |
|--------------|--|
| Device Modes | application-accelerator<br>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**

# script

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

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

|                           |   |              |                                    |                |   |                  |                          |
|---------------------------|---|--------------|------------------------------------|----------------|---|------------------|--------------------------|
| <b>Syntax Description</b> | <table border="1"> <tr> <td><b>check</b></td><td>Checks the validity of the script.</td></tr> <tr> <td><b>execute</b></td><td>Executes the script. The script file must be a SYSFS file in the current directory.</td></tr> <tr> <td><i>file_name</i></td><td>Name of the script file.</td></tr> </table> | <b>check</b> | Checks the validity of the script. | <b>execute</b> | Executes the script. The script file must be a SYSFS file in the current directory. | <i>file_name</i> | Name of the script file. |
| <b>check</b>              | Checks the validity of the script.  |              |                                    |                |   |                  |                          |
| <b>execute</b>            | Executes the script. The script file must be a SYSFS file in the current directory.   |              |                                    |                |   |                  |                          |
| <i>file_name</i>          | Name of the script file.  |              |                                    |                |   |                  |                          |

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-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, interception type, disk configuration, and licenses) on the WAAS device or to complete basic configuration after upgrading to the 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  
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 how to access 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
Step 1: The following defaults can be configured:
Device mode: Application-accelerator
Interception Method: Inline
Management Interface: InlineGroup 1/1
Autosense: yes
Timezone: UTC 0 0

To keep above defaults and continue configuration, press 'y'.
To change above defaults and continue configuration, press 'n' [y]:
```

---

 show aaa accounting

# show aaa accounting

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

**show aaa accounting**

---

**Defaults** No default behavior or values.

---

**Command Modes** EXEC

---

**Device Modes** application-accelerator  
central-manager

---

**Usage Guidelines** Use the **show aaa accounting** 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** command display.

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

| Field           | Description   |
|-----------------|---|
| Accounting Type | AAA accounting configuration for the following types of user accounts: <ul style="list-style-type: none"> <li>• Exec</li> <li>• Command level 0</li> <li>• Command level 15</li> <li>• System</li> </ul>  |
| Record Event(s) | Configuration of the AAA accounting notice that is sent to the accounting server.   |
| stop-only       | WAAS device that sends a stop record accounting notice at the end of the specified activity or event to the TACACS+ accounting server.  |
| start-stop      | WAAS device that 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.<br><br>The start accounting record is sent in the background. The requested user service begins regardless of whether the start accounting record was acknowledged by the TACACS+ accounting server. |

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

| Field      | Description  |
|------------|--|
| wait-start | WAAS device that sends both a start and a stop accounting record to the TACACS+ accounting server. The requested user service does not begin until the start accounting record is acknowledged. A stop accounting record is also sent. |
| disabled   | Accounting that is disabled for the specified event.   |
| Protocol   | Accounting protocol that is configured.  |

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

---

 show accelerator

# show accelerator

To display the status and configuration of the application accelerators, use the **show accelerator** EXEC command.

**show accelerator [{cifs | detail | epm | http | mapi | nfs | ssl | video}]**

| Syntax Description | cifs<br>(Optional) Displays the status for the CIFS application accelerator.  |
|--------------------|---|
| <b>detail</b>      | (Optional) Displays the license information, configuration state, and operational state for all accelerators, and additional accelerator and policy engine configuration. |
| <b>epm</b>         | (Optional) Displays the status for the EPM application accelerator.   |
| <b>http</b>        | (Optional) Displays the status for the HTTP application accelerator.  |
| <b>mapi</b>        | (Optional) Displays the status for the MAPI application accelerator.  |
| <b>nfs</b>         | (Optional) Displays the status for the NFS application accelerator.   |
| <b>ssl</b>         | (Optional) Displays the status for the SSL application accelerator.   |
| <b>video</b>       | (Optional) Displays the status for the video application accelerator.   |

---

**Defaults** No default behavior or values.

---

**Command Modes** EXEC

---

**Device Modes** application-accelerator

---

**Examples** Table 3-2 describes the fields shown in the **show accelerator** command display for all application accelerators. Specific application accelerators display additional configuration status information.

**Table 3-2 Field Description for the show accelerator Command**

| Field                            | Description  |
|----------------------------------|--|
| Accelerator                      | Name of the accelerator.   |
| Licensed                         | Yes or No.   |
| Config State                     | Accelerator is Enabled or Disabled.  |
| Operational State                | Shutdown, Initializing, Running, Cleaning Up, or Expired License.  |
| Policy Engine Config Item: State | Registered (policy engine is communicating with the accelerator) or Not Registered (policy engine is not communicating with the accelerator; seen when the accelerator is disabled). |

**Table 3-2 Field Description for the show accelerator Command (continued)**

| Field  | Description  |
|--|--|
| Policy Engine Config Item: Default Action    | Drop or Use. Specifies the action to be taken if the accelerator refuses to handle the connection (because of overload or other reasons). Drop means the connection is dropped, and Use means the connection uses a reduced set of policy actions (such as TFO and DRE). |
| Policy Engine Config Item: Connection Limit  | Connection limit. The limit configured by the accelerator which states how many connections may be handled before new connection requests are rejected.  |
| Policy Engine Config Item: Effective Limit   | Effective connection limit. The dynamic limit relating to how many connections may be handled before new connection requests are rejected. This limit is affected by resources that have been reserved, but not yet used.  |
| Policy Engine Config Item: Keepalive timeout | Connection keepalive timeout in seconds. Keepalive messages are sent by each AO.   |

**Related Commands**

[\(config\) accelerator cifs](#)  
[\(config\) accelerator epm](#)  
[\(config\) accelerator http](#)  
[\(config\) accelerator mapi](#)  
[\(config\) accelerator nfs](#)  
[\(config\) accelerator ssl](#)  
[\(config\) accelerator video](#)  
[show statistics accelerator](#)

---

 show alarms

## show alarms

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

**show alarms critical [detail [support]]**

**show alarms detail [support]**

**show alarms history [start\_num [end\_num [detail [support]]]] | critical [start\_num [end\_num [detail [support]]]]**

**show alarms major [start\_num [end\_num [detail [support]]]]**

**show alarms minor [start\_num [end\_num [detail [support]]]]**

**show alarms status**

| Syntax Description |  |
|--------------------|--|
| <b>critical</b>    | Displays critical alarm information.                               |
| <b>detail</b>      | (Optional) Displays detailed information for each alarm.           |
| <b>support</b>     | (Optional) Displays additional information about each alarm.       |
| <b>history</b>     | 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.    |
| <b>major</b>       | Displays information about major alarms.                           |
| <b>minor</b>       | Displays information about minor alarms.                           |
| <b>status</b>      | Displays the status of various alarms and alarm overload settings. |

---

**Defaults** No default behavior or values.

---

**Command Modes** EXEC

---

**Device Modes** application-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 the 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 that indicate a major service (for example, the cache service) has been damaged or lost. Urgent action is necessary to restore this service. However, other node components are fully functional and the existing service should be minimally impacted.
- Minor—Alarms that indicate that a condition that will not affect a service has occurred, but 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 the 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 alarm overload status of the WAAS device and alarm overload configuration.

## Examples

[Table 3-3](#) describes the fields shown in the **show alarms history** command 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 or 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 predefined values and is application specific. |

[Table 3-4](#) describes the fields shown in the **show alarms status** command display.

show alarms

**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.  |
| 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  
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** command 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**

# show authentication

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

**show authentication {user | content-request}**

|                            |   |
|----------------------------|---|
| <b>Syntax Descriptions</b> | <b>user</b> Displays authentication configuration for user login to the system.<br><b>content-request</b> Displays content request authentication configuration information in the disconnected mode. |
|----------------------------|---|

|                 |                                |
|-----------------|--------------------------------|
| <b>Defaults</b> | No default behavior or values. |
|-----------------|--------------------------------|

|                      |      |
|----------------------|------|
| <b>Command Modes</b> | EXEC |
|----------------------|------|

|                     |  |
|---------------------|--|
| <b>Device Modes</b> | application-accelerator<br>central-manager |
|---------------------|--|

|                         |   |
|-------------------------|---|
| <b>Usage Guidelines</b> | 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 <b>show authentication user</b> EXEC command. |
|-------------------------|---|

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

|                 |  |
|-----------------|--|
| <b>Examples</b> | Table 3-6 describes the fields shown in the <b>show authentication user</b> command display. |
|-----------------|--|

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

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

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

| Field          | Description   |
|----------------|---|
| 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** command 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 configuration](#)

[clear arp-cache](#)

[show statistics authentication](#)

---

 show auto-discovery

# show auto-discovery

To display Traffic Flow Optimization (TFO) auto-discovery information for a WAE, use the **show auto-discovery** EXEC command.

```
show auto-discovery {blacklist [netmask netmask] | list [| {begin regex [regex] | exclude regex [regex] | include regex [regex]}]}
```

| Syntax Description     |   |
|------------------------|---|
| <b>blacklist</b>       | Displays the entries in the blacklist server table.   |
| <b>netmask netmask</b> | (Optional) Displays the network mask to filter the table output (A.B.C.D/).                   |
| <b>list</b>            | Lists TCP flows that the WAE is currently optimizing or passing through.                      |
| <b> </b>               | (Optional) Specifies the output modifier.   |
| <b>begin regex</b>     | Begins with the line that matches the regular expression. You can enter multiple expressions. |
| <b>exclude regex</b>   | Excludes lines that match the regular expression. You can enter multiple expressions.         |
| <b>include regex</b>   | Includes lines that match the regular expression. You can enter multiple expressions.         |

---

 Command Modes EXEC

---

 Device Modes application-accelerator

---

 Examples The following is sample output from the **show auto-discovery list** command:

```
WAE# show auto-discovery list

E: Established, S: Syn, A: Ack, F: Fin, R: Reset
s: sent, r: received, O: Options, P: Passthrough

Src-IP:Port          Dst-IP:Port      Orig-St  Term-St
```

---

 Related Commands
 

- [show statistics auto-discovery](#)
- [show statistics filtering](#)
- [show statistics tfo](#)
- [show statistics connection closed](#)

# show auto-register

To display the status of the automatic registration feature on a WAE, 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** command 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. | Configuration status of the autoregistration feature. |

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

**show banner**

# 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  
central-manager

**Examples** Table 3-9 describes the fields shown in the **show banner** command 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  | Configured message of the day.              |
| Login banner is: acb | Configured login banner.                    |
| Exec banner is: abc  | 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**

|                           |             |   |
|---------------------------|-------------|---|
| <b>Syntax Description</b> | <b>list</b> | Displays the bypass list entries. You can have a maximum of 50 entries. |
|---------------------------|-------------|---|

|                 |                                |
|-----------------|--------------------------------|
| <b>Defaults</b> | No default behavior or values. |
|-----------------|--------------------------------|

|                      |      |
|----------------------|------|
| <b>Command Modes</b> | EXEC |
|----------------------|------|

|                     |                         |
|---------------------|-------------------------|
| <b>Device Modes</b> | application-accelerator |
|---------------------|-------------------------|

|                 |   |
|-----------------|---|
| <b>Examples</b> | <a href="#">Table 3-10</a> describes the fields shown in the <b>show bypass list</b> command 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.<br><br>A static-config entry is a bypass list entry that is configured by the user. An auth-traffic entry is a type of dynamic entry that the internal software adds automatically when the server requests authentication. |

|                         |                                 |
|-------------------------|---------------------------------|
| <b>Related Commands</b> | <a href="#">(config) bypass</a> |
|-------------------------|---------------------------------|

**show cdp**

# show cdp

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

```
show cdp entry {* | neighbor} [protocol | version]
show cdp interface
  [GigabitEthernet slot/port | InlinePort slot/port/{lan/wan}]
show cdp neighbors
  [detail | GigabitEthernet slot/port [detail] | InlinePort slot/port/{lan/wan}[detail]]
show cdp {holdtime | run | timer | traffic}
```

| Syntax Description                    |   |
|---------------------------------------|---|
| <b>entry</b>                          | (Optional) Displays information for a specific CDP neighbor entry.                      |
| <b>*</b>                              | Specifies all neighbors.  |
| <b>neighbor</b>                       | The CDP neighbor entry to display.  |
| <b>protocol</b>                       | (Optional) Displays the CDP protocol information.                                       |
| <b>version</b>                        | (Optional) Displays the CDP version.  |
| <b>interface</b>                      | Displays interface status and configuration.  |
| <b>GigabitEthernet slot/port</b>      | (Optional) Displays Gigabit Ethernet configuration (slot 1–2 and port number).          |
| <b>InlinePort slot/port/{lan/wan}</b> | (Optional) Displays Inline Port configuration (slot 1–2, port number, LAN or WAN port). |
| <b>neighbors</b>                      | Displays CDP neighbor entries.  |
| <b>detail</b>                         | (Optional) Displays detailed information.   |
| <b>holdtime</b>                       | Displays the length of time that CDP information is held by neighbors.                  |
| <b>run</b>                            | Displays the CDP process status.  |
| <b>timer</b>                          | Displays the time when CDP information is resent to neighbors.                          |
| <b>traffic</b>                        | Displays CDP statistical information.   |

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator  
central-manager

**Usage Guidelines** The **show cdp** command displays information about 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** command 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 <b>cdp timer</b> 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 <b>cdp holdtime</b> 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** command 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. The field depends on the type of neighbor.   |
| DECnet address          | Non-IP network address. The field depends on the 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:<br>R—Router<br>T—Transparent bridge<br>B—Source-routing bridge<br>S—Switch<br>H—Host<br>I—IGMP device<br>r—Repeater |
| 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** command display.

show cdp

**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. The field depends on the type of neighbor. |
| DECnet address              | Non-IP network address. The field depends on the type of neighbor. |

Table 3-14 describes the fields shown in the **show cdp entry neighbor version** command 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** command 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** command 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.  |
| Encapsulation                        | Encapsulation.   |
| Sending CDP packets every XX seconds | Time interval at which CDP packets are sent.   |
| Holdtime                             | Time, in seconds, that the current device will hold the CDP advertisement from a transmitting router before discarding it. |
| CDP protocol is XX                   | Protocol being used by the connectivity media.   |

[Table 3-17](#) describes the fields shown in the **show cdp neighbors** command 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 Intrfce           | (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:<br>R—Router<br>T—Transparent bridge<br>B—Source-routing bridge<br>S—Switch<br>H—Host<br>I—IGMP device<br>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** command 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.   |

show cdp

**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** command display.

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

| Field      | Description                         |
|------------|-------------------------------------|
| CDP is XX. | Whether CDP is enabled or disabled. |

Table 3-20 describes the field in the **show cdp timer** command 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** command 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. 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. 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 that the checksum (verifying) operation failed on incoming CDP advertisements.   |
| Encaps failed        | (Encapsulations Failed) Number of times that 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 that 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<br>advertisements<br>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<br>advertisements<br>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 arp-cache](#)  
[debug cdp](#)

**show cifs**

# show cifs

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

**show cifs auto-discovery {enabled | host-db | last}**

**show cifs cache {disk-use | entry-count}**

**show cifs connectivity peers**

**show cifs mss**

**show cifs requests {count | waiting}**

**show cifs sessions {count | list}**

| Syntax Description    |   |
|-----------------------|---|
| <b>auto-discovery</b> | Displays the CIFS auto-discovery status and run-time data.  |
| <b>enabled</b>        | (Optional) Displays current state of CIFS auto-discovery.   |
| <b>host-db</b>        | (Optional) Displays currently known hosts.  |
| <b>last</b>           | (Optional) Displays last auto-discovered entries.   |
| <b>cache</b>          | Displays CIFS cache information.  |
| <b>disk-use</b>       | Displays the total disk usage for CIFS cache.   |
| <b>entry-count</b>    | Displays the count of internal cache resources used for cached files.                                 |
| <b>connectivity</b>   | Displays Run-time information on Edge-Core connectivity.  |
| <b>peers</b>          | Displays a list of connected Cores.   |
| <b>mss</b>            | Displays the TCP maximum segment size (MSS) for the CIFS adapter. The segment size range is 512–1460. |
| <b>requests</b>       | Displays run-time information on active CIFS requests.  |
| <b>count</b>          | Displays the number of pending CIFS requests.   |
| <b>waiting</b>        | Displays the number of waiting CIFS requests.   |
| <b>sessions</b>       | Displays run-time information on active CIFS sessions.  |
| <b>count</b>          | Displays the connected session count.   |
| <b>list</b>           | Displays the list of connected CIFS sessions.   |

|                 |                                |
|-----------------|--------------------------------|
| <b>Defaults</b> | No default behavior or values. |
|-----------------|--------------------------------|

|                      |      |
|----------------------|------|
| <b>Command Modes</b> | EXEC |
|----------------------|------|

|                     |                         |
|---------------------|-------------------------|
| <b>Device Modes</b> | application-accelerator |
|---------------------|-------------------------|

|                         |   |
|-------------------------|---|
| <b>Usage Guidelines</b> | The <b>show cifs</b> command operates on legacy mode WAFS. For information on the transparent CIFS accelerator, use the <b>show accelerator</b> or <b>show statistics accelerator</b> commands. |
|-------------------------|---|

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.

---

**Examples**

The following is sample output from the **show cifs connectivity peers** command:

```
WAE# show cifs connectivity peers
In_533202151_2.43.60.38
```

---

**Related Commands**

[cifs](#)

**show clock**

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

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-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 the 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 you configure a standard time zone is configured. You can configure summer time only 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 so that you can choose a customized name that does not conflict with the predefined names of the standard time zones. Most predefined names of the standard time zones have two components, a region name and a zone name. You can list time zones by several criteria, such as regions and zones. 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** command 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** command 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**

## 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 | secure-store}
```

|                           |   |
|---------------------------|---|
| <b>Syntax Description</b> |   |
| <b>database</b>           | Displays embedded database maintenance information.   |
| <b>content</b>            | Writes the database content to a file.  |
| <b>dump filename</b>      | Dumps all database content to a text file. Specifies the name of the file to be saved under local1 directory. |
| <b>text</b>               | Writes the database content to a file in text format.   |
| <b>xml</b>                | Writes the database content to a file in XML format.  |
| <b>info</b>               | Displays CMS application information.   |
| <b>secure-store</b>       | Displays the status of the CMS secure store.  |

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator  
central-manager

**Examples** Table 3-24 describes the fields shown in the **show cms info** command 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 <b>central-manager address</b> 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. |
| Registered with WAAS Central Manager | Address of the Central Manager with which the device is registered.  |

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

| Field                     | Description  |
|---------------------------|--|
| Status                    | Connection status of the device to the Central Manager. This field may contain one of three values: online, offline, or pending. |
| Time of last config-sync  | Time when the device management service last contacted the 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** command 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.<br><b>Note</b> 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 <b>central-manager address</b> 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.  |

show cms

[Table 3-26](#) describes the field in the **show cms database content text** command 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. The <b>show cms database content text</b> 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** command 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. The <b>show cms database content xml</b> 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 store status, use the **show cms secure-store** EXEC command.

**show cms secure-store**

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

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator  
central-manager

**Usage Guidelines** The **show cms secure-store** command will display one of the following status messages (Table 3-28):

**Table 3-28 Status Messges for the show cms secure-store Command**

| Message   | Description                               |
|---|---|
| <b>secure-store not initialized</b>                                 | Secure store is not initialized.          |
| <b>secure-store is initialized, enter pass-phrase to open store</b> | Secure store is initialized and not open. |
| <b>secure-store initialized and open</b>                            | Secure store is initialized and open.     |

**Examples** The following is sample output from the **show cms secure-store** command:

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

**Related Commands** [cms secure-store](#)

show crypto

## show crypto

To display crypto layer information, use the **show crypto** EXEC command.

```
show crypto {certificate-detail {factory-self-signed | management | word} | certificates}
```

| Syntax Description  | certificate-detail      Displays a certificate in detail. |
|---------------------|---|
| factory-self-signed | Displays WAAS self-signed certificates in detail.         |
| management          | Displays WAAS management certificates in detail.          |
| word                | Filename of the certificate to display.                   |
| certificates        | Displays a summary of all PKI certificates.               |

|          |                                |
|----------|--------------------------------|
| Defaults | No default behavior or values. |
|----------|--------------------------------|

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

|              |  |
|--------------|--|
| Device Modes | application-accelerator<br>central-manager |
|--------------|--|

|          |   |
|----------|---|
| Examples | Table 3-29 describes the fields in the <b>show crypto certificate-detail</b> command display. |
|----------|---|

**Table 3-29 Field Descriptions for the show crypto certificate-detail Command**

| Field                   | Description  |
|-------------------------|--|
| Version                 | Certificate version.   |
| Serial Number           | Certificate serial number.   |
| Signature Algorithm     | Certificate signature algorithm.                                     |
| Issuer                  | Information on the signer of the certificate.                        |
| Validity                |  |
| Not Before              | The date and time before which the certificate is not valid.         |
| Not After               | The date and time after which the certificate is not valid.          |
| Subject                 | Information on the holder of the certificate.                        |
| Subject Public Key Info |  |
| Public Key Algorithm    | Fields display X.509 certificate information as defined in RFC 5280. |
| RSA Public Key          |  |
| Modulus                 |  |
| Exponent                |  |
| X509v3 extensions       |  |

**Table 3-29 Field Descriptions for the show crypto certificate-detail Command**

| Field                           | Description  |
|---------------------------------|--|
| X509v3 Subject Key Identifier   | Fields display X.509 certificate information as defined in RFC 5280. |
| X509v3 Authority Key Identifier |  |
| X509v3 Basic Constraints        |  |
| Signature Algorithm             |  |
| BEGIN CERTIFICATE               | The actual certificate follows until the End Certificate line.       |
| END CERTIFICATE                 | The line that signifies the end of the certificate.                  |

Table 3-30 describes the field in the **show device-mode configured** command display.

**Table 3-30 Field Descriptions for the show crypto certificates Command**

| Field                           | Description  |
|---------------------------------|--|
| Certificate Only Store          | Certificate Authority (CA) certificates.   |
| Managed Store                   | User-defined certificates. Used under the server-cert-key section of SSL accelerated services. This certificate is used as a server certificate for client-to-WAE connections. |
| Local Store                     | Certificates that are configured on the WAE by default.  |
| Machine Self signed Certificate | Certificate from the WAE to the server when client authentication is requested by the server.  |
| Format                          | Format of the certificate (PEM or PKCS12).   |
| Subject                         | The name of the holder of the certificate.   |
| Issuer                          | Who signed the certificate.  |
| Management Service Certificate  | Certificate used to identify the WAE with the Central Manager.   |
| Format                          | Format of the certificate (PEM or PKCS12).   |
| EEC: Subject                    | The name of the holder of the certificate.   |
| Issuer                          | Who signed the certificate.  |

**Related Commands**

[show statistics crypto ssl ciphers](#)

**show debugging**

# 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.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator  
central-manager

**Usage Guidelines** The **show debugging** command shows which debug options have been enabled or disabled. If there are no debug options configured, the **show debugging** command shows no output.

The **dre**, **epm**, **flow**, **print-spooler**, **rbcpc**, **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.

The **show debugging** command displays only the type of debugging enabled, not the specific subset of the command.

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

```
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
```

In this example, 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.

**Related Commands** [debug all](#)

# 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}
```

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | <b>configured</b> Displays the configured device mode, which has not taken effect yet.<br><b>current</b> Displays the current device mode. |
|---------------------------|--|

|                 |                                |
|-----------------|--------------------------------|
| <b>Defaults</b> | No default behavior or values. |
|-----------------|--------------------------------|

|                      |      |
|----------------------|------|
| <b>Command Modes</b> | EXEC |
|----------------------|------|

|                     |  |
|---------------------|--|
| <b>Device Modes</b> | application-accelerator<br>central-manager |
|---------------------|--|

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

|                 |  |
|-----------------|--|
| <b>Examples</b> | The following is sample output from the <b>show device mode</b> command. It displays the current mode in which the WAAS device is operating. |
|-----------------|--|

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

Current device mode: application-accelerator

[Table 3-31](#) describes the field in the **show device-mode current** command display.

**Table 3-31 Field Description for the show device-mode current Command**

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

The following is sample output from the **show device configured** command. It displays the configured device mode that has not yet taken effect.

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

Configured device mode: central-manager

**show device-mode**

Table 3-32 describes the field in the **show device-mode configured** command display.

**Table 3-32 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 directed-mode

To view the status and port assigned to directed mode on a device, use the **show directed-mode** EXEC command.

## show directed-mode

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

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator

**Examples** The following is sample output from the **show directed-mode** EXEC command:

```
WAE# show directed-mode

Configuration Status: Enabled
Config Item           Mode      Value
-----              ----      -----
UDP port             Default   4050
```

This example shows that directed mode is enabled and it is using UDP port 4050.

**Related Commands**

- [show statistics directed-mode](#)
- [show statistics connection closed](#)
- [\(config\) directed-mode](#)

■ show disks

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

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-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.

### 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, SCSI, and Serial Advanced Technology Attachment [SATA] disk drive) 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

The following is sample output from the **show disks failed-sectors** command. It displays a list of failed sectors on all disk drives.

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

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

The following is sample output from the **show disks failed-sectors** command when you specify a disk drive. It displays 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.

[Table 3-33](#) describes the fields shown in the **show disks failed-disk-id** command display.

**Table 3-33 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 3-34](#) describes the fields shown in the **show disks details** command display.

**Table 3-34 Field Descriptions for the show disks details Command**

| Field   | Description   |
|---|---|
| Physical disk information or RAID Physical disk information | Lists the disks by number. On RAID-5 systems, this field is called RAID Physical disk information.  |
| disk00  | <p>Availability of the disk: Present, Not present or Not responding, Not used (*), or Online (for RAID-5 disks).</p> <p>Disk identification number and type, for example: (h00 c00i00 100 - DAS).</p> <p>Disk size in megabytes and gigabytes, for example: 140011MB (136.7GB).</p> |
| disk01  | Same type of information is shown for each disk.  |
| RAID Logical drive information                              | RAID-5 logical drive status and error conditions. (Only shown for RAID-5 systems.)  |
| 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].  |
| Disk encryption status                                      | Indicates if the disk encryption feature is enabled or disabled.  |

The following is sample output from the **show disks tech-support** command. 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.

```
WAE# show disks tech-support
/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 3-35** describes some typical fields in the **show disks tech-support** command 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 3-35 Field Descriptions for the show disks tech-support Command (RAID-1)**

| 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 3-36** describes the fields shown in the **show disks tech-support** command display for a RAID-5 appliance.

**Table 3-36 Field Descriptions for the show disks tech-support Command (RAID-5)**

| 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.                           |

show disks

**Table 3-36 Field Descriptions for the show disks tech-support Command (RAID-5)**

| Field                            | Description  |
|----------------------------------|--|
| 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.  |
| 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       |  |

**Table 3-36 Field Descriptions for the show disks tech-support Command (RAID-5)**

| Field                   | Description   |
|-------------------------|---|
| 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.   |
| 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.                                   |

Table 3-37 describes the fields in the **show disks tech-support details** command display for a RAID-1 appliance that supports SMART. Details in this display depend on the drive manufacturer and vary between drives.

**Table 3-37 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.   |

show disks

**Table 3-37 Field Descriptions for the show disks tech-support details Command (continued)**

| Field                                | Description  |
|--------------------------------------|--|
| 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.   |
| 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. |

**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.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator

**Examples** Table 3-38 describes the fields shown in the **show egress-methods** command display.

**Table 3-38 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 tcp](#)

[\(config\) egress-method](#)

show filtering list

# show filtering list

To display information about the incoming and outgoing TFO flows that the WAE currently has, use the **show filtering list** EXEC command.

```
show filtering list [! {begin regex [regex] | exclude regex [regex] | include regex [regex] }] [! {begin
    regex [regex] | exclude regex [regex] | include regex [regex]}]
```

|                           |  |             |   |          |                             |                    |   |                      |   |                      |   |
|---------------------------|--|-------------|---|----------|-----------------------------|--------------------|---|----------------------|---|----------------------|---|
| <b>Syntax Description</b> | <table border="0"> <tr> <td><b>list</b></td><td>(Optional) Lists TCP flows that the WAE is currently optimizing or passing through.</td></tr> <tr> <td><b>!</b></td><td>(Optional) Output modifier.</td></tr> <tr> <td><b>begin regex</b></td><td>Begins with the line that matches the regular expression. You can enter multiple expressions.</td></tr> <tr> <td><b>exclude regex</b></td><td>Excludes lines that match the regular expression. You can enter multiple expressions.</td></tr> <tr> <td><b>include regex</b></td><td>Includes lines that match the regular expression. You can enter multiple expressions.</td></tr> </table> | <b>list</b> | (Optional) Lists TCP flows that the WAE is currently optimizing or passing through. | <b>!</b> | (Optional) Output modifier. | <b>begin regex</b> | Begins with the line that matches the regular expression. You can enter multiple expressions. | <b>exclude regex</b> | Excludes lines that match the regular expression. You can enter multiple expressions. | <b>include regex</b> | Includes lines that match the regular expression. You can enter multiple expressions. |
| <b>list</b>               | (Optional) Lists TCP flows that the WAE is currently optimizing or passing through.  |             |   |          |                             |                    |   |                      |   |                      |   |
| <b>!</b>                  | (Optional) Output modifier.  |             |   |          |                             |                    |   |                      |   |                      |   |
| <b>begin regex</b>        | Begins with the line that matches the regular expression. You can enter multiple expressions.  |             |   |          |                             |                    |   |                      |   |                      |   |
| <b>exclude regex</b>      | Excludes lines that match the regular expression. You can enter multiple expressions.  |             |   |          |                             |                    |   |                      |   |                      |   |
| <b>include regex</b>      | Includes lines that match the regular expression. You can enter multiple expressions.  |             |   |          |                             |                    |   |                      |   |                      |   |

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator

**Usage Guidelines** The **show filtering list** 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 is sample output from the **show filtering list** command. It displays TFO connection information for the WAE.

```
WAE# show filtering list
E: Established, S: Syn, A: Ack, F: Fin, R: Reset
s: sent, r: received, O: Options, P: Passthrough
B: Bypass, L: Last Ack, W: Time Wait, D: Done
T: Timedout, C: Closed
```

| Local-IP:Port     | Remote-IP:Port    | Tuple(Mate)          | State |
|-------------------|-------------------|----------------------|-------|
| 10.99.11.200:1398 | 10.99.22.200:80   | 0xcb709c0(0xcb70a00) | E     |
| 10.99.11.200:1425 | 10.99.22.200:80   | 0xcb70780(0xcb707c0) | E     |
| 10.99.11.200:1439 | 10.99.22.200:5222 | 0xcb703c0(0xcb70b40) | Sr    |
| 10.99.11.200:1440 | 10.99.22.200:5222 | 0xcb70400(0xcb70440) | Sr    |
| 10.99.22.200:1984 | 10.99.11.200:80   | 0xcb70600(0xcb70640) | E     |
| 10.99.22.200:1800 | 10.99.11.200:23   | 0xcb70480(0x0 )      | PE    |
| 10.99.11.200:1392 | 10.99.22.200:80   | 0xcb70f80(0x0 )      | E     |

|                   |                   |                        |    |
|-------------------|-------------------|------------------------|----|
| 10.99.22.200:20   | 10.99.11.200:1417 | 0xcb701c0(0xcb70180)   | E  |
| 10.99.11.200:1417 | 10.99.22.200:20   | 0xcb70180(0x0 )        | E  |
| 10.99.22.200:1987 | 10.99.11.200:80   | 0xcb70240(0xcb70200)   | E  |
| 10.99.11.200:1438 | 10.99.22.200:5222 | 0xcb70900(0xcb70580)   | Sr |
| 10.99.22.200:1990 | 10.99.11.200:80   | 0xcb70100(0xcb70140)   | E  |
| 10.99.22.200:80   | 10.99.11.200:1426 | 0xcb70740(0xcb70700)   | E  |
| 10.99.22.200:80   | 10.99.11.200:1425 | 0xcb707c0(0xcb70780)   | E  |
| 10.99.22.200:1985 | 10.99.11.200:80   | 0xcb70a40(0xcb70a80)   | E  |
| 10.99.22.200:80   | 10.99.11.200:1410 | 0xcb70500(0xcb70540)   | E  |
| 10.99.22.200:80   | 10.99.11.200:1398 | 0xcb70a00(0xcb709c0)   | E  |
| 10.99.22.200:80   | 10.99.11.200:1392 | 0xcb70f40(0xcb70f80)   | E  |
| 10.0.19.5:54247   | 10.1.242.5:80     | 0xc9e5b400(0xc9e5b100) | ED |



**Note** The “ED” state occurs when one socket in the pair is closed (D), but the mate is still established (E).

## Related Commands

- [show accelerator](#)
- [show statistics filtering](#)
- [show statistics auto-discovery](#)
- [show statistics connection closed](#)

**show flash**

## 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  
central-manager

**Examples** Table 3-39 describes the fields shown in the **show flash** command display.

**Table 3-39 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  
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 3-40 describes the fields shown in the **show hardware** command display.

**Table 3-40 Field Descriptions for the show hardware Command**

| Field   | Description   |
|---|---|
| Cisco Wide Area Application Services Software (WAAS)                                  | Software application, copyright, release, and build information.  |
| Copyright (c) year by Cisco Systems, Inc.   |   |
| Cisco Wide Area Application Services Software Release XXX (build bXXX month day year) |   |
| 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. |
| CPU 0 is  | CPU manufacturer information.                                     |
| Total X CPU   | Number of CPUs on the device.                                     |

**Table 3-40 Field Descriptions for the show hardware Command (continued)**

| <b>Field</b>                   | <b>Description</b>   |
|--------------------------------|--|
| 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 (*).<br>Disk identification number and type, for example:(h00 c00i00 100 - DAS).<br>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.   |

**Table 3-40 Field Descriptions for the show hardware Command (continued)**

| Field                       | Description  |
|-----------------------------|--|
| 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

## 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  
central-manager

**Usage Guidelines** The **show hosts** command lists the name servers and their corresponding IP addresses. It also lists the hostnames, their corresponding IP addresses, and their corresponding aliases (if applicable) in a host table summary.

**Examples** Table 3-41 describes the fields shown in the **show hosts** command display.

**Table 3-41 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.   |
| <b>Host Table</b> |   |
| 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 <b>host</b> global configuration command. |

**Related Commands** [\(config\) ip hosts](#)

# 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  
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 3-42 describes the fields shown in the **show inetd** command display.

**Table 3-42 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](#)

**show interface**

# 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 1 | usb}
```

|                           |                                   |  |
|---------------------------|-----------------------------------|--|
| <b>Syntax Description</b> | <b>GigabitEthernet slot/port</b>  | Displays the Gigabit Ethernet interface device information (only on suitably equipped systems). 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 (/). |
|                           | <b>ide control_num</b>            | Displays the IDE interface device information (controller number 0–1).   |
|                           | <b>InlineGroup slot/grpnumber</b> | Displays the inline group information. Slot and inline group number for the selected interface.  |
|                           | <b>InlinePort</b>                 | Displays the inline port information. Slot and inline group number for the selected interface.   |
|                           | <b>lan</b>                        | Displays the inline port information for the LAN port.   |
|                           | <b>wan</b>                        | Displays the inline port information for the WAN port.   |
|                           | <b>PortChannel port-num</b>       | Displays the port channel interface device information (number 1).   |
|                           | <b>scsi device_num</b>            | Displays the SCSI interface device information (number 0–7).   |
|                           | <b>standby 1</b>                  | Displays the standby group information.  |
|                           | <b>usb</b>                        | Displays the USB interface device information.   |

|                 |                                |
|-----------------|--------------------------------|
| <b>Defaults</b> | No default behavior or values. |
|-----------------|--------------------------------|

|                      |      |
|----------------------|------|
| <b>Command Modes</b> | EXEC |
|----------------------|------|

|                     |  |
|---------------------|--|
| <b>Device Modes</b> | application-accelerator<br>central-manager |
|---------------------|--|

|                 |  |
|-----------------|--|
| <b>Examples</b> | The following is sample output from the <b>show interface</b> command. It 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 3-43 describes the fields shown in the **show interface GigabitEthernet** command display.

**Table 3-43 Field Descriptions for the show interface GigabitEthernet Command**

| Field                      | Description   |
|----------------------------|---|
| Description                | Description of the device, as configured by using the <b>description</b> option of the <b>interface</b> 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.  |
| Link State                 | Interface and link status.  |
| Mode                       | Speed setting, transmission mode, and transmission speed for this interface.  |

Table 3-44 describes the fields shown in the **show interface InlinePort** command display.

show interface

**Table 3-44 Field Descriptions for the show interface InlinePort Command**

| <b>Field</b>                          | <b>Description</b>  |
|---------------------------------------|---|
| 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.  |
| Internet address                      | IP address (for WAN port only).   |
| Broadcast address                     | Broadcast address (for WAN port only).  |
| Netmask                               | Subnet mask (for WAN port only).  |
| 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.  |

**Table 3-44 Field Descriptions for the show interface InlinePort Command (continued)**

| Field        | Description  |
|--------------|--|
| Base address | Base address. hexadecimal value.   |
| Flags        | Interface status indicators. Values include Up, Broadcast, Running, and Multicast. |
| Link State   | Interface and link status.   |
| Mode         | Speed setting, transmission mode, and transmission speed for this interface.       |

Table 3-45 describes the fields shown in the **show interface PortChannel** command display.

**Table 3-45 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.  |
| Link State                 | Interface and link status.  |

show interface

[Table 3-46](#) describes the field shown in the **show interface scsi** command display.

**Table 3-46 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 3-47](#) describes the fields shown in the **show interface standby** command display.

**Table 3-47 Field Descriptions for the show interface standby Command**

| Field               | Description   |
|---------------------|---|
| Description         | Description of the device, as configured by using the <b>description</b> option of the <b>interface</b> global configuration command.   |
| Interface Standby 1 | Number that identifies the standby group and the number of associated physical interfaces.  |
| 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, and indicates if the interface is active (has an active layer 2 connection to a switch), primary (configured as primary in the running configuration), and in use (carrying network traffic). |
| Type                | Type of interface. Always Ethernet.   |
| ...                 | The following fields are the same as for a gigabit Ethernet interface, as shown in <a href="#">Table 3-43</a> .   |

#### Related Commands

[\(config\) interface GigabitEthernet](#)

[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  
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 nonvolatile memory of the WAAS device.

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 nonvolatile memory of the WAAS device 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 3-48 describes the fields shown in the **show inventory** command display.

**Table 3-48 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**

# 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]**

|                           |   |
|---------------------------|---|
| <b>Syntax Description</b> | <i>acl-name</i> (Optional) Information for a specific access list, using an alphanumeric identifier up to 30 characters, beginning with a letter.<br><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  
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 3-49 describes the fields shown in the **show ip access-list** command display.

**Table 3-49 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 3-49 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:<br><i>interface slot/port</i><br><i>interface direction</i><br><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:<br><i>application type</i><br><i>access list type and number</i><br><i>associated port</i> |

**Related Commands**[clear arp-cache](#)[\(config\) ip access-list](#)

**show ip routes**

# 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  
central-manager

**Usage Guidelines** The **show ip routes** 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 3-50 describes the fields shown in the **show ip routes** command display.

**Table 3-50 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.<br><br>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 kdump

To display the kernel crash dump information for a WAAS device, use the **show kdump** EXEC command.

## show kdump

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

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator  
central-manager

**Examples** Table 3-51 describes the fields shown in the **show kdump** command display.

**Table 3-51 Field Descriptions for the show kdump Command**

| Field             | Description                                       |
|-------------------|---|
| Kdump state       | Enabled or not enabled.                           |
| Kdump operation   | Operational or not operational.                   |
| Kdump crashkernel | Crash kernel information (Memory @ Base Address). |

**Related Commands** [\(config\) kernel kdump](#)  
[\(config\) logging console](#)

---

 show kerberos

## 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  
central-manager

---

**Examples** Table 3-52 describes the fields shown in the **show kerberos** command display.

**Table 3-52 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 arp-cache](#)  
[\(config\) logging console](#)

# show license

To display license information for a WAAS device, use the **show license** EXEC command.

## show license

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

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator  
central-manager

**Examples** The following is sample output from the **show license** command. It lists the WAAS licenses, giving the name, status, date applied, and the name of the user that applied the license for each active license.

```
WAE# show license
License Name      Status      Activation Date      Activated by
-----
Transport        not active
Enterprise       active       11/12/2008          admin
Video            not active
Virtual-Blade    not active
```

**Related Commands** [clear arp-cache](#)  
[license add](#)

---

 show logging

# 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  
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 is sample output from the **show logging** command. It 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 arp-cache](#)  
[\(config\) logging console](#)  
[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  
central-manager

**Examples** Table 3-53 describes the fields shown in the **show memory** command display.

**Table 3-53 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**

## show ntp

To display the NTP parameters for a WAAS device, use the **show ntp** EXEC command.

**show ntp status**

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | <b>status</b> Displays NTP status.   |
| <b>Defaults</b>           | No default behavior or values.   |
| <b>Command Modes</b>      | EXEC   |
| <b>Device Modes</b>       | application-accelerator<br>central-manager   |
| <b>Examples</b>           | Table 3-54 describes the fields shown in the <b>show ntp status</b> command display. |

**Table 3-54 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 (local, unicast, multicast, or broadcast).  |
| 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. |
| delay       | Estimated delay (in milliseconds) between the requester and the server.  |

**Table 3-54 Field Descriptions for the show ntp status Command (continued)**

| Field  | Description                          |
|--------|--------------------------------------|
| offset | Clock offset relative to the server. |
| jitter | Clock jitter.                        |

**Related Commands**[clock](#)[\(config\) clock](#)[\(config\) ntp](#)

---

 show policy-engine application

# 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}**

|                           |                       |  |
|---------------------------|-----------------------|--|
| <b>Syntax Description</b> | <b>classifier</b>     | Displays information about the specified application classifier. If no classifier is specified, the <b>show policy-engine application</b> 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.  |
|                           | <b>dynamic</b>        | Shows the application dynamic match information.   |
|                           | <b>name</b>           | Shows the application names list.  |

---

|          |                                |
|----------|--------------------------------|
| Defaults | No default behavior or values. |
|----------|--------------------------------|

---

|                      |      |
|----------------------|------|
| <b>Command Modes</b> | EXEC |
|----------------------|------|

---

|                     |                         |
|---------------------|-------------------------|
| <b>Device Modes</b> | application-accelerator |
|---------------------|-------------------------|

---

|                         |   |
|-------------------------|---|
| <b>Usage Guidelines</b> | Use the <b>show policy-engine application dynamic</b> command to display auto-discovered CIFS file servers that are added to the list (for WAFS legacy mode only). 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. |
|-------------------------|---|

---

|                 |  |
|-----------------|--|
| <b>Examples</b> | <a href="#">Table 3-55</a> describes the fields shown in the <b>show policy-engine application classifier</b> command display. |
|-----------------|--|

**Table 3-55 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:<br>0) AFS<br>match dst port range 7000 7009<br>1) Altiris-CarbonCopy<br>match dst port eq 1680 |

**Table 3-56** describes the fields shown in the **show policy-engine application dynamic** command display.

**Table 3-56 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.  |

**show policy-engine application**

**Table 3-57** describes the fields shown in the **show policy-engine application name** command display.

**Table 3-57 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  
(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

# show policy-engine status

To display high-level information about a WAE policy engine, use the **show policy-engine status** EXEC command.

**show policy-engine status**

---

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

---

**Defaults** No default behavior or values.

---

**Command Modes** EXEC

---

**Device Modes** application-accelerator

---

**Usage Guidelines** The **show policy-engine status** command displays information including the usage of the available resources, which include application names, classifiers, conditions, and service classes.

---

**Examples** Table 3-58 describes the fields shown in the **show policy-engine status** command display.

**Table 3-58 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.                             |
| Service-Classes                | Total number of service classes configured. Number of service classes being used. Number of service classes available. The maximum number of service classes allowed is 256. |

---

**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
(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**

# 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}**

|                           |   |
|---------------------------|---|
| <b>Syntax Description</b> | <b>drivers</b> Displays printer drivers on this print server.<br><b>user <i>username</i></b> Specifies a username that belongs to the print admin group.<br><b>process</b> Displays information about the print server and print spooler. |
|---------------------------|---|

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator  
central-manager

**Examples** Table 3-59 describes the fields shown in the **show print-services process** command display.

**Table 3-59 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.  |
| <b>Print Server Status</b> |   |
| 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.   |
| Connected at               | Date and time of connection to the print server.  |

**Table 3-59 Field Descriptions for the show print-services process Command (continued)**

| Field   | Description  |
|---|--|
| 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 configuration](#)[\(config\) print-services](#)[show authentication](#)[windows-domain](#)[\(config\) windows-domain](#)

**show processes**

# 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 secs | count num]]
```

| Syntax Description |  |
|--------------------|--|
| <b>cpu</b>         | (Optional) Displays CPU utilization.   |
| <b>debug pid</b>   | (Optional) Prints the system call and signal traces for a specified process identifier to display system progress. |
| <b>memory</b>      | (Optional) Displays memory allocation processes.   |
| <b>system</b>      | (Optional) Displays system load information in terms of updates.   |
| <b>delay secs</b>  | (Optional) Specifies the delay between updates, in seconds (1–60).   |
| <b>count num</b>   | (Optional) Specifies the number of updates that are displayed (1–100).   |

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-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. The **show processes debug** 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.



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 3-60 describes the fields shown in the **show processes** command display.

**Table 3-60 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.<br>R = running<br>S = sleeping in an interruptible wait<br>D = sleeping in an uninterruptible wait or swapping<br>Z = zombie<br>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

# 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  
central-manager

**Examples** Table 3-61 describes the fields shown in the **show radius-server** command display.

**Table 3-61 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

## show running-config

To display a WAAS device current running configuration on the terminal, use the **show running-config** EXEC command. The **show running-config** command replaces the **write terminal** command.

**show running-config [no-policy]**

|                           |   |
|---------------------------|---|
| <b>Syntax Description</b> | <b>no-policy</b><br><br>(Optional) Does not display policy engine configuration.  |
| <b>Defaults</b>           | No default behavior or values.  |
| <b>Command Modes</b>      | EXEC  |
| <b>Device Modes</b>       | application-accelerator<br>central-manager  |
| <b>Usage Guidelines</b>   | Use this EXEC command in conjunction with the <b>show startup-config</b> command to compare the information in running memory to the startup configuration used during bootup.  |
| <b>Examples</b>           | The following is sample output from the <b>show running-config</b> command. It displays the currently running configuration of a WAAS device.<br><br>WAE# <b>show running-config</b><br>! WAAS version 4.0.0<br>!<br>device mode central-manager<br>!<br>!<br>hostname waas-cm<br>!<br>!<br>!<br>!<br>exec-timeout 60<br>!<br>!<br>primary-interface GigabitEthernet 1/0<br>!<br>!<br>... |
| <b>Related Commands</b>   | <b>configure</b><br><br><b>copy running-config</b>  |

**copy startup-config**

**show services**

# show services

To display services-related information for a WAAS device, use the **show services** EXEC command.

```
show services {ports [port-num] | summary}
```

|                           |   |
|---------------------------|---|
| <b>Syntax Description</b> | <b>ports</b> Displays services by port number.<br><i>port-num</i> (Optional) Up to 8 port numbers (1–65535).<br><b>summary</b> Displays the services summary. |
|---------------------------|---|

|                 |                                |
|-----------------|--------------------------------|
| <b>Defaults</b> | No default behavior or values. |
|-----------------|--------------------------------|

|                      |      |
|----------------------|------|
| <b>Command Modes</b> | EXEC |
|----------------------|------|

|                     |  |
|---------------------|--|
| <b>Device Modes</b> | application-accelerator<br>central-manager |
|---------------------|--|

|                 |  |
|-----------------|--|
| <b>Examples</b> | The following is sample output from the <b>show services</b> command. It 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 the current values of the Samba configuration file, *smb.conf*, on a WAAS device, 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  
central-manager

**Usage Guidelines** The **show smb-conf** 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 is sample output from the **show smb-conf** command. It 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
```

**show smb-conf**

```

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   |   |
|----------------------|---|
| <b>alarm-history</b> | Displays SNMP alarm history information.          |
| <b>engineID</b>      | Displays local SNMP engine identifier.            |
| <b>event</b>         | Displays events configured through the Event MIB. |
| <b>group</b>         | Displays SNMP groups.                             |
| <b>stats</b>         | Displays SNMP statistics.                         |
| <b>user</b>          | Displays SNMP users.                              |

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator  
central-manager

**Usage Guidelines** The **show snmp alarm-history** command provides information on various SNMP variables and statistics on SNMP operations.

**Examples** Table 3-62 describes the fields shown in the **show snmp alarm-history** command display.

**Table 3-62 Field Descriptions for the show snmp alarm-history Command**

| Field    | Description  |
|----------|--|
| Index    | Displays 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 the table below to map module names to module IDs.)       |
| Category | Traps sent by a WAE contain numeric category IDs. (See the table below to map category names to category IDs.) |
| Descr    | Provides description of the WAAS software alarm and the application that generated the alarm.                  |

show snmp

[Table 3-63](#) summarizes the mapping of module names to module IDs.

**Table 3-63 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 3-64](#) summarizes the mapping of category names to category IDs.

**Table 3-64 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 3-65](#) describes the fields shown in the **show snmp engineID** command display.

**Table 3-65 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 3-66](#) describes the fields shown in the **show snmp event** command display. The **show snmp event** command displays information about the SNMP events that were set using the [snmp trigger](#) command:

**Table 3-66 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. |

**Table 3-66 Field Descriptions for the show snmp event Command (continued)**

| Field          | Description  |
|----------------|--|
| (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 <b>show</b> output.   |
| Comment:       | Description of the trigger 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:          | <p>Type of trigger test to perform based on the SNMP trigger configured. The Test field may contain the following types of tests:</p> <ul style="list-style-type: none"> <li>Absent—Absent existence of a test</li> <li>Boolean—Boolean value test</li> <li>Equal—Equality threshold test</li> <li>Falling—Falling threshold test</li> <li>Greater-than—Greater-than threshold test</li> <li>Less-than—Less-than threshold test</li> <li>On-change—Changed existence test</li> <li>Present—Present present test</li> <li>Rising—Rising threshold test</li> </ul> |
| ObjectOwner:   | Name of the object owner who created the trigger using the <b>snmp trigger create</b> 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.  |
| Cmp:           | <p>Comparison. Type of boolean comparison to perform. The numbers 1–6 correspond to these Boolean comparisons:</p> <ul style="list-style-type: none"> <li>unequal (1)</li> <li>equal (2)</li> <li>less (3)</li> <li>lessOrEqual (4)</li> <li>greater (5)</li> <li>greaterOrEqual (6)</li> </ul>  |

show snmp

**Table 3-66 Field Descriptions for the show snmp event Command (continued)**

| <b>Field</b>       | <b>Description</b>   |
|--------------------|--|
| 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 <b>show</b> output. The fields are repeated for each instance listed in this <b>show</b> command. |

Table 3-67 describes the fields shown in the **show snmp group** command display.

**Table 3-67 Field Descriptions for the show snmp group Command**

| <b>Field</b>   | <b>Description</b>  |
|----------------|---|
| 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 3-68 describes the fields shown in the **show snmp stats** command display.

**Table 3-68 Field Descriptions for the show snmp stats Command**

| <b>Field</b>                                  | <b>Description</b>  |
|---|---|
| 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.                      |

**Table 3-68 Field Descriptions for the show snmp stats Command (continued)**

| Field                         | Description  |
|-------------------------------|--|
| 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 3-69 describes the fields shown in the **show snmp user** command display.

**Table 3-69 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**
- (config) **snmp-server notify inform**
- (config) **snmp-server user**

■ show snmp

(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  
central-manager

**Examples** Table 3-70 describes the fields shown in the **show ssh** command display.

**Table 3-70 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 startup-config

# 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 arguments or keywords.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-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 is sample output from the **show startup-config** command. It 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 accelerator

## show statistics accelerator

To display application accelerator general statistics for a WAAS device, use the **show statistics accelerator** EXEC command.

```
show statistics accelerator cifs [detail | expert mbean attrib]
show statistics accelerator detail
show statistics accelerator epm [detail]
show statistics accelerator generic {connections {cifs | epm | http | mapi | nfs | ssl | video} | detail}
show statistics accelerator http [detail]
show statistics accelerator mapi [detail]
show statistics accelerator nfs [detail]
show statistics accelerator ssl [detail]
show statistics accelerator video [detail]
```

| Syntax Description         |  |
|----------------------------|--|
| <b>cifs</b>                | Displays statistics for the CIFS application accelerator.                              |
| <b>detail</b>              | Displays detailed statistics.  |
| <b>expert mbean attrib</b> | Displays CIFS accelerator expert mode attributes. Mbean name and Mbean attribute name. |
| <b>epm</b>                 | Displays statistics for the EPM application accelerator.                               |
| <b>generic</b>             | Displays statistics for the generic application accelerator.                           |
| <b>connections</b>         | Displays generic connection statistics.  |
| <b>http</b>                | Displays statistics for the HTTP application accelerator.                              |
| <b>mapi</b>                | Displays statistics for the MAPI application accelerator.                              |
| <b>nfs</b>                 | Displays statistics for the NFS application accelerator.                               |
| <b>ssl</b>                 | Displays statistics for the SSL application accelerator.                               |
| <b>video</b>               | Displays statistics for the video application accelerator.                             |

---

**Defaults** No default behavior or values.

---

**Command Modes** EXEC

---

**Device Modes** application-accelerator

**Usage Guidelines**

Using the **show statistics accelerator** command with no options displays a summary of the statistical information for all application accelerators. To obtain detailed statistics for an application accelerator, use the command options to filter the results.

**Examples**

[Table 3-71](#) describes the fields shown in the **show statistics accelerator cifs** command display.

**Table 3-71 Field Descriptions for the show statistics accelerator cifs Command**

| Field                                   | Description   |
|---|---|
| Time Accelerator was started            | Time that the accelerator was started.  |
| Time Statistics were Last Reset/Cleared | Time that the statistics were last reset or cleared.  |
| Total Handled Connections               | Connections handled since the accelerator was started or its statistics last reset.   |
| Total Optimized Connections             | Connections previously and currently optimized by the accelerator.  |
| Total Pushed Down Connections           | Connections initially accepted by accelerator, but later handed off to generic optimization with no acceleration. Occurs if the CIFS server requires a digital signature.   |
| Total Dropped Connections               | Connections dropped for reasons other than client/server socket errors or close.  |
| Current Active Connections              | Current active connections.   |
| Current Pending Connections             | Current connections pending to be accepted.   |
| Maximum Active Connections              | Maximum active connections handled simultaneously.  |
| Local response number                   | Number of local CIFS command responses sent to the client without waiting for a response from the peer WAE.   |
| Average local response time             | Average time used for local responses, in microseconds.   |
| Remote response number                  | Number of CIFS commands forwarded to the CIFS server for a response.  |
| Average remote response time            | Average time used for remote responses, in microseconds.  |
| Policy Engine Statistics                |   |
| Session timeouts                        | Number of times the accelerator application did not issue a keepalive to the Policy Engine in a timely manner. A session refers to the particular registration of the accelerator application within the Policy Engine. |
| Total timeouts                          | Total number of times the accelerator application did not issue a keepalive to the Policy Engine in a timely manner. This may encompass multiple registrations.   |
| Last keepalive received                 | Amount of time since the last keepalive (seconds).  |

show statistics accelerator

**Table 3-71 Field Descriptions for the show statistics accelerator cifs Command (continued)**

| Field  | Description  |
|--|--|
| Last registration occurred                     | Amount of time since the accelerator application registered with the Policy Engine (seconds). Most likely causes are: <ul style="list-style-type: none"> <li>• WAE was rebooted</li> <li>• Configuration change with the accelerator application enabled</li> <li>• Restart of the accelerator application by the Node Manager</li> </ul>  |
| Hits   | Number of connections that had a configured policy that specified the use of the accelerator application.  |
| Updated Released                               | Number of hits that were released during auto-discovery and did not make use of the accelerator application.   |
| Active Connections                             | Number of hits that represent either active connections using the accelerator application or connections that are still in the process of performing auto-discovery.   |
| Completed Connections                          | Number of hits that have made use of the accelerator application and have completed.   |
| Drops  | Number of hits that attempted use of the accelerator application but were rejected for some reason. A separate hit and drop will be tallied for each TCP SYN packet received for a connection. This includes the original SYN and any retries.   |
| Rejected Connection Counts Due To:<br>(Total:) | <ul style="list-style-type: none"> <li>• Number of all of the reject reasons that represent hits that were not able to use the accelerator applications. Reject reasons include the following:               <ul style="list-style-type: none"> <li>• Not registered</li> <li>• Keepalive timeout</li> <li>• No license</li> <li>• Load level not within range</li> <li>• Connection limit exceeded</li> <li>• Rate limit exceeded (a new connection exceeded the number of connections allowed within the time window)</li> <li>• Minimum TFO not available</li> <li>• Resource manager (minimum resources not available)</li> <li>• Global config optimization disabled</li> <li>• TFO limit exceeded (systemwide connection limit reached)</li> <li>• Server-side invoked</li> <li>• DM deny (Policy Engine dynamic match deny rule matched)</li> <li>• No DM accept was matched</li> </ul> </li> </ul> |
| Auto-Discovery Statistics                      |  |
| Connections queued for accept                  | Number of connections added to the accelerator connection accept queue by auto discovery.  |

**Table 3-71 Field Descriptions for the show statistics accelerator cifs Command (continued)**

| Field                     | Description   |
|---------------------------|---|
| Accept queue add failures | Number of connections that could not be added to the accelerator connection accept queue due to a failure. The failure could possibly be due to the accelerator not being present, or a queue overflow. |
| AO discovery successful   | For the accelerators that work in dual-ended mode, accelerator discovery (as part of auto discovery) is performed. This counter indicates the number of times accelerator discovery was successful.     |
| AO discovery failure      | The number of times accelerator discovery failed. Possible reasons include the accelerator not being enabled or running on the peer WAE, or the license not configured for the accelerator.             |

Table 3-72 describes the fields shown in the **show statistics accelerator epm detail** command display.

**Table 3-72 Field Descriptions for the show statistics accelerator epm Command**

| Field  | Description  |
|--|--|
| Global TCP AO connection statistics              |  |
| Time Accelerator was started                     | Time that the accelerator was started.               |
| Time Statistics were Last Reset/Cleared          | Time that the statistics were last reset or cleared. |
| Total Handled Connections                        | Total connections handled.                           |
| Total Optimized Connections                      | Total optimized connections.                         |
| Total Pushed Down Connections                    | Total pushed down connections.                       |
| Total Dropped Connections                        | Total dropped connections.                           |
| Current Active Connections                       | Current active connections.                          |
| Current Pending Connections                      | Current pending connections.                         |
| Maximum Active Connections                       | Maximum active connections.                          |
| Total Requests                                   | Total requests.                                      |
| Total Requests Successfully Parsed               | Total requests successfully parsed.                  |
| Total Request Errors                             | Total request errors.                                |
| Total Responses                                  | Total responses.                                     |
| Total Responses Successfully Parsed              | Total responses successfully parsed.                 |
| Total Service-unavailable Responses              | Total service-unavailable responses.                 |
| Total Requests for UUID not in Policy Engine Map | Total requests for UUID not in policy engine map.    |
| Total Response Errors                            | Total response errors.                               |

Table 3-73 describes the fields shown in the **show statistics accelerator generic connections detail** command display. This command shows the aggregated statistics for all connections.

show statistics accelerator

**Table 3-73 Field Descriptions for the show statistics accelerator generic Command**

| Field  | Description   |
|--|---|
| Time elapsed since "clear statistics"                            | Time that has elapsed since the statistics were last reset.   |
| Time Accelerator was started                                     | Local time accelerator was started or restarted.  |
| Time Statistics were Last Reset/Cleared                          | Local time accelerator was last started or restarted, or the <b>clear statistics</b> command was executed since accelerator was last started or restarted.  |
| Total Handled Connections  | <p>Connections handled since the accelerator was started or its statistics last reset. Incremented when a connection is accepted or reused. Never decremented.</p> <p>This value will always be greater than or equal to the Current Active Connections statistic. Includes all connections accepted by the accelerator even if later pushed down to generic optimization, dropped, or handed-off to another accelerator.</p> <p>Total Handled Connections = Total Optimized Connections + Total Pushed Down Connections + Total Dropped Connections.</p> |
| Total Optimized Connections                                      | Connections previously and currently optimized by the accelerator. This includes: Current Active Connections + Total Fast Connections + Fast connections initiated by peer.   |
| Total Connections Handed-off with Compression Policies Unchanged | Connections initially accepted by accelerator, but later handed off to generic optimization without policy changes so the current negotiated policies for compression (DRE/LZ) will be used.  |
| Total Dropped Connections  | Connections dropped for any reason other than client/server socket errors or close (for instance, out of resources).  |
| Current Active Connections                                       | <p>Number of WAN side connections currently established and either in use or free for fast connection use.</p> <p>WAN side connections currently established and in use can be calculated as follows: Current Active Connections - Total Active Connections Free For Fast Connection Use Not cleared using <b>clear statistics accelerator</b> command.</p>   |
| Current Pending Connections                                      | Number of SYN requests queued waiting for the accelerator to accept.  |
| Maximum Active Connections                                       | Highest number of active connections since accelerator was last started/restarted. Not cleared using the <b>clear statistics accelerator</b> command.   |
| Global Generic AO Connection Statistics                          |   |

**Table 3-73 Field Descriptions for the show statistics accelerator generic Command (continued)**

| Field   | Description  |
|---|--|
| Total number of connections handled           | Connections handled since the accelerator was started or its statistics last reset. Incremented when a connection is accepted or reused. Never decremented.<br><br>This value will always be greater than or equal to the Current Active Connections statistic. Includes all connections accepted by the accelerator even if later pushed down to generic optimization, dropped, or handed-off to another accelerator.<br><br>Total Handled Connections = Total Optimized Connections + Total Pushed Down Connections + Total Dropped Connections. |
| Total number of active connections            | Total number of hits that represent either active connections using the accelerator application.   |
| Total number of bytes transferred from client | Total number of bytes transferred from the client side.  |
| Total number of bytes transferred from server | Total number of bytes transferred from the server side.  |
| Policy Engine Statistics                      |  |
| Session timeouts                              | The number of times the accelerator application did not issue a keepalive to the Policy Engine in a timely manner. A session refers to the particular registration of the accelerator application within the Policy Engine.  |
| Total timeouts                                | The total number of times the accelerator application did not issue a keepalive to the Policy Engine in a timely manner. This may encompass multiple registrations.  |
| Last keepalive received                       | The amount of time since the last keepalive (seconds).   |
| Last registration occurred                    | The amount of time since the accelerator application registered with the Policy Engine (seconds). Most likely causes are: <ul style="list-style-type: none"> <li>• WAE was rebooted</li> <li>• Configuration change with the accelerator application enabled</li> <li>• Restart of the accelerator application by the Node Manager</li> </ul>  |
| Hits  | Number of connections that had a configured policy that specified the use of the accelerator application.  |
| Updated Released                              | Number of hits that were released during Auto-Discovery and did not make use of the accelerator application.   |
| Active Connections                            | Number of hits that represent either active connections using the accelerator application or connections that are still in the process of performing Auto-Discovery.   |
| Completed Connections                         | Number of hits that have made use of the accelerator application and have completed.   |

show statistics accelerator

**Table 3-73 Field Descriptions for the show statistics accelerator generic Command (continued)**

| Field  | Description  |
|--|--|
| Drops  | Number of hits that attempted use of the accelerator application but were rejected for some reason. A separate hit and drop will be tallied for each TCP SYN packet received for a connection. This includes the original SYN and any retries.   |
| Rejected Connection Counts Due To:<br>(Total:) | <ul style="list-style-type: none"> <li>• The number of all of the reject reasons that represent hits that were not able to use the accelerator applications. Reject reasons include the following:           <ul style="list-style-type: none"> <li>• Not registered</li> <li>• Keepalive timeout</li> <li>• No license</li> <li>• Load level not within range</li> <li>• Connection limit exceeded</li> <li>• Rate limit exceeded (a new connection exceeded the number of connections allowed within the time window)</li> <li>• Minimum TFO not available</li> <li>• Resource manager (minimum resources not available)</li> <li>• Global config optimization disabled</li> <li>• TFO limit exceeded (systemwide connection limit reached)</li> <li>• Server-side invoked</li> <li>• DM deny (Policy Engine dynamic match deny rule matched)</li> <li>• No DM accept was matched</li> </ul> </li> </ul> |

Table 3-74 describes the fields shown in the **show statistics accelerator http** command display.

**Table 3-74 Field Descriptions for the show statistics accelerator http Command**

| Field                                   | Description   |
|---|---|
| Time Accelerator was started            | Local time accelerator was started or restarted.  |
| Time Statistics were Last Reset/Cleared | Local time accelerator was last started or restarted, or the <b>clear statistics accelerator [http   all]</b> command was executed since accelerator was last started or restarted. |

**Table 3-74 Field Descriptions for the show statistics accelerator http Command (continued)**

| Field  | Description   |
|--|---|
| Total Handled Connections  | <p>Connections handled since the accelerator was started or its statistics last reset. Incremented when a connection is accepted or reused. Never decremented.</p> <p>This value will always be greater than or equal to the Current Active Connections statistic. Includes all connections accepted by the accelerator even if later pushed down to generic optimization, dropped, or handed-off to another accelerator.</p> <p>Total Handled Connections = Total Optimized Connections + Total Pushed Down Connections + Total Dropped Connections.</p> |
| Total Optimized Connections                                      | <p>Connections previously and currently optimized by the HTTP Accelerator. This includes: Current Active Connections + Total Fast Connections + Fast connections initiated by peer.</p>   |
| Total Connections Handed-off with Compression Policies Unchanged | <p>Connections initially accepted by accelerator, but later handed off to generic optimization without policy changes so the current negotiated policies for compression (DRE/LZ) will be used.</p>   |
| Total Dropped Connections  | <p>Connections dropped for any reason other than client/server socket errors or close (for instance, out of resources).</p>   |
| Current Active Connections.                                      | <p>Number of WAN side connections currently established and either in use or free for fast connection use.</p> <p>WAN side connections currently established and in use can be calculated as follows: Current Active Connections - Total Active Connections Free For Fast Connection Use<br/>Not cleared using <b>clear statistics accelerator [http   all]</b> command.</p>  |
| Current Pending Connections                                      | <p>Number of SYN requests queued waiting for the accelerator to accept.</p>   |
| Maximum Active Connections                                       | <p>Highest number of active connections since accelerator was last started/restarted. Not cleared using the <b>clear statistics accelerator [http   all]</b> command.</p>   |
| Total Time Saved (ms)  | <p>Total time saved in milliseconds. Incremented on client side WAE by 1 RTT whenever an idle fast connection is reused instead of establishing a new WAN connection.</p>   |
| Current Active Connections Free for Fast Connection Use          | <p>Number of Current Active Connections that are idle and available for reuse as a fast connection. Incremented when an in-use active connection becomes idle and is available for reuse as a fast connection.</p> <p>Decremented when an available idle active connection is reused or its idle timeout (5 secs) is reached. Not cleared using the <b>clear statistics accelerator [http   all]</b> command.</p>   |

show statistics accelerator

**Table 3-74 Field Descriptions for the show statistics accelerator http Command (continued)**

| Field   | Description   |
|---|---|
| Total Connections Handed-off                                    | Total Pushed Down Connections + Total Connections Handed-off with Compression Policies Disabled.  |
| Total Connections Handed-off with Compression Policies Disabled | Total number of connections handed off to generic optimization with compression policies disabled. This statistic includes handoffs for SSL CONNECT requests received by the HTTP Accelerator.                                    |
| Total Connections Handed-off to SSL                             | Total number of connections handed off to the SSL accelerator as a result of SSL CONNECT requests received by the HTTP Accelerator.   |
| Total Connection Hand-off Failures                              | Total number of connections that were attempted to be handed off but the hand off failed.   |
| Total Fast Connection Successes                                 | Total number of times a client side idle active WAN connection was able to be reused instead of establishing a new WAN connection.  |
| Total Fast Connection Failures                                  | Total number of times a client side idle active WAN connection was attempted to be reused, but the reuse failed.  |
| Maximum Fast Connections on a Single Connection                 | Maximum number of times a single connection was reused. This is the “best case” of number of reuses on a single connection.<br>Limited to be less than maximum session reuse count (currently defined as 100 - an arbitrary max). |
| Total CONNECT Requests with Incomplete Message                  | Total number of SSL CONNECT requests with an incomplete message.  |
| Percentage of connection time saved                             | (Total Time Saved / (Total Time Saved + Total Round Trip Time For All Connections)) * 100.  |
| Total Round Trip Time for All Connections (ms)                  | Total RTT for all WAN connections that have been established.   |
| Total Fast Connections Initiated by Peer                        | Total number of times the server side WAN connection was a fast connection initiated by the client side peer.<br>This statistic should match the Total Fast Connections on the peer WAE.  |
| Policy Engine Statistics  |   |
| Session timeouts  | The number of times the accelerator application did not issue a keepalive to the Policy Engine in a timely manner. A session refers to the particular registration of the accelerator application within the Policy Engine.       |
| Total timeouts  | The total number of times the accelerator application did not issue a keepalive to the Policy Engine in a timely manner. This may encompass multiple registrations.   |
| Last keepalive received   | The amount of time since the last keepalive (seconds).  |

**Table 3-74 Field Descriptions for the show statistics accelerator http Command (continued)**

| Field                      | Description   |
|----------------------------|---|
| Last registration occurred | The amount of time since the accelerator application registered with the Policy Engine (seconds). Most likely causes are: <ul style="list-style-type: none"> <li>• WAE was rebooted</li> <li>• Configuration change with the accelerator application enabled</li> <li>• Restart of the accelerator application by the Node Manager</li> </ul> |
| Hits                       | Number of connections that had a configured policy that specified the use of the accelerator application.   |
| Updated Released           | Number of hits that were released during Auto-Discovery and did not make use of the accelerator application.  |
| Active Connections         | Number of hits that represent either active connections using the accelerator application or connections that are still in the process of performing Auto-Discovery.  |
| Completed Connections      | Number of hits that have made use of the accelerator application and have completed.  |
| Drops                      | Number of hits that attempted use of the accelerator application but were rejected for some reason. A separate hit and drop will be tallied for each TCP SYN packet received for a connection. This includes the original SYN and any retries.  |

show statistics accelerator

**Table 3-74 Field Descriptions for the show statistics accelerator http Command (continued)**

| Field  | Description  |
|--|--|
| Rejected Connection Counts Due To:<br>(Total:) | <ul style="list-style-type: none"> <li>The number of all of the reject reasons that represent hits that were not able to use the accelerator applications. Reject reasons include the following:</li> <li>Not registered</li> <li>Keepalive timeout</li> <li>No license</li> <li>Load level not within range</li> <li>Connection limit exceeded</li> <li>Rate limit exceeded (a new connection exceeded the number of connections allowed within the time window)</li> <li>Minimum TFO not available</li> <li>Resource manager (minimum resources not available)</li> <li>Global config optimization disabled</li> <li>TFO limit exceeded (systemwide connection limit reached)</li> <li>Server-side invoked</li> <li>DM deny (Policy Engine dynamic match deny rule matched)</li> <li>No DM accept was matched</li> </ul> |
| <b>Auto-Discovery Statistics</b>               |  |
| Connections queued for accept                  | Number of connections added to the accelerator connection accept queue by auto discovery.  |
| Accept queue add failures                      | Number of connections that could not be added to the accelerator connection accept queue due to a failure. The failure could possibly be due to accelerator not being present, or a queue overflow.  |
| AO discovery successful                        | For the accelerators that work in dual-ended mode, accelerator discovery (as part of auto discovery) is performed. This counter indicates the number of times accelerator discovery was successful.  |
| AO discovery failure                           | The number of times accelerator discovery failed. Possible reasons include accelerator not being enabled or running on the peer WAE, or the license not configured for the accelerator.  |

Table 3-75 describes the fields shown in the **show statistics accelerator mapi** command display.

**Table 3-75 Field Descriptions for the show statistics accelerator map Command**

| <b>Field</b>   | <b>Description</b>   |
|--|--|
| Time Accelerator was started                                     | Time that the accelerator was started.   |
| Time statistics were Last Reset/Cleared                          | Time that the statistics were last reset.  |
| Total Handled Connections  | Number of connections handled since the accelerator was started.   |
| Total Optimized Connections                                      | Number of connections handled since the accelerator was started, from start to finish.                                 |
| Total Connections Handed-off with Compression Policies Unchanged | Number of connections received by the accelerator but to which only generic optimizations were done (no acceleration). |
| Total Dropped Connections  | Number of connections dropped for reasons other than client/server socket errors or close.                             |
| Current Active Connections                                       | Number of connections currently being handled by the accelerator.  |
| Current Pending Connections                                      | Number of connections pending to be accepted.  |
| Maximum Active Connections                                       | Maximum number of simultaneous connections handled by the accelerator.   |
| Number of Synch Get Buffer Requests                              | Number of MAPI SyncGetBuffer calls made. Each call downloads a chunk of data from a cached folder.                     |
| Minimum Synch Get Buffer Size (bytes)                            | Minimum chunk size downloaded by the MAPI SyncGetBuffer call.  |
| Maximum Synch Get Buffer Size (bytes)                            | Maximum chunk size downloaded by the MAPI SyncGetBuffer call.  |
| Average Synch Get Buffer Size (bytes)                            | Average chunk size downloaded by the MAPI SyncGetBuffer call.  |
| Number of Read Stream Requests                                   | Number of MAPI ReadStream calls made. Each call downloads a chunk of data from a noncached folder.                     |
| Minimum Read Stream Buffer Size (bytes)                          | Minimum chunk size downloaded by the MAPI ReadStream call.   |
| Maximum Read Stream Buffer Size (bytes)                          | Maximum chunk size downloaded by the MAPI ReadStream call.   |
| Average Read Stream Buffer Size (bytes)                          | Average chunk size downloaded by the MAPI ReadStream call.   |
| Minimum Accumulated Read Ahead Data Size (bytes)                 | Minimum data size for MAPI read ahead.   |
| Maximum Accumulated Read Ahead Data Size (bytes)                 | Maximum data size for MAPI read ahead.   |
| Average Accumulated Read Ahead Data Size (bytes)                 | Average data size for MAPI read ahead.   |
| Local Response Count   | Number of local MAPI command responses sent to the client without waiting for a response from the peer WAE.            |
| Average Local Response Time (usec)                               | Average time used for local responses, in microseconds.  |

show statistics accelerator

**Table 3-75 Field Descriptions for the show statistics accelerator mapi Command (continued)**

| Field                               | Description   |
|-------------------------------------|---|
| Remote Response Count               | Number of MAPI commands forwarded to the Exchange server for a response.  |
| Average Remote Response Time (usec) | Average time used for remote responses, in microseconds.  |
| Current 2K Accelerated Sessions     | Number of accelerated sessions to Outlook 2000 clients. Sessions (users), not TCP connections.  |
| Current 2K3 Accelerated Sessions    | Number of accelerated sessions to Outlook 2003 clients. Sessions (users), not TCP connections.  |
| Current 2K7 Accelerated Sessions    | Number of accelerated sessions to Outlook 2007 clients. Sessions (users), not TCP connections.  |
| Secured Connections                 | Number of connections to Outlook clients that use encryption. Such connections are not accelerated by the MAPI accelerator.   |
| Lower than 2K Sessions              | Number of sessions to clients using a version of Outlook lower than Outlook 2000. Such connections are not accelerated by the MAPI accelerator.   |
| Higher than 2K7 Sessions            | Number of sessions to clients using a version of Outlook higher than Outlook 2007. Such connections are not accelerated by the MAPI accelerator.  |
| Policy Engine Statistics            |   |
| Session timeouts                    | The number of times the accelerator application did not issue a keepalive to the Policy Engine in a timely manner. A session refers to the particular registration of the accelerator application within the Policy Engine.   |
| Total timeouts                      | The total number of times the accelerator application did not issue a keepalive to the Policy Engine in a timely manner. This may encompass multiple registrations.   |
| Last keepalive received             | The amount of time since the last keepalive (seconds).  |
| Last registration occurred          | The amount of time since the accelerator application registered with the Policy Engine (seconds). Most likely causes are: <ul style="list-style-type: none"> <li>• WAE was rebooted</li> <li>• Configuration change with the accelerator application enabled</li> <li>• Restart of the accelerator application by the Node Manager</li> </ul> |
| Hits                                | Number of connections that had a configured policy that specified the use of the accelerator application.   |
| Updated Released                    | Number of hits that were released during Auto-Discovery and did not make use of the accelerator application.  |
| Active Connections                  | Number of hits that represent either active connections using the accelerator application or connections that are still in the process of performing Auto-Discovery.  |

**Table 3-75 Field Descriptions for the show statistics accelerator map Command (continued)**

| Field  | Description  |
|--|--|
| Completed Connections                          | Number of hits that have made use of the accelerator application and have completed.   |
| Drops  | Number of hits that attempted use of the accelerator application but were rejected for some reason. A separate hit and drop will be tallied for each TCP SYN packet received for a connection. This includes the original SYN and any retries.   |
| Rejected Connection Counts Due To:<br>(Total:) | <ul style="list-style-type: none"> <li>• The number of all of the reject reasons that represent hits that were not able to use the accelerator applications. Reject reasons include the following:</li> <li>• Not registered</li> <li>• Keepalive timeout</li> <li>• No license</li> <li>• Load level not within range</li> <li>• Connection limit exceeded</li> <li>• Rate limit exceeded (a new connection exceeded the number of connections allowed within the time window)</li> <li>• Minimum TFO not available</li> <li>• Resource manager (minimum resources not available)</li> <li>• Global config optimization disabled</li> <li>• TFO limit exceeded (systemwide connection limit reached)</li> <li>• Server-side invoked</li> <li>• DM deny (Policy Engine dynamic match deny rule matched)</li> <li>• No DM accept was matched</li> </ul> |
| <b>Auto-Discovery Statistics</b>               |  |
| Connections queued for accept                  | Number of connections added to the accelerator connection accept queue by auto discovery.  |
| Accept queue add failures                      | Number of connections that could not be added to the accelerator connection accept queue due to a failure. The failure could possibly be due to accelerator not being present, or a queue overflow.  |

show statistics accelerator

**Table 3-75 Field Descriptions for the show statistics accelerator mapi Command (continued)**

| Field                   | Description   |
|-------------------------|---|
| AO discovery successful | For the accelerators that work in dual-ended mode, accelerator discovery (as part of auto discovery) is performed. This counter indicates the number of times accelerator discovery was successful. |
| AO discovery failure    | The number of times accelerator discovery failed. Possible reasons include accelerator not being enabled or running on the peer WAE, or the license not configured for the accelerator.             |

Table 3-76 describes the fields shown in the **show statistics accelerator nfs** command display.

**Table 3-76 Field Descriptions for the show statistics accelerator nfs Command**

| Field  | Description  |
|--|--|
| Time Accelerator was started                                     | Time that the accelerator was started.   |
| Time Statistics were Last Reset/Cleared                          | Time that the statistics were last reset.  |
| Total Handled Connections  | Number of connections handled since the accelerator was started.   |
| Total Optimized Connections                                      | Number of connections optimized by the accelerator.  |
| Total Connections Handed-off with Compression Policies Unchanged | Number of connections received by the accelerator but to which only generic optimizations were done (no acceleration). |
| Total Dropped Connections  | Number of connections dropped for reasons other than client/server socket errors or close.                             |
| Current Active Connections                                       | Number of connections currently being handled by the accelerator.  |
| Current Pending Connections                                      | Number of connections currently pending for the accelerator.   |
| Maximum Active Connections                                       | Maximum number of simultaneous connections handled by the accelerator.   |
| Total RPC Calls per Authentication Flavor                        | Array of the number of RPC calls for each NFS authentication type.   |
| Total RPC Calls with Unknown Authentication Flavor               | Number of RPC calls with an unknown authentication type.   |
| Total RPC Calls per NFS version                                  | Array of the number of RPC calls for each NFS version.   |
| Total RPC Calls with Unknown NFS Version                         | Number of RPC calls with an unknown NFS version.   |
| Total Requests   | Total number of NFS requests received.   |
| Total Local Replies  | Number of requests that resulted in WAAS generating a local reply.   |
| Percentage of Requests Served Locally                            | Percentage of requests served locally by the WAAS device.  |

**Table 3-76 Field Descriptions for the show statistics accelerator nfs Command (continued)**

| Field   | Description   |
|---|---|
| Percentage of Requests Served Remotely            | Percentage of requests served remotely by the NFS server.   |
| Average Time to Generate Local READ Reply (ms)    | Average time to generate a local read reply, in milliseconds.   |
| Average Time to Generate Local WRITE Reply (ms)   | Average time to generate a local write reply, in milliseconds.  |
| Average Time to Generate Local GETATTR Reply (ms) | Average time to generate a local GETATTR reply, in milliseconds.  |
| Average Time to Generate Local Reply (ms)         | Average time to generate a local reply, in milliseconds.  |
| Average Time to Receive Remote Reply (ms)         | Average time to receive a remote reply from the NFS server, in milliseconds.  |
| Meta-Data Cache Access Count                      | Number of times the meta data cache was accessed.   |
| Meta-Data Cache Hit Count                         | Number of meta data cache hits.   |
| Remaining number Of Entries in Meta-Data Cache    | Number of available entries in the meta data cache.   |
| Meta-Data Cache Hit Ratio                         | Percentage of meta data accesses served from the meta data cache.   |
| Policy Engine Statistics                          |   |
| Session timeouts                                  | The number of times the accelerator application did not issue a keepalive to the Policy Engine in a timely manner. A session refers to the particular registration of the accelerator application within the Policy Engine.   |
| Total timeouts                                    | The total number of times the accelerator application did not issue a keepalive to the Policy Engine in a timely manner. This may encompass multiple registrations.   |
| Last keepalive received                           | The amount of time since the last keepalive (seconds).  |
| Last registration occurred                        | The amount of time since the accelerator application registered with the Policy Engine (seconds). Most likely causes are: <ul style="list-style-type: none"> <li>• WAE was rebooted</li> <li>• Configuration change with the accelerator application enabled</li> <li>• Restart of the accelerator application by the Node Manager</li> </ul> |
| Hits  | Number of connections that had a configured policy that specified the use of the accelerator application.   |
| Updated Released                                  | Number of hits that were released during Auto-Discovery and did not make use of the accelerator application.  |
| Active Connections                                | Number of hits that represent either active connections using the accelerator application or connections that are still in the process of performing Auto-Discovery.  |

show statistics accelerator

**Table 3-76 Field Descriptions for the show statistics accelerator nfs Command (continued)**

| Field  | Description  |
|--|--|
| Completed Connections                          | Number of hits that have made use of the accelerator application and have completed.   |
| Drops  | Number of hits that attempted use of the accelerator application but were rejected for some reason. A separate hit and drop will be tallied for each TCP SYN packet received for a connection. This includes the original SYN and any retries.   |
| Rejected Connection Counts Due To:<br>(Total:) | <ul style="list-style-type: none"> <li>• The number of all of the reject reasons that represent hits that were not able to use the accelerator applications. Reject reasons include the following:</li> <li>• Not registered</li> <li>• Keepalive timeout</li> <li>• No license</li> <li>• Load level not within range</li> <li>• Connection limit exceeded</li> <li>• Rate limit exceeded (a new connection exceeded the number of connections allowed within the time window)</li> <li>• Minimum TFO not available</li> <li>• Resource manager (minimum resources not available)</li> <li>• Global config optimization disabled</li> <li>• TFO limit exceeded (systemwide connection limit reached)</li> <li>• Server-side invoked</li> <li>• DM deny (Policy Engine dynamic match deny rule matched)</li> <li>• No DM accept was matched</li> </ul> |
| Auto-Discovery Statistics                      |  |
| Connections queued for accept                  | Number of connections added to the accelerator connection accept queue by auto discovery.  |
| Accept queue add failures                      | Number of connections that could not be added to the accelerator connection accept queue due to a failure. The failure could possibly be due to accelerator not being present, or a queue overflow.  |

**Table 3-76 Field Descriptions for the show statistics accelerator nfs Command (continued)**

| Field                   | Description   |
|-------------------------|---|
| AO discovery successful | For the accelerators that work in dual-ended mode, accelerator discovery (as part of auto discovery) is performed. This counter indicates the number of times accelerator discovery was successful. |
| AO discovery failure    | The number of times accelerator discovery failed. Possible reasons include accelerator not being enabled or running on the peer WAE, or the license not configured for the accelerator.             |

Table 3-77 describes the fields shown in the **show statistics accelerator ssl detail** command display.

**Table 3-77 Field Descriptions for the show statistics accelerator ssl detail Command**

| Field  | Description   |
|--|---|
| Time Accelerator was started                                     | Time stamp of when the accelerator was started. Will change if the accelerator is restarted for any reason.   |
| Time Statistics were Last Reset/Cleared                          | Time stamp of when the accelerator statistics were last set to zero. This value should be the same as the Time Accelerator was started field if the <b>clear stat accelerator all</b> or <b>clear stat accelerator ssl</b> commands were never issued. Otherwise it will show the time at which the <b>clear stat accelerator all</b> or <b>clear stat accelerator ssl</b> commands were last issued. |
| Total Handled Connections  | The number of connections that the SSL accelerator received to provide acceleration services. This includes connections that may have been accelerated successfully, as well as connections which may have experienced errors after arriving at the SSL accelerator.  |
| Total Optimized Connections                                      | The number of connections in which a successful SSL handshake was completed and the connection entered the data transfer phase. Connections that experienced errors during SSL handshake are not counted here. Connections that experienced errors after handshake are counted here. Connections that experienced errors during SSL re-handshake (renegotiation) are also counted here.               |
| Total Connections Handed-off with Compression Policies Unchanged | The number of connections that the SSL accelerator bypassed. No acceleration of these connections was done. This could be because SSL version 2 was negotiated, non-SSL traffic was detected, or SSL accelerator version and/or cipher configuration dictated that the connection should be bypassed.   |

show statistics accelerator

**Table 3-77 Field Descriptions for the show statistics accelerator ssl detail Command (continued)**

| Field                             | Description   |
|-----------------------------------|---|
| Total Dropped Connections         | The number of connections that the SSL accelerator ended prematurely. This could be due to verification failures, revocation check failures, errors detected during the handshake or data transfer phase of the connection, or due to internal errors. Other counters below may shed more light as to why connections were dropped. |
| Current Active Connections        | The number of connections currently being optimized by the SSL accelerator.   |
| Current Pending Connections       | The number of connections that have been determined to be accelerated by the SSL accelerator, and have been queued to be picked up by the accelerator.  |
| Maximum Active Connections        | The maximum value ever reached by the Current Active Connections counter. This counter will be reset if the accelerator is restarted or statistics are cleared.   |
| Total LAN Bytes Read              | The number of bytes read by the SSL accelerator from the original side of the flow.   |
| Total Reads on LAN                | The number of read operations performed by the SSL accelerator on the original side of the flow.  |
| Total LAN Bytes Written           | The number of bytes written by the SSL accelerator on the original side of the flow.  |
| Total Writes on LAN               | The number of write operations performed by the SSL accelerator on the original side of the flow.   |
| Total WAN Bytes Read              | The number of bytes read by the SSL accelerator from the optimized side of the flow.  |
| Total Reads on WAN                | The number of read operations performed by the SSL accelerator on the optimized side of the flow.   |
| Total WAN Bytes Written           | The number of bytes written by the SSL accelerator on the optimized side of the flow.   |
| Total Writes on WAN               | The number of write operations performed by the SSL accelerator on the optimized side of the flow.  |
| Total LAN Handshake Bytes Read    | The number of bytes read from the original side of flows during the handshake phase of flows.   |
| Total LAN Handshake Bytes Written | The number of bytes written to the original side of flows during the handshake phase of flows.  |
| Total WAN Handshake Bytes Read    | The number of bytes read to the optimized side of flows during the handshake phase of flows.  |
| Total WAN Handshake Bytes Written | The number of bytes written to the optimized side of flows during the handshake phase of flows.   |
| Total Accelerator Bytes Read      | An SSL accelerator internal counter. (Bytes read from original side of DRE).  |
| Total Accelerator reads           | An SSL accelerator internal counter. (Read operations performed on original side of DRE).   |

**Table 3-77 Field Descriptions for the show statistics accelerator ssl detail Command (continued)**

| Field  | Description  |
|--|--|
| Total Accelerator Bytes Written                  | An SSL accelerator internal counter. (Bytes written to original side of DRE).  |
| Total Accelerator Writes                         | An SSL accelerator internal counter. (Write operations performed on original side of DRE).   |
| Total DRE Bytes Read                             | An SSL accelerator internal counter. (Bytes read from optimized side of DRE).  |
| Total DRE Reads                                  | An SSL accelerator internal counter. (Read operations performed on the optimized side of DRE).   |
| Total DRE Bytes Written                          | An SSL accelerator internal counter. (Bytes read from optimized side of DRE).  |
| Total DRE Writes                                 | An SSL accelerator internal counter. (Write operations performed on the optimized side of DRE).  |
| Total Failed Handshakes                          | The number of connections that ended during the handshake phase.   |
| Pipe-through due to cipher mismatch              | The number of connections bypassed by SSL accelerator because the SSL cipher negotiated on the flow is configured to be not optimized, or not supported by the WAAS device.  |
| Pipe-through due to version mismatch             | The number of connections bypassed by SSL accelerator because the SSL version negotiated on the flow is configured to be not optimized, or not supported by the WAAS device. |
| Pipe-through due to detection of non-SSL traffic | The number of connections bypassed by SSL accelerator because the content of the flow did not appear to contain SSL messages   |
| Total SSLv3 Negotiated on LAN                    | The number of connections that used SSL version 3 on the original side of the flow.  |
| Total TLSv1 Negotiated on LAN                    | The number of connections that used TLS version 1 on the original side of the flow.  |
| Total SSLv3 Negotiated on WAN                    | The number of connections that used SSL version 3 on the optimized side of the flow.   |
| Total TLSv1 Negotiated on WAN                    | The number of connections that used TLS version 1 on the optimized side of the flow.   |
| Total SSLv3 Negotiated on Peer                   | The number of connections that used SSL version 3 on the control connection between WAAS devices.  |
| Total TLSv1 Negotiated on Peer                   | The number of connections that used TLS version 1 on the control connection between WAAS devices.  |
| Total renegotiations requested by server         | The number of SSL “Hello Request” messages detected by the SSL accelerator.  |
| Total SSL renegotiations performed               | The number of SSL renegotiation attempts (successful and unsuccessful) detected by the SSL accelerator.  |

show statistics accelerator

**Table 3-77 Field Descriptions for the show statistics accelerator ssl detail Command (continued)**

| Field   | Description  |
|---|--|
| [W2W-Srvr] Number of session hits                           | The number of times inter-WAAS SSL session resumption was successful on flows where this WAE was the Core WAE.   |
| [W2W-Srvr] Number of session misses                         | The number of times inter-WAAS SSL full handshake was carried out, on flows where this WAE was the Core WAE.   |
| [W2W-Srvr] Number of sessions timeout                       | The number of SSL sessions that were not reused because they were timed out.   |
| [W2W-Srvr] Number of sessions deleted because of cache full | The number of sessions evicted from inter-WAAS session cache to make room for new sessions.  |
| [W2W-Srvr] Number of bad sessions deleted                   | The number of sessions evicted from inter-WAAS session cache as they were rendered unsuitable for reuse, likely due to connection errors.  |
| [W2W-Comm] Number of sessions inserted into cache           | The number of sessions inserted into the inter-WAAS session cache  |
| [W2W-Comm] Number of sessions evicted from cache            | The number of sessions evicted from the inter-WAAS session cache.  |
| [W2W-Comm] Number of sessions in cache                      | The number of session currently cached in the inter-WAAS session cache.  |
| [W2W-CInt] Number of session hits                           | The number of times an inter-WAAS session resumption was successful on flows where this WAE was the Edge WAE.  |
| [W2W-CInt] Number of session misses                         | The number of times an inter-WAAS full SSL handshake was carried out, on flows where this WAE was the Edge WAE   |
| [W2W-CInt] Number of sessions timeout                       | The number of SSL sessions that were not reused because they were timed out  |
| [W2W-CInt] Number of sessions deleted because of cache full | The number of sessions evicted from inter-WAAS session cache to make room for new sessions   |
| [W2W-CInt] Number of bad sessions deleted                   | The number of sessions evicted from inter-WAAS session cache as they were rendered unsuitable for reuse, likely due to connection errors.  |
| [C2S-Srvr] Number of session hits                           | The number of times a client-requested session was found in the client-facing session cache (even if eventually a full handshake had to be carried out due to session miss between Core WAE and server). |
| [C2S-Srvr] Number of session misses                         | The number of times a client-requested session was not found in the client-facing session cache.   |
| [C2S-Srvr] Number of sessions timeout                       | The number of sessions in the client-facing session cache that were not reused because they were timed out.  |
| [C2S-Srvr] Number of sessions deleted because of cache full | The number of sessions evicted from the client-facing session cache to make room for new sessions.   |

**Table 3-77 Field Descriptions for the show statistics accelerator ssl detail Command (continued)**

| Field  | Description  |
|--|--|
| [C2S-Srvr] Number of bad sessions deleted                    | The number of sessions evicted from the client-facing session cache as they were rendered unsuitable for reuse, likely due to connection errors.                           |
| [C2S-Srvr] Number of sessions inserted into cache            | The number of sessions inserted into the client-facing session cache.  |
| [C2S-Srvr] Number of sessions evicted from cache             | The number of sessions evicted from the client-facing session cache.   |
| [C2S-Srvr] Number of sessions in cache                       | The number of sessions currently cached in the client-facing session cache.  |
| [C2S-Clnt] Number of session hits                            | The number of times a Core-WAE requested session was successfully reused between the Core WAE and server.  |
| C2S-Clnt] Number of session misses                           | The number of times a full SSL handshake had to be carried out between the Core WAE and server.  |
| [C2S-Clnt] Number of sessions timedout                       | The number of times a session in the server-facing session cache could not be reused because it was timed out.   |
| [C2S-Clnt] Number of sessions deleted because of cache full  | The number of sessions evicted from the server-facing session cache to make room for new sessions.   |
| [C2S-Clnt] Number of bad sessions deleted                    | The number of sessions evicted from the server-facing session cache as they were rendered unsuitable for reuse, likely due to connection errors.                           |
| [C2S-Clnt] Number of sessions inserted into cache            | The number of sessions inserted into the server-facing session cache.  |
| [C2S-Clnt] Number of sessions evicted from cache             | The number of sessions evicted from the server-facing session cache.   |
| [C2S-Clnt] Number of sessions in cache                       | The number of sessions currently cached in the server-facing session cache.  |
| Total Successful Certificate Verifications                   | The number of times a certificate was successfully verified (could be client or server).   |
| Total Failed Certificate Verifications                       | The number of times a certificate verification failed (could be for various reasons, other counters may indicate why).   |
| Failed certificate verifications due to invalid certificates | The number of certificate verification attempts failed because the certificate was invalid. An inspection of the SSL accelerator errorlog may indicate the reasons.        |
| Failed Certificate Verifications based on OCSP Check         | The number of certificate verification attempts deemed unsuccessful based on results of OCSP revocation check.   |
| Failed Certificate Verifications (non OCSP)                  | The number of certificate verification attempts deemed unsuccessful based on results of the certificate verification operation.  |
| Total Failed Certificate Verifications due to Other Errors   | The number of certificate verification failures due to other problems (including internal errors). An inspection of the SSL accelerator errorlog may indicate the reasons. |

show statistics accelerator

**Table 3-77 Field Descriptions for the show statistics accelerator ssl detail Command (continued)**

| Field  | Description  |
|--|--|
| Total OCSP Connections Outstanding                       | The number of OCSP requests currently in progress.   |
| Total OCSP Requests Processed                            | The number of OCSP requests completed (including successful and unsuccessful responses).   |
| Maximum Concurrent OCSP Requests                         | The maximum value ever reached by Total OCSP Connections Outstanding counter. This will be reset if the accelerator is restarted or statistics are cleared.  |
| Total Successful OCSP Requests                           | The number of OCSP requests that were completed with a valid response from the OCSP responder.   |
| Total Successful OCSP Requests Returning OK Status       | The number of OCSP request where the certificate status was OK.  |
| Total Successful OCSP Requests with 'NONE' Revocation    | The number of OCSP requests where the OCSP status was deemed OK because of fallback to method configuration: none.   |
| Total Successful OCSP Requests Returning REVOKED Status  | The number of OCSP requests where the certificate status was REVOKED.  |
| Total Successful OCSP Requests Returning UNKNOWN Status  | The number of OCSP requests where the responder did not know the status of the certificate.  |
| Total Failed OCSP Requests                               | The number of OCSP requests which could not be completed successfully.   |
| Total Failed OCSP Requests due to Other Errors           | The number of OCSP requests deemed failed due to internal errors.  |
| Total Failed OCSP Requests due to Connection Errors      | The number of OCSP requests deemed failed because a connection to the OCSP responder could not be set up.  |
| Total Failed OCSP Requests due to Connection Timeouts    | The number of OCSP requests deemed failed because no response was received from the OCSP responder.  |
| Total Failed OCSP Requests due to Insufficient Resources | The number of OCSP requests deemed failed because there was insufficient memory to carry out the revocation check.   |
| Total OCSP Bytes Read                                    | The number of bytes read from connections to OCSP responders.  |
| Total OCSP Write Bytes                                   | The number of bytes written to connections to OCSP responders.   |
| Flows dropped due to verification check                  | The number of connections dropped by this WAE because verification of the client or server certificate failed.   |
| Flows dropped due to revocation check                    | The number of connections dropped by this WAE because revocation check of the client or server certificate failed.   |
| Flows dropped due to other reasons                       | The number of connections dropped by this WAE because of errors which may have prevented the verification check or revocation check from returning a valid result. An inspection of the SSL accelerator errorlog may indicate the reasons. |

Table 3-78 describes the fields shown in the **show statistics accelerator video detail** command display.

**Table 3-78 Field Descriptions for the show statistics accelerator video detail Command**

| Field                                 | Description   |
|---------------------------------------|---|
| Time elapsed since “clear statistics” | Time elapsed since the statistics were last reset.  |
| Connections handled                   |   |
| Total handled                         | Number and percentage of connections handled.   |
| Windows-media live accelerated        | Number and percentage of accelerated connections.   |
| Un-accelerated pipethrough            | Number and percentage of connections passed through the video accelerator but not accelerated.  |
| Un-accelerated dropped due to config  | Number and percentage of connections dropped because the video accelerator detected that the connection could not be accelerated and was configured to drop unaccelerated video traffic. See the fields in the Unaccelerated Connections section for the reasons that the video accelerator cannot accelerate a connection. |
| Error dropped connections             | Number and percentage of dropped connections due to errors.   |
| Windows-media active sessions         |   |
| Outgoing (client) sessions            | Current and maximum number of active Windows Media sessions with clients.   |
| Incoming (server) sessions            | Current and maximum number of active Windows Media sessions with servers.   |
| Unaccelerated Connections             |   |
| Total Unaccelerated                   | Number of unaccelerated connections.  |
| Unsupported player                    | Number of unaccelerated connections due to an unsupported player.   |
| Unsupported transport                 | Number of unaccelerated connections due to an unsupported transport.  |
| Unsupported protocol                  | Number of unaccelerated connections due to an unsupported protocol.   |
| Windows-media VoD                     | Number of unaccelerated connections due to client requesting a video on demand stream.  |
| Max stream bitrate overload           | Number of unaccelerated connections due to stream bit-rate overload.  |
| Max aggregate bitrate overload        | Number of unaccelerated connections due to aggregate bit-rate overload.   |
| Max concurrent sessions overload      | Number of unaccelerated connections due to client session overload.   |
| Other                                 | Number of unaccelerated connections due to other causes.  |
| Error dropped connections             |   |
| Total errors                          | Total number of dropped connections due to errors.  |

show statistics accelerator

**Table 3-78 Field Descriptions for the show statistics accelerator video detail Command**

| Field                           | Description   |
|---------------------------------|---|
| Client timeouts                 | Number of client timeouts.  |
| Server timeouts                 | Number of server timeouts.  |
| Client stream errors            | Number of client stream errors.   |
| Server stream errors            | Number of server stream errors.   |
| Other errors                    | Number of other errors.   |
| Windows-media byte savings      |   |
| % Bytes saved                   | Percentage of bytes saved by the video accelerator.   |
| Incoming (server) bytes         | Number of incoming bytes.   |
| Outgoing (client) bytes         | Number of outgoing bytes.   |
| Windows-media aggregate bitrate |   |
| Total bitrate                   | Total current and maximum bit rate, including both incoming and outgoing traffic.   |
| Outgoing (client) bitrate       | Current and maximum bit rate to clients.  |
| Incoming (server) bitrate       | Current and maximum bit rate from servers.  |
| Policy Engine Statistics        |   |
| Session timeouts                | The number of times the accelerator application did not issue a keepalive to the Policy Engine in a timely manner. A session refers to the particular registration of the accelerator application within the Policy Engine.   |
| Total timeouts                  | The total number of times the accelerator application did not issue a keepalive to the Policy Engine in a timely manner. This may encompass multiple registrations.   |
| Last keepalive received         | The amount of time since the last keepalive (seconds).  |
| Last registration occurred      | The amount of time since the accelerator application registered with the Policy Engine (seconds). Most likely causes are: <ul style="list-style-type: none"> <li>• WAE was rebooted</li> <li>• Configuration change with the accelerator application enabled</li> <li>• Restart of the accelerator application by the Node Manager</li> </ul> |
| Hits                            | Number of connections that had a configured policy that specified the use of the accelerator application.   |
| Updated Released                | Number of hits that were released during Auto-Discovery and did not make use of the accelerator application.  |
| Active Connections              | Number of hits that represent either active connections using the accelerator application or connections that are still in the process of performing Auto-Discovery.  |
| Completed Connections           | Number of hits that have made use of the accelerator application and have completed.  |

**Table 3-78 Field Descriptions for the show statistics accelerator video detail Command**

| Field  | Description  |
|--|--|
| Drops  | Number of hits that attempted use of the video accelerator application but were dropped by the Policy Engine because it detected an overload condition and the video accelerator was configured to drop unaccelerated video traffic due to overload conditions. A separate hit and drop will be tallied for each TCP SYN packet received for a connection. This includes the original SYN and any retries.   |
| Rejected Connection Counts Due To:<br>(Total:) | <ul style="list-style-type: none"> <li>• The number of all of the reject reasons that represent hits that were not able to use the accelerator applications. Reject reasons include the following:</li> <li>• Not registered</li> <li>• Keepalive timeout</li> <li>• No license</li> <li>• Load level not within range</li> <li>• Connection limit exceeded</li> <li>• Rate limit exceeded (a new connection exceeded the number of connections allowed within the time window)</li> <li>• Minimum TFO not available</li> <li>• Resource manager (minimum resources not available)</li> <li>• Global config optimization disabled</li> <li>• TFO limit exceeded (systemwide connection limit reached)</li> <li>• Server-side invoked</li> <li>• DM deny (Policy Engine dynamic match deny rule matched)</li> <li>• No DM accept was matched</li> </ul> |
| <b>Auto-Discovery Statistics</b>               |  |
| Connections queued for accept                  | Number of connections added to the accelerator connection accept queue by auto discovery.  |
| Accept queue add failures                      | Number of connections that could not be added to the accelerator connection accept queue due to a failure. The failure could possibly be due to accelerator not being present, or a queue overflow.  |

■ **show statistics accelerator**

**Table 3-78 Field Descriptions for the show statistics accelerator video detail Command**

| Field                   | Description   |
|-------------------------|---|
| AO discovery successful | For the accelerators that work in dual-ended mode, accelerator discovery (as part of auto discovery) is performed. This counter indicates the number of times accelerator discovery was successful. |
| AO discovery failure    | The number of times accelerator discovery failed. Possible reasons include accelerator not being enabled or running on the peer WAE, or the license not configured for the accelerator.             |

**Related Commands**

[show accelerator](#)

[show statistics connection closed](#)

# show statistics aoim

To display AO (accelerator) Information Manager statistics for a WAAS device, use the **show statistics aoim** EXEC command.

**show statistics aoim [local | peer | detail]**

|                           |   |
|---------------------------|---|
| <b>Syntax Description</b> | <b>aoim</b> Displays statistics for the AO Information Manager for all local application accelerators and all known peers.<br><b>local</b> Displays statistics only for all locally registered application accelerators.<br><b>peer</b> Displays statistics only for all peer WAAS devices encountered.<br><b>detail</b> Displays detailed statistics that include policy engine and auto-discovery statistics. |
|---------------------------|---|

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator

**Usage Guidelines** Use the **show statistics aoim** command with no options to display statistical information for locally registered application accelerators and all peer WAAS devices that the local WAAS device has encountered.

**Examples** Table 3-79 describes the statistics that are displayed by the **show statistics aoim** EXEC command. Only the Local AOIM Statistics section is displayed when you use the **local** option. Only the Peer AOIM Statistics section is displayed when you use the **peer** option. The Detailed AOIM Statistics section is displayed only when you use the **detail** option.

**Table 3-79 Field Descriptions for the show statistics aoim Command**

| Field                            | Description   |
|----------------------------------|---|
| Local AOIM Statistics            |   |
| Total # Peer Syncs               | Number of times that the AO Information Manager has synchronized with a peer WAAS device. |
| Current # Peer Syncs in Progress | Number of currently active peer synchronizations in progress.                             |
| Maximum # Peer Syncs in Progress | Historical maximum number of concurrently active peer synchronizations in progress.       |
| AOIM DB Size                     | Memory size of the AO Information Management database.                                    |

show statistics aoim

**Table 3-79 Field Descriptions for the show statistics aoim Command (continued)**

| Field                            | Description   |
|----------------------------------|---|
| Number of Peers                  | Number of known or encountered peer WAAS devices.   |
| Number of Local AOs              | Number of application accelerators registered on this WAAS device.  |
| Total # of AO Handoffs & Inserts | Number of application accelerators invoked to handle a connection once a peer synchronization has completed.  |
| AO                               | Name of the locally registered application accelerator.   |
| Version                          | Software version of the locally registered application accelerator.   |
| Registered                       | Registration status of the local application accelerator. An application accelerator may be deregistered but the AO Information Manager will still retain knowledge about it, marking it as unregistered.   |
| # Handoffs                       | Number of times a connection was passed directly to the application accelerator after a peer synchronization has completed.   |
| # Inserts                        | Number of times a connection was passed indirectly to the application accelerator after a peer synchronization has completed.   |
| # Incompatible                   | Number of times a connection was not passed to the application accelerator due to software incompatibility with the peer application accelerator on the peer WAAS device after synchronization has completed.   |
| <b>Peer AOIM Statistics</b>      |   |
| Number of Peers                  | Number of peer WAAS devices encountered.  |
| PEER                             | MAC address of the peer WAAS device, and whether it has been formally registered with the AO Information database.  |
| Peer Software Version            | WAAS software version and build number running on the peer WAAS device. WAAS software versions prior to 4.1 do not have the AO Information Management mechanism, so they are reported as having a software version of 4.0.x.  |
| Peer IP Address                  | IP address of the primary network interface of the peer WAAS device.  |
| AO                               | Name of the registered application accelerator on the peer WAAS device.   |
| VERSION                          | Software version of the registered application accelerator on the peer WAAS device.   |
| COMPATIBLE                       | The compatibility status of the application accelerator on the peer WAAS device with a matching locally-registered application accelerator on this device. Possible values are Y (yes/compatible), N (no/incompatible), and U (unknown). The unknown state may occur if no matching local application accelerator is registered on the local WAAS device.   |
| #CONNNS                          | Number of incoming connections found to have a compatible application accelerator on both the local and peer WAAS devices and scheduled to be processed by the locally compatible application accelerator. Certain conditions may result in a discrepancy between a connection being scheduled to be processed by an application accelerator and being successfully processed, so this value may diverge somewhat from the number of connections that a specific local application accelerator reports. |
| <b>Detailed AOIM Statistics</b>  |   |
| <b>Policy Engine Statistics</b>  |   |

**Table 3-79 Field Descriptions for the show statistics aoim Command (continued)**

| Field                      | Description   |
|----------------------------|---|
| Session timeouts           | The number of times the accelerator application did not issue a keepalive to the Policy Engine in a timely manner. A session refers to the particular registration of the accelerator application within the Policy Engine.   |
| Total timeouts             | The total number of times the accelerator application did not issue a keepalive to the Policy Engine in a timely manner. This may encompass multiple registrations.   |
| Last keepalive received    | The amount of time since the last keepalive (seconds).  |
| Last registration occurred | The amount of time since the accelerator application registered with the Policy Engine (seconds). Most likely causes are: <ul style="list-style-type: none"> <li>• WAE was rebooted</li> <li>• Configuration change with the accelerator application enabled</li> <li>• Restart of the accelerator application by the Node Manager</li> </ul> |
| Hits                       | Number of connections that had a configured policy that specified the use of the accelerator application.   |
| Updated Released           | Number of hits that were released during Auto-Discovery and did not make use of the accelerator application.  |
| Active Connections         | Number of hits that represent either active connections using the accelerator application or connections that are still in the process of performing Auto-Discovery.  |
| Completed Connections      | Number of hits that have made use of the accelerator application and have completed.  |
| Drops                      | Number of hits that attempted use of the accelerator application but were rejected for some reason. A separate hit and drop will be tallied for each TCP SYN packet received for a connection. This includes the original SYN and any retries.  |

show statistics aoim

**Table 3-79 Field Descriptions for the show statistics aoim Command (continued)**

| Field                                       | Description  |
|---|--|
| Rejected Connection Counts Due To: (Total:) | <ul style="list-style-type: none"> <li>• The number of all of the reject reasons that represent hits that were not able to use the accelerator applications. Reject reasons include the following:</li> <li>• Not registered</li> <li>• Keepalive timeout</li> <li>• No license</li> <li>• Load level not within range</li> <li>• Connection limit exceeded</li> <li>• Rate limit exceeded (a new connection exceeded the number of connections allowed within the time window)</li> <li>• Minimum TFO not available</li> <li>• Resource manager (minimum resources not available)</li> <li>• Global config optimization disabled</li> <li>• TFO limit exceeded (systemwide connection limit reached)</li> <li>• Server-side invoked</li> <li>• DM deny (Policy Engine dynamic match deny rule matched)</li> <li>• No DM accept was matched</li> </ul> |
| <b>Auto-Discovery Statistics</b>            |  |
| Connections queued for accept               | Number of connections added to the accelerator connection accept queue by auto discovery.  |
| Accept queue add failures                   | Number of connections that could not be added to the accelerator connection accept queue due to a failure. The failure could possibly be due to accelerator not being present, or a queue overflow.  |
| AO discovery successful                     | For the accelerators that work in dual-ended mode, accelerator discovery (as part of auto discovery) is performed. This counter indicates the number of times accelerator discovery was successful.  |
| AO discovery failure                        | The number of times accelerator discovery failed. Possible reasons include accelerator not being enabled or running on the peer WAE, or the license not configured for the accelerator.  |

#### Related Commands

[show statistics accelerator](#)

# show statistics application

To view the performance statistics for applications running on your WAAS device, use the **show statistics application** EXEC command.

**show statistics application [app\_name | savings app\_name]**

|                           |   |
|---------------------------|---|
| <b>Syntax Description</b> | <i>app_name</i> Displays the statistics for the name of the application.<br><b>savings</b> <i>app_name</i> Displays savings statistics for the name of the application. |
|---------------------------|---|

|                 |                                |
|-----------------|--------------------------------|
| <b>Defaults</b> | No default behavior or values. |
|-----------------|--------------------------------|

|                      |      |
|----------------------|------|
| <b>Command Modes</b> | EXEC |
|----------------------|------|

|                     |  |
|---------------------|--|
| <b>Device Modes</b> | application-accelerator<br>central-manager |
|---------------------|--|

|                         |  |
|-------------------------|--|
| <b>Usage Guidelines</b> | The <b>show statistics application</b> command displays statistics for all of the application traffic running on your network. To view the statistics for one specific class of applications only, use the <i>app_name</i> variable. |
|-------------------------|--|

Table 3-80 lists the valid *app\_name* values you can use with the **show statistics application** EXEC command. For a description of the applications supported by WAAS, see [Appendix A, “Default Application Policies”](#) in the *Cisco Wide Area Application Services Configuration Guide*.

**Table 3-80 app\_name Variable Values for the show statistics application Command**

| <b>app_name Values</b> |                         |                    |                    |
|------------------------|-------------------------|--------------------|--------------------|
| authentication         | backup                  | cad                | call-management    |
| conferencing           | console                 | content-management | directory-services |
| email-and-messaging    | enterprise-applications | file-system        | file-transfer      |
| instant-messaging      | name-services           | other              | p2p                |
| printing               | remote-desktop          | replication        | sql                |
| ssh                    | storage                 | streaming          | systems-management |
| version-management     | vpn                     | wafs               | web                |

|                 |  |
|-----------------|--|
| <b>Examples</b> | Table 3-81 describes the statistics for each class of application that are displayed by the <b>show statistics application</b> EXEC command. |
|-----------------|--|

show statistics application

**Table 3-81 Statistic Descriptions for the show statistics application Command**

| Statistic        | Description   |
|------------------|---|
| Internal Client  | Traffic initiated by the WAE device   |
| Internal Server  | Traffic terminated by the WAE device  |
| Opt Preposition  | Optimized traffic on the WAN side, initiated by the WAE device for preposition purposes                                     |
| Opt TCP Only     | Optimized traffic on the WAN side, optimized at the TFO level only  |
| Opt TCP Plus     | Optimized traffic on the WAN side, optimized at the TFO and DRE/LZ/accelerator levels                                       |
| Orig Preposition | Original traffic (unoptimized) on the LAN side, initiated by the WAE device for preposition purposes                        |
| Orig TCP Only    | Original traffic on the LAN side, optimized at the TFO level only   |
| Orig TCP Plus    | Original traffic on the LAN side, optimized at the TFO and DRE/LZ/accelerator levels  |
| Overall          | Combined TCP only, TCP plus, and preposition traffic together   |
| Preposition      | Traffic initiated by the WAE device for preposition purposes  |
| PT Client        | Pass-through traffic going from the client to the server  |
| PT Config        | Traffic that was passed through because of a defined policy   |
| PT Intermediate  | Traffic that was passed through because the WAE device is between two other WAE devices                                     |
| PT No Peer       | Traffic that was passed through because there was no peer WAAS device   |
| PT Server        | Pass-through traffic going from the server to the client  |
| PT_Other         | Traffic that was passed through because of WAAS device overload, asymmetric routing, blacklisting, or several other reasons |
| TCP Only         | Traffic that is optimized at the TFO level only   |
| TCP Plus         | Traffic that is optimized at the TFO and DRE/LZ/accelerator levels  |

Table 3-82 describes the result values shown for the statistics in the **show statistics application** command display.

**Table 3-82 Result Value Descriptions for the show statistics application Command**

| Result            | Description   |
|-------------------|---|
| Bytes             | The amount of traffic shown as a count of the number of bytes                             |
| Packets           | The amount of traffic shown as a count of the number of packets                           |
| Inbound           | Traffic received by the WAE device  |
| Outbound          | Traffic sent by the WAE device  |
| Active            | The number of connections that are active   |
| Completed         | The number of connection that have been completed   |
| Compression Ratio | The amount of compressed traffic compared to the amount of original, uncompressed traffic |

---

Related Commands [show statistics](#)

---

■ show statistics authentication

# 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  
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 is sample output from the **show statistics authentication** command. It 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 configuration](#)  
[clear arp-cache](#)  
[show authentication](#)

# show statistics auto-discovery

To display Traffic Flow Optimization (TFO) auto-discovery statistics for a WAE, use the **show statistics auto-discovery** EXEC command.

**show statistics auto-discovery [blacklist]**

|                           |   |
|---------------------------|---|
| <b>Syntax Description</b> | <b>blacklist</b> (Optional) Displays the blacklist server statistics. |
|---------------------------|---|

|                 |                                |
|-----------------|--------------------------------|
| <b>Defaults</b> | No default behavior or values. |
|-----------------|--------------------------------|

|                      |      |
|----------------------|------|
| <b>Command Modes</b> | EXEC |
|----------------------|------|

|                     |                         |
|---------------------|-------------------------|
| <b>Device Modes</b> | application-accelerator |
|---------------------|-------------------------|

|                 |  |
|-----------------|--|
| <b>Examples</b> | <a href="#">Table 3-83</a> describes the result values shown for the statistics in the <b>show statistics application</b> command display. |
|-----------------|--|

**Table 3-83 Result Value Descriptions for the show statistics auto-discovery Command**

| Result                   | Description   |
|--------------------------|---|
| Auto discovery structure |   |
| Allocation Failure       | Number of auto-discovery allocation failures.               |
| Allocation Success       | Number of auto-discovery allocation successes.              |
| Deallocations            | Number of auto-discovery connections that were deallocated. |
| Timed Out                | Number of autodiscovery allocations that timed out.         |
| Auto discovery table     |   |
| Bucket Overflows         | Number of auto-discovery table buffer overflows.            |
| Table Overflows          | Number of auto-discovery table overflows.                   |
| Entry Adds               | Number of auto-discovery table option additions.            |
| Entry Drops              | Number of auto-discovery table option deletions.            |
| Entry Count              | Total number of auto-discovery table option entries.        |
| Lookups                  | Number of auto-discovery table lookups performed.           |
| Bind hash add failures   | Number of hash table binds that failed.                     |
| Flow creation failures   | Number of flow creation attempts that failed.               |
| Route Lookup             |   |
| Failures                 | Number of route table lookups that failed.                  |
| Success                  | Number of route table lookups that succeeded.               |

show statistics auto-discovery

**Table 3-83 Result Value Descriptions for the show statistics auto-discovery Command**

| Result                                 | Description   |
|--|---|
| Socket                                 |   |
| Allocation failures                    | Number of socket allocations that failed.   |
| Accept pair allocation failures        | Number of socket pair allocations that failed.  |
| Unix allocation failures               | Number of Unix socket allocations that failed.  |
| Connect lookup failures                | Number of socket connection lookups that failed.  |
| Packets                                |   |
| Memory allocation failures             | Number of packet memory allocations that failed.  |
| Total Sent                             | Total number of auto-discovery packets sent.  |
| Total Received                         | Total number of auto-discovery packets received.  |
| Incorrect length or checksum received  | Number of packets received with an incorrect length or checksum.  |
| Invalid filtering tuple received       | Number of packets received with an incorrect filtering tuple.   |
| Received for dead connection           | Number of packets received for invalid connections.   |
| Ack dropped in synack received state   | Number of acknowledgement packets dropped that were in the synchronize acknowledgement state.   |
| Non Syn dropped in nystate state       | Number on non-SYN packets dropped that were in the nystate state.   |
| Syn-ack packets to int. client dropped | Number of synack packets dropped when being sent to internal client.  |
| Packets dropped state already exists   | Number of packets for which the dropped state already exists.   |
| Auto discovery failure                 |   |
| No peer or asymmetric route            | Auto-discovery failed because no peer was found, or asymmetric routing configuration was indicated.                                       |
| Insufficient option space              | Auto-discovery failed because there was not enough space to add options.  |
| Invalid option content                 | Auto-discovery failed because the content of an option was invalid.   |
| Invalid connection state               | Auto-discovery failed because the connection state was invalid.   |
| Missing Ack conf                       | Auto-discovery failed because of missing auto discovery options that were sent from the edge WAE sends to the core WAE on the ack packet. |
| Intermediate device                    | Auto-discovery failed because a device was discovered between the WAEs.   |
| Version mismatch                       | Auto-discovery failed because the WAAS software versions did not match.   |
| Incompatible Peer                      | Auto-discovery failed because the peer accelerator is not compatible with the accelerator on this WAE.                                    |

**Table 3-83 Result Value Descriptions for the show statistics auto-discovery Command**

| <b>Result</b>                             | <b>Description</b>   |
|---|--|
| AOIM Sync with Peer still in progress     | Auto-discovery failed because AOIM synchronization is still in progress between the peers. |
| Auto discovery success TO                 |  |
| Internal server                           | The address of the internal server.  |
| External server                           | The address of the external server.  |
| Auto discovery success FOR                |  |
| Internal client                           | The address of the internal client.  |
| External client                           | The address of the external client.  |
| Auto discovery success SYN retransmission |  |
| Zero retransmit                           | No retransmissions were required for auto-discovery SYN success.                           |
| One retransmit                            | One retransmission were required for auto-discovery SYN success.                           |
| Two+ retransmit                           | Two or more retransmissions were required for auto-discovery SYN success.                  |
| AO discovery                              |  |
| AO discovery successful                   | Auto-discovery of an application optimizer was successful.                                 |
| AO discovery failure                      | Auto-discovery of an application optimizer was not successful.                             |
| Auto discovery Miscellaneous              |  |
| RST received                              | Number of resets received.   |
| SYNs found with our device id             | SYN packets received indicating WAEs device ID.  |
| SYN retransmit count resets               | Number of resets to the SYN retrasnmission count.  |

**Related Commands**

[show auto-discovery](#)  
[show statistics filtering](#)  
[show statistics tfo](#)  
[show statistics connection closed](#)

---

 show statistics cifs

## show statistics cifs

To display the CIFS statistics information, use the **show statistics cifs** EXEC command.

```
show statistics cifs {cache details | requests}
```

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | <b>cache details</b> Statistics for the CIFS cache.<br><b>requests</b> Statistics for CIFS requests. |
|---------------------------|--|

|                 |                                |
|-----------------|--------------------------------|
| <b>Defaults</b> | No default behavior or values. |
|-----------------|--------------------------------|

|                      |      |
|----------------------|------|
| <b>Command Modes</b> | EXEC |
|----------------------|------|

|                     |                         |
|---------------------|-------------------------|
| <b>Device Modes</b> | application-accelerator |
|---------------------|-------------------------|

|                         |   |
|-------------------------|---|
| <b>Usage Guidelines</b> | Use the <b>show statistics cifs</b> EXEC command to view the CIFS traffic details itemized by request type. The <b>show statistics cifs</b> 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. |
|-------------------------|---|

|                 |  |
|-----------------|--|
| <b>Examples</b> | Table 3-84 describes the fields in the <b>show statistics cifs requests</b> command display. |
|-----------------|--|

**Table 3-84 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.                           |
| CONNECT                     | Connection check command.   |
| total                       | Total number of requests for this command.  |

**Table 3-84 Field Descriptions for the show statistics cifs requests Command (continued)**

| Field          | Description   |
|----------------|---|
| 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 connection

# show statistics connection

To display all connection statistics for a WAAS device, use the **show statistics connection** EXEC command.

## show statistics connection

```
client-ip {ip_address | hostname} | client-port port |
detail [client-ip {ip_address | hostname} | client-port port | peer-id peer_id | server-ip
{ip_address | hostname} | server-port port] |
peer-id peer_id | server-ip {ip_address | hostname} | server-port port] | conn-id connection_id
```

| Syntax Description | <b>client-ip</b>             | (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.   |
|                    | <b>client-port port</b>      | (Optional) Displays the connection statistics for the client with the specified port number (1–65535).                                    |
|                    | <b>detail</b>                | (Optional) Displays detailed connection statistics.   |
|                    | <b>peer-id peer_id</b>       | (Optional) Displays the connection statistics for the peer with the specified identifier. Number from 0 to 4294967295 identifying a peer. |
|                    | <b>server-ip</b>             | (Optional) Displays the connection statistics for the server with the specified IP address or hostname.                                   |
|                    | <b>server-port port</b>      | (Optional) Displays the connection statistics for the server with the specified port number (1–65535).                                    |
|                    | <b>conn-id connection_id</b> | (Optional) Displays the connection statistics for the connection with the specified identifier.   |

---

**Defaults** No default behavior or values.

---

**Command Modes** EXEC

---

**Device Modes** application-accelerator

---

**Usage Guidelines** The **show statistics connection** command displays the statistics for all TCP connections. This information is updated in real time.

Using the **show statistics connection** command with no options displays a summary of all the TCP connections on the WAE. 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-id) show summary information and not details.

---

**Examples** Table 3-85 describes the fields shown in the **show statistics connection** command display.

**Table 3-85 Field Descriptions for the show statistics connection Command**

| <b>Field</b>                                   | <b>Description</b>  |
|--|---|
| Current Active Optimized Flows                 | Number of current active optimized TCP connections of all types.  |
| Current Active Optimized TCP Plus Flows        | Number of current active connections using DRE/LZ optimization or handled by an accelerator.  |
| Current Active Optimized TCP Only Flows        | Number of current active connections using TFO optimization only.   |
| Current Active Optimized TCP Preposition Flows | Number of current active connections that were originated by an accelerator to acquire data in anticipation of its future use.  |
| Current Active Auto-Discovery Flows            | Number of current active connections in the auto-discovery state.   |
| Current Active Pass-Through Flows              | Number of current active pass-through connections.  |
| Historical Flows                               | Number of closed TCP connections for which statistical data exists.   |
| ConnID   | Identification number assigned to the connection.   |
| Source IP:Port                                 | IP address and port of the incoming source connection.  |
| Dest IP:Port                                   | IP address and port of the outgoing destination connection.   |
| PeerID   | The MAC address of the peer device.   |
| Accel  | Types of acceleration in use on the connection.<br>D = DRE, L = LZ, T = TCP optimization, C = CIFS, E = EPM, G = generic, H = HTTP, M = MAPI, N = NFS, S = SSL, V = video |
| Local IP:Port                                  | IP address and port of the incoming local connection.   |
| Remote IP:Port                                 | IP address and port of the outgoing remote connection.  |
| ConnType                                       | Type and status of the connection, for example pass-through or optimized.   |

**Related Commands**[clear arp-cache](#)[show statistics accelerator](#)[show statistics connection egress-methods](#)

---

 show statistics connection auto-discovery

# show statistics connection auto-discovery

To display auto-discovery connection statistics for a WAAS device, use the **show statistics connection auto-discovery** EXEC command.

```
show statistics connection auto-discovery
  client-ip {ip_address | hostname} | client-port port | peer-id peer_id |
  server-ip {ip_address | hostname} | server-port port
```

|                           |   |
|---------------------------|---|
| <b>Syntax Description</b> | <b>auto-discovery</b> (Optional) Displays active connection statistics for auto-discovery connections.<br><b>client-ip</b> (Optional) Displays the connection statistics for the client with the specified IP address or hostname.<br><i>ip_address</i> IP address of a client or server.<br><i>hostname</i> Hostname of a client or server.<br><b>client-port</b> <i>port</i> (Optional) Displays the connection statistics for the client with the specified port number (1–65535).<br><b>peer-id</b> <i>peer_id</i> (Optional) Displays the connection statistics for the peer with the specified identifier. Number from 0 to 4294967295 identifying a peer.<br><b>server-ip</b> (Optional) Displays the connection statistics for the server with the specified IP address or hostname.<br><b>server-port</b> <i>port</i> (Optional) Displays the connection statistics for the server with the specified port number (1–65535). |
| <b>Defaults</b>           | No default behavior or values.  |
| <b>Command Modes</b>      | EXEC  |
| <b>Device Modes</b>       | application-accelerator   |
| <b>Usage Guidelines</b>   | <p>This command displays the statistics for auto-discovery TCP connections. This information is updated in real time.</p> <p>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-id) show summary information and not details.</p>  |
| <b>Examples</b>           | Table 3-86 describes the fields shown in the <b>show statistics connection auto-discovery</b> display.  |

**Table 3-86 Field Descriptions for the show statistics connection auto-discovery Command**

| <b>Field</b>                                   | <b>Description</b>  |
|--|---|
| Current Active Optimized Flows                 | Number of current active optimized TCP connections of all types.  |
| Current Active Optimized TCP Plus Flows        | Number of current active connections using DRE/LZ optimization or handled by an accelerator.  |
| Current Active Optimized TCP Only Flows        | Number of current active connections using TFO optimization only.   |
| Current Active Optimized TCP Preposition Flows | Number of current active connections that were originated by an accelerator to acquire data in anticipation of its future use.                      |
| Current Active Auto-Discovery Flows            | Number of current active connections in the auto-discovery state.   |
| Current Active Pass-Through Flows              | Number of current active pass-through connections.  |
| Historical Flows                               | Number of closed TCP connections for which statistical data exists.   |
| Local IP:Port                                  | IP address and port of the incoming local connection.   |
| Remote IP:Port                                 | IP address and port of the outgoing remote connection.  |
| PeerID   | The MAC address of the peer device.   |
| O-ST   | Origin state of the connection.<br>E = Established, S = Syn, A = Ack, F = Fin, R = Reset,<br>s = sent, r = received, O = Options, P = Passthrough   |
| T-ST   | Terminal state of the connection.<br>E = Established, S = Syn, A = Ack, F = Fin, R = Reset,<br>s = sent, r = received, O = Options, P = Passthrough |
| ConnType                                       | Type of the connection.   |

**Related Commands**[show statistics accelerator](#)[show statistics connection egress-methods](#)

---

 show statistics connection closed

# show statistics connection closed

To display closed connection statistics for a WAAS device, use the **show statistics connection closed** EXEC command.

```
show statistics connection closed
  [cifs | detail | dre | epm | http | mapi | nfs | ssl | tfo | [video [windows-media]]
   [client-ip {ip_address | hostname} | client-port port | conn-id connection_id |
    peer-id peer_id | server-ip {ip_address | hostname} | server-port port]
```

| Syntax Description           |  |
|------------------------------|--|
| <b>closed</b>                | (Optional) Displays closed connection statistics for optimized connections.  |
| <b>cifs</b>                  | (Optional) Displays closed connection statistics for connections optimized by the CIFS application accelerator.                                  |
| <b>detail</b>                | (Optional) Displays detailed closed connection statistics.   |
| <b>dre</b>                   | (Optional) Displays closed connection statistics for connections optimized by the DRE feature.   |
| <b>epm</b>                   | (Optional) Displays closed connection statistics for connections optimized by the EPM application accelerator.                                   |
| <b>http</b>                  | (Optional) Displays closed connection statistics for connections optimized by the HTTP application accelerator.                                  |
| <b>mapi</b>                  | (Optional) Displays closed connection statistics for connections optimized by the MAPI application accelerator.                                  |
| <b>nfs</b>                   | (Optional) Displays closed connection statistics for connections optimized by the NFS application accelerator.                                   |
| <b>ssl</b>                   | (Optional) Displays active connection statistics for connections optimized by the SSL application accelerator.                                   |
| <b>tfo</b>                   | (Optional) Displays closed connection statistics for connections optimized by the TFO application accelerator.                                   |
| <b>video</b>                 | (Optional) Displays closed connection statistics for connections optimized by the video application accelerator.                                 |
| <b>windows-media</b>         | (Optional) Displays active connection statistics for connections optimized by the video application accelerator for Windows Media streams.       |
| <b>client-ip</b>             | (Optional) Displays the closed 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.  |
| <b>client-port port</b>      | (Optional) Displays the closed connection statistics for the client with the specified port number (1–65535).                                    |
| <b>conn-id connection_id</b> | (Optional) Displays closed connection statistics for the connection with the specified identifier.   |
| <b>peer-id peer_id</b>       | (Optional) Displays the closed connection statistics for the peer with the specified identifier. Number from 0 to 4294967295 identifying a peer. |
| <b>server-ip</b>             | (Optional) Displays the connection statistics for the server with the specified IP address or hostname.  |
| <b>server-port port</b>      | (Optional) Displays the connection statistics for the server with the specified port number (1–65535).   |

| <b>Defaults</b>  | No default behavior or values.  |
|--|---|
| <b>Command Modes</b>   | EXEC  |
| <b>Device Modes</b>  | application-accelerator   |
| <b>Usage Guidelines</b>  | Using the <b>show statistics connection closed</b> command with no options displays a summary of the closed TCP connections on the WAE. 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-id) show summary information and not details. |
| <b>Examples</b>  | Table 3-87 describes the fields shown in the <b>show statistics connection closed</b> command display.  |
| <b>Table 3-87 Field Descriptions for the show statistics connection closed Command</b> |   |
| Field  | Description   |
| Current Active Optimized Flows   | Number of current active optimized TCP connections of all types.  |
| Current Active Optimized TCP Plus Flows  | Number of current active connections using DRE/LZ optimization or handled by an accelerator.  |
| Current Active Optimized TCP Only Flows  | Number of current active connections using TFO optimization only.   |
| Current Active Optimized TCP Preposition Flows   | Number of current active connections that were originated by an accelerator to acquire data in anticipation of its future use.  |
| Current Active Auto-Discovery Flows  | Number of current active connections in the auto-discovery state.   |
| Current Active Pass-Through Flows  | Number of current active pass-through connections.  |
| Historical Flows   | Number of closed TCP connections for which statistical data exists.   |
| ConnID   | Identification number assigned to the connection.   |
| Source IP:Port   | IP address and port of the incoming source connection.  |
| Dest IP:Port   | IP address and port of the outgoing destination connection.   |
| PeerID   | The MAC address of the peer device.   |
| Accel  | Types of acceleration in use on the connection.<br>D = DRE, L = LZ, T = TCP optimization, C = CIFS, E = EPM,<br>G = generic, H = HTTP, M = MAPI, N = NFS, S = SSL,<br>V = video   |
| <b>Related Commands</b>  | <a href="#">clear arp-cache</a><br><a href="#">show statistics accelerator</a>  |

■ show statistics connection closed

**show statistics connection egress-methods**

# show statistics connection conn-id

To display connection ID statistics for a WAAS device, use the **show statistics connection conn-id** EXEC command.

**show statistics connection conn-id *connection\_id***

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | <b>conn-id <i>connection_id</i></b> (Optional) Displays connection statistics for the connection with the specified identifier number. |
|---------------------------|--|

|                 |                                |
|-----------------|--------------------------------|
| <b>Defaults</b> | No default behavior or values. |
|-----------------|--------------------------------|

|                      |      |
|----------------------|------|
| <b>Command Modes</b> | EXEC |
|----------------------|------|

|                     |                         |
|---------------------|-------------------------|
| <b>Device Modes</b> | application-accelerator |
|---------------------|-------------------------|

|                         |   |
|-------------------------|---|
| <b>Usage Guidelines</b> | The <b>show statistics connection conn-id</b> command displays the statistics for individual TCP connections. This information is updated in real time. |
|-------------------------|---|

|                 |   |
|-----------------|---|
| <b>Examples</b> | Table 3-84 describes the fields shown in the <b>show statistics connection conn-id</b> command display. |
|-----------------|---|

**Table 3-88 Field Descriptions for the show statistics connection conn-id Command**

| Field                         | Description   |
|-------------------------------|---|
| <b>Connection Information</b> |   |
| Peer ID                       | MAC address of the peer device.   |
| Connection Type               | Type of connection established with the peer.   |
| Start Time                    | Date and time connection started.   |
| Source IP Address             | IP address of the connection source.  |
| Source Port Number            | Port number of the connection source.   |
| Destination IP Address        | IP address of the connection destination.   |
| Destination Port Number       | Port number of the connection destination.  |
| Application Name              | Name of the application traffic on the connection.  |
| Classifier Name               | Name of the application classifier on the connection.   |
| Map Name                      | Name of the policy engine application map.  |
| Directed Mode                 | State of directed mode: true (on) or false (off).   |
| Preposition Flow              | Flow was originated by an accelerator to acquire data in anticipation of its future use: true or false. |

show statistics connection conn-id

**Table 3-88 Field Descriptions for the show statistics connection conn-id Command (continued)**

| Field                                     | Description  |
|---|--|
| Policy Details: Configured                | Name of the configured application policy.   |
| Policy Details: Derived                   | Named of the derived application policy.   |
| Policy Details: Peer                      | Name of the application policy on the peer side.   |
| Policy Details: Negotiated                | Name of the negotiated application acceleration policy.  |
| Policy Details: Applied                   | Name of the applied application acceleration policy.   |
| Accelerator Details: Configured           | Accelerators configured.   |
| Accelerator Details: Derived              | Accelerators derived.  |
| Accelerator Details: Applied              | Accelerators applied.  |
| Accelerator Details: Hist                 | Accelerators historically used.  |
| Original and Optimized Bytes Read/Written | Number of bytes that have been read and written on the original (incoming) side and the optimized (outgoing) side.   |
| <b>DRE Stats</b>                          |  |
| Encode                                    | Statistics for compressed messages.  |
| Overall: [msg   in   out   ratio]         | Aggregated statistics for compressed messages.<br>msg = Total number of messages.<br>in = Number of bytes before decompression.<br>out = Number of bytes after decompression.<br>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.   |
| Avg Latency                               | Average latency (transmission delay) of the DRE traffic.   |
| Encode Th-put                             | Speed of DRE traffic throughput, in kilobytes per second.  |
| Message Size Distribution                 | Percentage of total messages that fall within indicated size ranges.   |
| <b>Connection Details</b>                 |  |
| Chunks                                    | Number of chunks encoded, decode, and anchored (forced).   |
| Total Messages                            | Total number of messages processed and the number of blocks used per message.  |
| Ack [msg   size]                          | Number and size of acknowledgement messages.   |
| Encode Bypass Due To                      | Reason for previous traffic encoding bypass.   |
| Nack                                      | Number and size of negative acknowledgement messages.  |
| R-tx                                      | Number of ready-to-transmit messages.  |
| Aggregation Encode/Decode                 | Aggregated statistics for compressed messages.   |
| <b>TFO Stats</b>                          |  |
| Conn-Type                                 | Type of connection.  |

**Table 3-88 Field Descriptions for the show statistics connection conn-id Command (continued)**

| Field                                      | Description   |
|--|---|
| Policy                                     | Policy in use on connection.  |
| EOT State [write   req   ack   read   ack] | End of transmission state for data written and read.  |
| Socket States                              | Socket states, including <b>read-shut</b> , <b>write-shut</b> , <b>close</b> , <b>choke</b> , and <b>envoy</b> .                                    |
| DRE Hints [local   remote   active]        | Number of DRE hints sent for the local, remote, and active connections.   |
| Read Encode/Decode Flows                   | Number of encode and decode messages, and total bytes used.   |
| Decoder Pending Queue                      | Size of the messages waiting in the decode queue, including maximum size, current size, average size, and the number of flow-control stop messages. |
| Encode/Decode                              | Number of calls encoded and decoded, the message latency (in ms), and the number of transmitted data/acknowledgment frames.                         |
| Writer Pending Queue                       | Size of the messages waiting in the write queue, including maximum size, current size, average size, and the number of flow-control stop messages.  |
| Write                                      | The size of the messages written, total number of messages, the average size, and the message latency (in ms).                                      |

**Related Commands**[clear arp-cache](#)[show statistics accelerator](#)[show statistics connection egress-methods](#)

---

show statistics connection egress-methods

# show statistics connection egress-methods

To display detailed egress method-related information about the connection segments for a WAE, use the **show statistics connection egress-methods** EXEC command.

```
show statistics connection egress-methods
  client-ip {ip_address | hostname} | client-port port | peer-id peer_id |
  server-ip {ip_address | hostname} | server-port port
```

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | <b>client-ip</b> (Optional) Displays the closed connection statistics for the client with the specified IP address or hostname.<br><b>ip_address</b> IP address of a client or server.<br><b>hostname</b> Hostname of a client or server.<br><b>client-port port</b> (Optional) Displays the closed connection statistics for the client with the specified port number (1–65535).<br><b>peer-id peer_id</b> (Optional) Displays the connection statistics for the peer with the specified identifier. Number from 0 to 4294967295 identifying a peer.<br><b>server-ip</b> (Optional) Displays the connection statistics for the server with the specified IP address or hostname.<br><b>server-port port</b> (Optional) Displays the connection statistics for the server with the specified port number (1–65535). |
|---------------------------|--|

---

**Defaults** No default behavior or values.

---

**Command Modes** EXEC

---

**Device Modes** application-accelerator

---

**Usage Guidelines** Using the **show statistics connection egress-methods** command without options displays detailed information about each of the TFO connections for a WAE.

The **show statistics connection egress-methods** 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](#)):

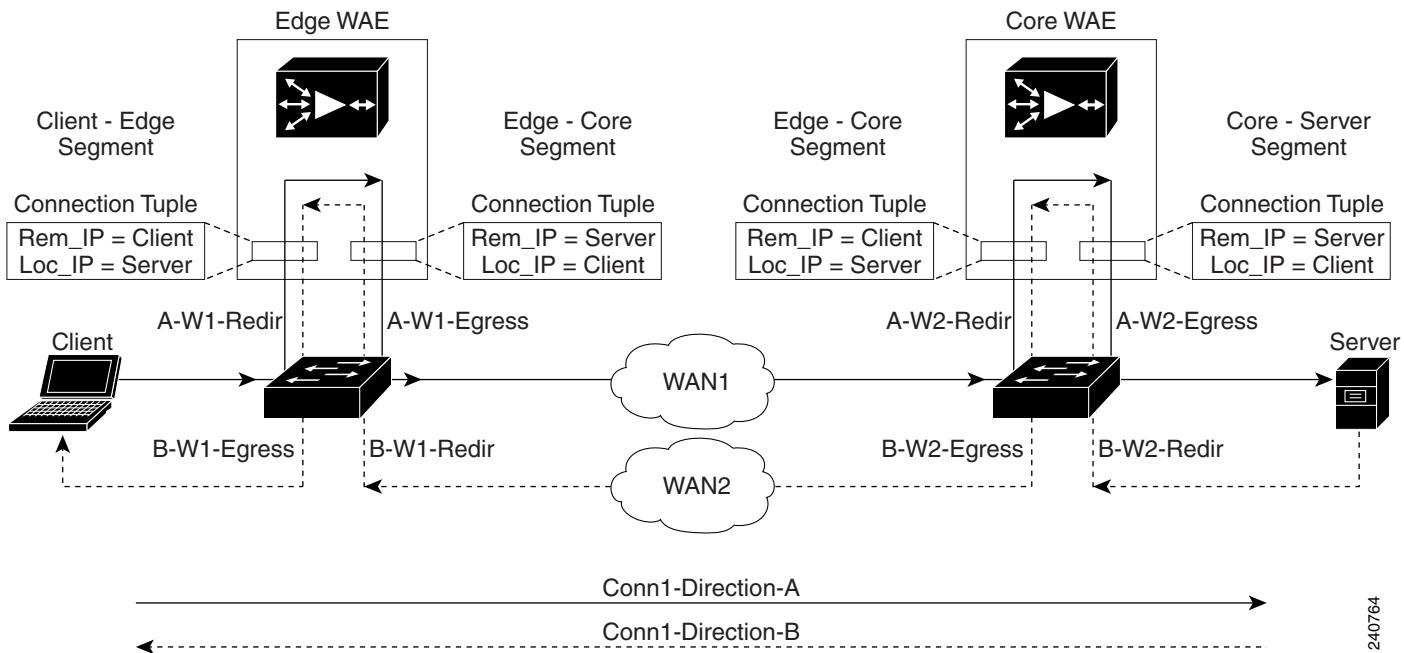
- Between the client and the Edge WAE
- Between the Edge WAE and the Core WAE
- Between the Core WAE and the server

In this example, the Edge WAE has two connection tuples for the two segments that it participates in the following:

- 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 3-89](#).) 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 3-89](#) describes the fields shown in the **show tfo egress-methods connection** command display.

show statistics connection egress-methods

**Table 3-89 Field Descriptions for the show tfo egress-methods connection Command**

| Field                           | Description   |
|---------------------------------|---|
| <b>TUPLE</b>                    |   |
| Client-IP:Port                  | IP address and port number of the client device in the connection tuple.  |
| Server-IP:Port                  | IP address and port number of the server device in the connection tuple.  |
| <b>MATE</b>                     |   |
| Client-IP:Port                  | IP address and port number of the client device in the mate connection tuple.   |
| Server-IP:Port                  | IP address and port number of the server 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. |
| <b>Intercepting device (ID)</b> |   |
| 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 statistics connection optimized

# show statistics connection optimized

To display optimized connection statistics for a WAAS device, use the **show statistics connection optimized** EXEC command.

## show statistics connection optimized

```
client-ip {ip_address | hostname} | client-port port | peer-id peer_id | server-ip {ip_address |
hostname} | server-port port |
{cifs | http | mapi | nfs | ssl | video {detail | windows-media {incoming | outgoing}} | dre { all |
savings | {cifs | http | mapi | nfs | ssl | video}}}]]
```

| Syntax Description             |   |
|--------------------------------|---|
| <b>optimized</b>               | (Optional) Displays active connection statistics for optimized connections.   |
| <b>client-ip</b>               | (Optional) Displays the closed 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.   |
| <b>client-port</b> <i>port</i> | (Optional) Displays the closed connection statistics for the client with the specified port number (1–65535).                                       |
| <b>peer-id</b> <i>peer_id</i>  | (Optional) Displays the connection statistics for the peer with the specified identifier. Number from 0 to 4294967295 identifying a peer.           |
| <b>server-ip</b>               | (Optional) Displays the connection statistics for the server with the specified IP address or hostname.   |
| <b>server-port</b> <i>port</i> | (Optional) Displays the connection statistics for the server with the specified port number (1–65535).  |
| <b>cifs</b>                    | (Optional) Displays closed connection statistics for connections optimized by the CIFS application accelerator.                                     |
| <b>http</b>                    | (Optional) Displays closed connection statistics for connections optimized by the HTTP application accelerator.                                     |
| <b>mapi</b>                    | (Optional) Displays closed connection statistics for connections optimized by the MAPI application accelerator.                                     |
| <b>nfs</b>                     | (Optional) Displays closed connection statistics for connections optimized by the NFS application accelerator.                                      |
| <b>ssl</b>                     | (Optional) Displays active connection statistics for connections optimized by the SSL application accelerator.                                      |
| <b>video</b>                   | (Optional) Displays closed connection statistics for connections optimized by the video application accelerator.                                    |
| <b>detail</b>                  | (Optional) Displays detailed closed connection statistics for connections optimized by the video application accelerator for Windows Media streams. |
| <b>windows-media</b>           | (Optional) Displays active connection statistics for connections optimized by the video application accelerator for Windows Media streams.          |
| <b>incoming</b>                | (Optional) Displays active incoming connection statistics for connections optimized by the video application accelerator for Windows Media streams. |
| <b>outgoing</b>                | (Optional) Displays active outgoing connection statistics for connections optimized by the video application accelerator for Windows Media streams. |
| <b>dre</b>                     | (Optional) Displays closed connection statistics for connections optimized by the DRE feature.  |

---

|                |   |
|----------------|---|
| <b>all</b>     | (Optional) Displays all the connection statistics for connections of the filtered type.     |
| <b>savings</b> | (Optional) Displays the savings connection statistics for connections of the filtered type. |

---

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator

**Usage Guidelines** The **show statistics connection optimized** command displays the statistics for optimized TCP connections. This information is updated in real time.

Using the **show statistics connection optimized** command with no options displays a summary of all the optimized TCP connections on the WAE. 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-id) show summary information and not details.

**Examples** Table 3-90 describes the fields shown in the **show statistics connection optimized** command display.

**Table 3-90 Field Descriptions for the show statistics connection optimized Command**

| Field  | Description  |
|--|--|
| Current Active Optimized Flows                 | Number of current active optimized TCP connections of all types.   |
| Current Active Optimized TCP Plus Flows        | Number of current active connections using DRE/LZ optimization or handled by an accelerator.                                   |
| Current Active Optimized TCP Only Flows        | Number of current active connections using TFO optimization only.  |
| Current Active Optimized TCP Preposition Flows | Number of current active connections that were originated by an accelerator to acquire data in anticipation of its future use. |
| Current Active Auto-Discovery Flows            | Number of current active connections in the auto-discovery state.  |
| Current Active Pass-Through Flows              | Number of current active pass-through connections.   |
| Historical Flows                               | Number of closed TCP connections for which statistical data exists.  |
| ConnID   | Identification number assigned to the connection.  |
| Source IP:Port                                 | IP address and port of the incoming source connection.   |
| Dest IP:Port                                   | IP address and port of the outgoing destination connection.  |

■ **show statistics connection optimized**

**Table 3-90 Field Descriptions for the show statistics connection optimized Command**

| Field  | Description   |
|--------|---|
| PeerID | The MAC address of the peer device.   |
| Accel  | Types of acceleration in use on the connection.<br>D = DRE, L = LZ, T = TCP optimization, C = CIFS, E = EPM,<br>G = generic, H = HTTP, M = MAPI, N = NFS, S = SSL,<br>V = video |

**Related Commands**

- [clear arp-cache](#)
- [show statistics accelerator](#)
- [show statistics connection egress-methods](#)

# show statistics connection pass-through

To display pass through connection statistics for a WAAS device, use the **show statistics connection pass-through** EXEC command.

## show statistics connection pass-through

```
client-ip {ip_address | hostname} | client-port port | peer-id peer_id |
server-ip {ip_address | hostname} | server-port port
```

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | <b>pass-through</b> (Optional) Displays active connection statistics for pass-through connections.<br><b>client-ip</b> (Optional) Displays the closed connection statistics for the client with the specified IP address or hostname.<br><i>ip_address</i> IP address of a client or server.<br><i>hostname</i> Hostname of a client or server.<br><b>client-port port</b> (Optional) Displays the closed connection statistics for the client with the specified port number (1–65535).<br><b>peer-id peer_id</b> (Optional) Displays the connection statistics for the peer with the specified identifier. Number from 0 to 4294967295 identifying a peer.<br><b>server-ip</b> (Optional) Displays the connection statistics for the server with the specified IP address or hostname.<br><b>server-port port</b> (Optional) Displays the connection statistics for the server with the specified port number (1–65535). |
|---------------------------|--|

|                 |                                |
|-----------------|--------------------------------|
| <b>Defaults</b> | No default behavior or values. |
|-----------------|--------------------------------|

|                      |      |
|----------------------|------|
| <b>Command Modes</b> | EXEC |
|----------------------|------|

|                     |                         |
|---------------------|-------------------------|
| <b>Device Modes</b> | application-accelerator |
|---------------------|-------------------------|

|                         |  |
|-------------------------|--|
| <b>Usage Guidelines</b> | The <b>show statistics connection pass-through</b> command displays the statistics for passed through TCP connections. This information is updated in real time. |
|-------------------------|--|

Using the **show statistics connection pass-through** command with no options displays a summary of all the passed through TCP connections on the WAE. 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-id) show summary information and not details.

|                 |  |
|-----------------|--|
| <b>Examples</b> | Table 3-91 describes the fields shown in the <b>show statistics connection pass-through</b> command display. |
|-----------------|--|

show statistics connection pass-through

**Table 3-91 Field Descriptions for the show statistics connection pass-through Command**

| Field  | Description  |
|--|--|
| Current Active Optimized Flows                 | Number of current active optimized TCP connections of all types.   |
| Current Active Optimized TCP Plus Flows        | Number of current active connections using DRE/LZ optimization or handled by an accelerator.                                   |
| Current Active Optimized TCP Only Flows        | Number of current active connections using TFO optimization only.  |
| Current Active Optimized TCP Preposition Flows | Number of current active connections that were originated by an accelerator to acquire data in anticipation of its future use. |
| Current Active Auto-Discovery Flows            | Number of current active connections in the auto-discovery state.  |
| Current Active Pass-Through Flows              | Number of current active pass-through connections.   |
| Historical Flows                               | Number of closed TCP connections for which statistical data exists.  |
| Local IP:Port                                  | IP address and port of the incoming local connection.  |
| Remote IP:Port                                 | IP address and port of the outgoing remote connection.   |
| PeerID   | The MAC address of the peer device.  |
| ConnType                                       | Status of the connection.  |

#### Related Commands

- [clear arp-cache](#)
- [show statistics accelerator](#)
- [show statistics connection egress-methods](#)

# show statistics crypto ssl ciphers

To display crypto SSL cipher usage statistics, use the **show statistics crypto ssl ciphers** EXEC command.

**show statistics crypto ssl ciphers**

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

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator

**Usage Guidelines** The **show statistics crypto ssl ciphers** command displays the number of times each cipher was used on each segment of optimized flows.

**Examples** Table 3-92 describes the fields shown in the **show statistics crypto ssl ciphers** command display.

**Table 3-92 Field Descriptions for the show statistics crypto ssl ciphers Command**

| Field   | Description  |
|---------|--|
| LAN     | Segment between WAAS devices and client or server. |
| WAN     | Segment between WAAS devices for data traffic.     |
| Peering | Segment between WAAS devices for control traffic.  |

**Related Commands** [show crypto](#)

---

 show statistics datamover

# show statistics datamover

To display statistics about the internal datamover component, use the **show statistics datamover** EXEC command.

**show statistics datamover**

---

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

---

**Defaults** No default behavior or values.

---

**Command Modes** EXEC

---

**Device Modes** application-accelerator

---

**Usage Guidelines** The **show statistics datamover** command displays the statistics for the internal datamover component.

---

**Examples** Table 3-96 describes the fields shown in the **show statistics datamover** command display.

**Table 3-93 Field Descriptions for the show statistics datamover Command**

| Field                             | Description   |
|-----------------------------------|---|
| Global Datamover Statistics       |   |
| Datamover users                   | Number of datamover clients (and Area blocks in the output).                                |
| Datamover container maps          | Number of container_map structures allocated.   |
| Datamover containers              | Number of container structures allocated.   |
| Datamover pages                   | Number of system pages used by datamover.   |
| Datamover kmalloc areas           | Number of kmalloc areas used by datamover.  |
| Calls to cs_compact               | Number of calls to cs_compact.  |
| Container map allocation failures | Number of container_map structure allocation failures.                                      |
| Container allocation failures     | Number of container structure allocation failures.  |
| Zone allocation failures          | Number of zone allocation failures.   |
| Kmem allocation failures          | Number of kernel memory allocation failures.  |
| Page allocation failures          | Number of page allocation failures.   |
| Area <i>n</i>                     | Name of application area. There is one Area block in the output for every datamover client. |
| Max Area size in pages            | Total datamover size limit in pages.  |
| Number of identifiers             | Number of distinct datamover objects.   |

**Table 3-93 Field Descriptions for the show statistics datamover Command (continued)**

| <b>Field</b>                   | <b>Description</b>   |
|--------------------------------|--|
| 32 . . . 2048 byte areas used  | Number of storage areas of each size.                              |
| Zone pages used                | Number of pages used for the 32-2048 byte storage areas.           |
| Non-zone pages used            | Number of pages used for page mapping.                             |
| Cloned identifiers             | Number of cloned identifiers.                                      |
| Number of lookup stalls        | Number of lookup stalls.   |
| Calls to cs_compact            | Number of calls to cs_compact.                                     |
| Calls to cs_dup                | Number of calls to cs_dup.   |
| Calls to cs_send_bycopy        | Number of calls to cs_send_bycopy.                                 |
| Calls to cs_send_envoy         | Number of calls to cs_send_envoy.                                  |
| Calls to cs_recv_bycopy        | Number of calls to cs_recv_bycopy.                                 |
| Calls to cs_recv_envoy         | Number of calls to cs_recv_envoy.                                  |
| Identifier allocation failures | Number of identifier allocation failures.                          |
| Address allocation failures    | Number of address allocation failures.                             |
| Total pages used               | Number of pages used and percentage of the maximum area size used. |

---

■ **show statistics directed-mode**

# show statistics directed-mode

To directed mode statistics for a device, use the **show statistics directed-mode** EXEC command.

**show statistics directed-mode**

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

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator

**Examples** Table 3-94 describes the fields shown in the **show statistics directed-mode** command display.

**Table 3-94 Field Descriptions for the show statistics directed-mode Command**

| Field                                      | Description   |
|--|---|
| Cumulative number of connections           | Cumulative number of directed mode connections.   |
| Total outgoing packets encapsulated        | Number of outgoing packets encapsulated.  |
| Total incoming packets de-capsulated       | Number of incoming packets decapsulated.  |
| Total RST+OPT packets received and dropped | Number of RST packets with option 33 set that are received and dropped.                 |
| Outgoing packet encapsulation failed       | Number of outgoing packet encapsulation failures.                                       |
| Invalid incoming packets received          | Number of invalid incoming packets.   |
| Invalid packet length received             | Number of incoming packets with an invalid length.                                      |
| Incoming packet pullups needed             | Number of incoming packets that were fragmented and needed copying from data fragments. |
| Incoming packets with inner fragments      | Number of incoming packets with inner fragments.  |

**Related Commands**

[clear arp-cache](#)  
[show directed-mode](#)  
[show statistics auto-discovery](#)  
[show statistics connection closed](#)  
[\(config\) directed-mode](#)

# show statistics dre

To display Data Redundancy Elimination (DRE) general statistics for a WAE, use the **show statistics dre** EXEC command,

**show statistics dre [detail]**

|                           |               |                                      |
|---------------------------|---------------|--------------------------------------|
| <b>Syntax Description</b> | <b>detail</b> | (Optional) Specifies to show detail. |
|---------------------------|---------------|--------------------------------------|

|                 |                                |
|-----------------|--------------------------------|
| <b>Defaults</b> | No default behavior or values. |
|-----------------|--------------------------------|

|                      |      |
|----------------------|------|
| <b>Command Modes</b> | EXEC |
|----------------------|------|

|                     |                         |
|---------------------|-------------------------|
| <b>Device Modes</b> | application-accelerator |
|---------------------|-------------------------|

|                 |   |
|-----------------|---|
| <b>Examples</b> | <b>Table 3-95</b> describes the fields shown in the <b>show statistics directed-mode</b> command display. This command shows the aggregated statistics for all connections. |
|-----------------|---|

**Table 3-95 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, 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).<br>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.  |
| Connections                  |  |
| Total (cumulative)           | Total cumulative connections.  |
| Encode                       |  |
| Overall: msg, in, out, ratio | All messages coming to DRE components. Number of messages, input bytes, output bytes, compression ratio (in less out, divided by in).          |

show statistics dre

**Table 3-95 Field Descriptions for the show statistics dre Command**

| Field                        | Description  |
|------------------------------|--|
| DRE: msg, in, out, ratio     | All messages handled by DRE compression. Number of DRE compressed messages, input bytes, output bytes, compression ratio (in less out, divided by in). |
| DRE Bypass: msg, in          | Number of messages bypassed by DRE. Number of messages, number of bytes.   |
| LZ: msg, in, out, ratio      | All messages handled by LZ. Number of messages, input bytes, output bytes, compression ratio (in less out, divided by in).                             |
| LZ: bypass: msg, in          | Number of messages bypassed by LZ. Number of messages, number of bytes.  |
| Avg latency: ms, Delayed msg | Average latency introduced to compress a message.  |
| Encode th-put                | Average message size.  |
| Message size distribution    | Message sizes divided into six size groups. Number of message fails into each group and distribution.  |
| Decode                       |  |
| Overall: msg, in, out, ratio | All messages coming to DRE components. Number of messages, input bytes, output bytes, compression ratio (in less out, divided by in).                  |
| DRE: msg, in, out, ratio     | All messages handled by DRE compression. Number of DRE compressed messages, input bytes, output bytes, compression ratio (in less out, divided by in). |
| LZ: msg, in, out, ratio      | Number of messages bypassed by DRE. Number of messages, number of bytes.   |
| LZ: bypass: msg, in          | All messages handled by LZ. Number of messages, input bytes, output bytes, compression ratio (in less out, divided by in).                             |
| Avg latency: ms, Delayed msg | Average latency introduced to compress a message.  |
| Decode th-put:               | Average message size.  |
| Message size distribution    | Message sizes divided into six size groups. Number of message fails into each group and distribution.  |

**Related Commands** [show statistics peer](#)

# show statistics filtering

To display statistics about the incoming and outgoing TFO flows that the WAE currently has, use the **show statistics filtering** EXEC command.

## show statistics filtering

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

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator

**Usage Guidelines** The **show statistics filtering** command displays statistics about the TCP flows that the WAE is handling.

**Examples** Table 3-96 describes the fields shown in the **show statistics filtering** command display.

**Table 3-96 Field Descriptions for the show statistics filtering Command**

| Field  | Description   |
|--|---|
| Number of filtering tuples                             | Number of filtering tuple structures.   |
| Number of filtering tuple collisions                   | Number of times creation of duplicate filtering tuples was detected and avoided.  |
| Packets dropped due to filtering tuple collisions      | Number of packet drops resulting from duplicate filtering tuple detection. Not all duplicate tuple detection results in packet drops. |
| Number of transparent packets locally delivered        | Number of incoming packets delivered to an application on the WAE that is optimizing the connection transparently.                    |
| Number of transparent packets dropped                  | Number of incoming transparent packets dropped.   |
| Packets dropped due to ttl expiry                      | Number of incoming packets dropped because their TTL had reached 0.   |
| Packets dropped due to bad route                       | Number of outgoing packets dropped because route lookup failed.   |
| Syn packets dropped with our own id in the options     | Syn packets output by the auto-discovery module that looped back to the WAE and were dropped.   |
| Syn-Ack packets dropped with our own id in the options | Syn-ack packets output by the auto-discovery module that looped back to the WAE and were dropped.                                     |

show statistics filtering

**Table 3-96 Field Descriptions for the show statistics filtering Command**

| Field  | Description  |
|--|--|
| Internal client syn packets dropped                  | Number of syn packets generated by a process on the WAE that were dropped.   |
| Syn packets received and dropped on estab. conn      | Number of syn packets received for a connection that was in established state. In established state, the syn packet is invalid and is dropped.                                     |
| Syn-Ack packets received and dropped on estab. conn  | Number of syn-ack packets received on a connection that was in established state. In established state, the syn-ack packet is invalid and is dropped.                              |
| Syn packets dropped due to peer connection alive     | Number of syn packets received on a partially terminated connection. In this state, the syn is invalid and is dropped.   |
| Syn-Ack packets dropped due to peer connection alive | Number of syn-ack packets received on a partially terminated connection. In this state, the syn-ack is invalid and is dropped.   |
| Packets recv'd on in progress conn. and not handled  | Number of first packets on an in-progress connection that were dropped. If the first packet seen by the WAE for a connection is not a syn, it is called an in-progress connection. |
| Packets dropped due to peer connection alive         | Number of packets received and dropped on a partially terminated connection.   |
| Packets dropped due to invalid TCP flags             | Number of TCP packets dropped because they had an invalid combination of the syn/find/ack/rst flags set.   |
| Packets dropped by FB packet input notifier          | Number of input packets dropped.   |
| Packets dropped by FB packet output notifier         | Number of output packets dropped.  |
| Number of errors by FB tuple create notifier         | Number of packets dropped because some action that was to be taken when a connection tuple is created failed.  |
| Number of errors by FB tuple delete notifier         | Number of packets dropped because some action that was to be taken when a connection tuple is destroyed failed.  |
| Dropped WCCP GRE packets due to invalid WCCP service | Number of incoming packets received by WCCP GRE intercept that were dropped because of invalid WCCP service information.   |
| Dropped WCCP L2 packets due to invalid WCCP service  | Number of incoming packets received by WCCP L2 intercept that were dropped because of invalid WCCP service information.  |
| Number of deleted tuple refresh events               | Number of times invalid tuples were submitted for garbage collection.  |
| Number of times valid tuples found on refresh list   | Number of times valid tuples were reclaimed from the garbage collector.  |

**Related Commands**[show filtering list](#)[show statistics auto-discovery](#)[show statistics connection closed](#)

# 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}
```

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | <b>filters</b> Displays flow filter statistics.<br><b>monitor</b> Displays flow performance statistics.<br><b>tcpstat-v1</b> Displays tcpstat-v1 collector statistics. |
|---------------------------|--|

|                 |                                |
|-----------------|--------------------------------|
| <b>Defaults</b> | No default behavior or values. |
|-----------------|--------------------------------|

|                      |      |
|----------------------|------|
| <b>Command Modes</b> | EXEC |
|----------------------|------|

|                     |                         |
|---------------------|-------------------------|
| <b>Device Modes</b> | application-accelerator |
|---------------------|-------------------------|

|                 |   |
|-----------------|---|
| <b>Examples</b> | <a href="#">Table 3-97</a> describes the fields shown in the <b>show statistics flow filters</b> command display. |
|-----------------|---|

**Table 3-97 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.<br>CSN: Client-Side Non-Optimized (Edge)<br>SSO: Server-Side Optimized (Edge)<br>CSO: Client-Side Optimized (Core)<br>SSN: Server-Side Non-Optimized (Core)<br>PT: Pass Through (Edge/Core/Intermediate)<br>IC: Internal Client |

show statistics flow

Table 3-98 describes the fields shown in the **show statistics flow monitor** command display.

**Table 3-98 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           | <p>Number of summaries that were discarded because disk space allocated for storage has reached its limit.</p> <p>The numbers in this field indicate when summaries are being collected faster than they are able to be transferred to the collector.</p> <p>Counters in this field generate a data_update alarm.</p> |
| 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 3-98 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.<br>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 arp-cache](#)

---

```
show statistics generic-gre
```

# show statistics generic-gre

To view the GRE tunnel statistics for each intercepting router, use the **show statistics generic-gre** EXEC command.

```
show statistics generic-gre
```

---

**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 **clear statistics generic-gre** EXEC command to clear the generic GRE statistics.

---

**Examples** Table 3-99 describes the fields shown in the **show statistics generic-gre** command display.

**Table 3-99 Field Descriptions for the show statistics generic-gre Command**

| Field   | Description  |
|---|--|
| Tunnel Destination                            | IP address of the GRE tunnel destination.                                    |
| Tunnel Peer Status                            | Tunnel peer status. When the egress method is not generic GRE, N/A is shown. |
| Tunnel Reference Count                        | Number of connections using the tunnel.                                      |
| Packets dropped due to failed encapsulation   | Number of generic GRE packets dropped due to failed encapsulation.           |
| Packets dropped due to no route found         | Number of generic GRE packets dropped due to no route found.                 |
| Packets sent                                  | Number of generic GRE packets sent.  |
| Packets sent to tunnel interface that is down | Number of generic GRE packets sent to a tunnel interface that is down.       |
| Packets fragmented                            | Number of outgoing generic GRE packets fragmented.                           |

---

**Related Commands**

- [clear arp-cache](#)
- [show egress-methods](#)
- [\(config\) egress-method](#)

# 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  
central-manager

**Examples** Table 3-100 describes the fields shown in the **show statistics icmp** command display.

**Table 3-100 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.   |

show statistics icmp

**Table 3-100 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 arp-cache](#)

# 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  
central-manager

**Examples** Table 3-101 describes the fields shown in the **show statistics ip** command display.

**Table 3-101 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.  |

show statistics ip

**Table 3-101 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 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 arp-cache](#)[\(config\) ip](#)

(config-if) ip  
show ip routes

---

 show statistics netstat

# 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  
central-manager

---

**Examples** Table 3-102 describes the fields shown in the **show statistics netstat** command display.

**Table 3-102 Field Descriptions for the show statistics netstat Command**

| Field                                     | Description   |
|---|---|
| Active Internet connections (w/o servers) | The following output prints the 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 pass-through

To display pass-through traffic statistics for a WAAS device, use the **show statistics pass-through** EXEC command.

## **show statistics pass-through**

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

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator

**Examples** Table 3-103 describes the fields shown in the **show statistics pass-through** command display.

**Table 3-103 Field Descriptions for the show statistics pass-through Command**

| Field              | Description   |
|--------------------|---|
| Outbound           |   |
| PT Client: Bytes   | Number of bytes passed through in the client to server direction.   |
| PT Client: Packets | Number of packets passed through in the client to server direction.   |
| PT Server: Bytes   | Number of bytes passed through in the server to client direction.   |
| PT Server: Packets | Number of packets passed through in the server to client direction.   |
| Active/Completed   |   |
| Overall            | Total number of connections passed through.   |
| No Peer            | Number of connections passed through because a remote peer WAE was not found.                                     |
| Rjct Capabilities  | Number of connections passed through due to capability mismatch.  |
| Rjct Resources     | Number of connections passed through due to unavailability of resources.  |
| App Config         | Number of connections passed through due to policy configuration.   |
| Global Config      | Number of connections passed through due to optimization being disabled globally.                                 |
| Asymmetric         | Number of connections passed through due to asymmetric routing in the network (could be an interception problem). |
| In Progress        | Number of connections passed through due to connections seen by the WAE mid-stream.                               |

show statistics pass-through

**Table 3-103 Field Descriptions for the show statistics pass-through Command (continued)**

| Field               | Description  |
|---------------------|--|
| Intermediate        | Number of connections passed through because the WAE was in between two other WAEs.                                      |
| Overload            | Number of connections passed through due to overload.  |
| Internal Error      | Number of connections passed through due to miscellaneous internal errors such as memory allocation failures, and so on. |
| App Override        | Number of connections passed through because an application accelerator requested the connection to be passed through.   |
| Server Black List   | Number of connections passed through due to the server IP being present in the black list.                               |
| AD Version Mismatch | Number of connections passed through due to auto discovery version incompatibility.                                      |
| AD AO Incompatible  | Number of connections passed through due application accelerator versions being incompatible.                            |
| AD AOIM Progress    | Number of connections passed through due to ongoing peer negotiations.   |
| DM Version Mismatch | Number of connections passed through because directed mode, though enabled locally, is not supported by the peer device. |

# show statistics peer

To display peer Data Redundancy Elimination (DRE) statistics for a WAE, use the **show statistics peer** EXEC command.

**show statistics peer**

**show statistics peer dre [context context-value | peer-id peer-id | peer-ip ip-address | peer-no peer-no]**

**show statistics peer dre detail [context context-value | peer-id peer-id | peer-ip ip-address | peer-no peer-no]]**

## Syntax Description

|                              |  |
|------------------------------|--|
| <b>context context-value</b> | Displays peer statistics for the specified context (0–4294967295). |
| <b>peer-id peer-id</b>       | (Optional) Specifies the MAC address of the peer (0–4294967295).   |
| <b>peer-ip ip_address</b>    | (Optional) Specifies the IP address of the peer.                   |
| <b>peer-no peer-no</b>       | (Optional) Specifies the peer number.                              |

## Defaults

No default behavior or values.

## Command Modes

EXEC

## Device Modes

application-accelerator

## Examples

Table 3-104 describes the fields shown in the **show statistics peer dre** command display. This command shows the peer DRE device connection information.

**Table 3-104 Field Descriptions for the show statistics peer dre 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.   |

show statistics peer

**Table 3-104 Field Descriptions for the show statistics peer dre Command (continued)**

| Field                                | Description  |
|--------------------------------------|--|
| Active:                              | Number of connections that are still open.   |
| 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                               | Statistics for compressed messages.  |
| Overall: [msg   in   out   ratio]    | Aggregated statistics for compressed messages.<br>msg = Total number of messages.<br>in = Number of bytes before decompression.<br>out = Number of bytes after decompression.<br>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                               | Statistics for decompressed messages.  |
| Overall: [msg   in   out   ratio]    | Aggregated statistics for decompressed messages.<br>msg = Total number of messages.<br>in = Number of bytes before decompression.<br>out = Number of bytes after decompression.<br>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).<br>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** [show statistics connection closed](#)

---

 show statistics radius

# 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  
central-manager

**Examples** Table 3-105 describes the fields shown in the **show statistics radius** command display.

**Table 3-105 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 3-105 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 arp-cache](#)  
[\(config\) radius-server](#)  
[show radius-server](#)

---

■ show statistics services

# 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  
central-manager

**Examples** Table 3-106 describes the fields shown in the **show statistics services** command display.

**Table 3-106 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  
central-manager

**Examples** Table 3-107 describes the fields shown in the **show statistics snmp** command display.

**Table 3-107 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.  |

■ **show statistics snmp**

**Table 3-107 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 synq

To display the cumulative statistics for the SynQ module, use the **show statistics synq** EXEC command.

**show statistics synq**

**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 statistics synq** command to display statistics for the SynQ module.

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

```
WWAE# show statistics 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
```

**Related Commands** [show synq list](#)

---

 show statistics tacacs

## 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  
central-manager

---

**Examples** Table 3-108 describes the fields shown in the **show statistics tacacs** command display.

**Table 3-108 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 3-108 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 arp-cache](#)  
[\(config\) tacacs](#)  
[show tacacs](#)

---

```
show statistics tcp
```

# 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  
central-manager

**Examples** Table 3-109 describes the fields shown in the **show statistics tcp** command display.

**Table 3-109 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 3-109 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.                    |
| TCP memory usage (KB)             | TCP memory usage.  |
| 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.  |
| 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.   |

show statistics tcp

**Table 3-109 Field Descriptions for the show statistics tcp Command (continued)**

| Field                                       | Description  |
|---|--|
| 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 reneging                           | Number of TCP SACK reneging.   |
| 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.   |
| 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.  |

**Table 3-109 Field Descriptions for the show statistics tcp Command (continued)**

| Field                                   | Description  |
|---|--|
| 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 arp-cache](#)[show tcp](#)[\(config\) tcp](#)

---

 show statistics tfo

# show statistics tfo

To display Traffic Flow Optimization (TFO) statistics for a WAE, use the **show statistics tfo** EXEC command.

**show statistics tfo [connection | detail]**

**show statistics tfo peer [peer-id *peer-id* | peer-ip *peer-ip* | peer-no *peer-no*]**

|                           |   |
|---------------------------|---|
| <b>Syntax Description</b> | <b>connection</b> (Optional) Displays aggregated TFO connection statistics.<br><b>detail</b> (Optional) Displays detailed TFO statistics.<br><b>peer</b> (Optional) Displays DRE peer statistics.<br><b>peer-id <i>peer-id</i></b> (Optional) Displays peer statistics for peer ID.<br><b>peer-ip <i>peer-ip</i></b> (Optional) Displays peer statistics for peer IP.<br><b>peer-no <i>peer-no</i></b> (Optional) Displays peer statistics for peer number. |
|---------------------------|---|

---

|                      |      |
|----------------------|------|
| <b>Command Modes</b> | EXEC |
|----------------------|------|

|                     |                         |
|---------------------|-------------------------|
| <b>Device Modes</b> | application-accelerator |
|---------------------|-------------------------|

---

|                 |   |
|-----------------|---|
| <b>Examples</b> | Table 3-110 describes the fields shown in the <b>show statistics tfo</b> command. The Policy Engine Statistics and Auto-Discovery Statistics sections are displayed only when you use the <b>detail</b> option. |
|-----------------|---|

**Table 3-110 Field Descriptions for the show statistics tfo Command**

| Field                                       | Description   |
|---|---|
| Total number of 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 bypass connections                   | Number of connections using TFO only, with no DRE or LZ.  |
| No. of normal closed connections            | Number of optimized connections closed without any issues using TCP FIN.                                |
| No. of reset connections                    | Number of connections closed with one of the following errors.  |
| 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).  |
| WAN socket close while waiting to write     | The socket between two WAEs (WAN socket) closed before completing writing into it.                      |
| AO socket close while waiting to write      | The socket between the WAE and the client/server (LAN socket) closed before completing writing into it. |

**Table 3-110 Field Descriptions for the show statistics tfo Command (continued)**

| Field   | Description   |
|---|---|
| WAN socket error close while waiting to read      | The socket between two WAEs (WAN socket) closed before completing reading from it.  |
| AO 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.   |
| WAN 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.)  |
| Unoptimized packet received on optimized side     | Unoptimized packet received by the WAE when it expected an optimized packet.  |
| Data buffer usages                                | Data buffer usage statistics for allocated (Used) and cloned buffers. The first column indicates the size of the data stored in the buffers; the second column indicates the size of the buffers; and the third column indicates the number of memory blocks used.                                  |
| Buffer Control                                    | Buffer control statistics for encode and decode queue buffers. The first column indicates the size of the buffers; the second column indicates the number of slow reads issued to control the queue size; and the third column indicates the number of stop reads issued to control the queue size. |
| Scheduler   | Scheduler queue sizes and number of jobs processed by each queue.   |
| Policy Engine Statistics                          |   |
| Session timeouts                                  | The number of times the TFO component did not issue a keepalive to the Policy Engine in a timely manner. A session refers to the particular registration of the TFO component within the Policy Engine.   |
| Total timeouts                                    | The total number of times the TFO component did not issue a keepalive to the Policy Engine in a timely manner. This may encompass multiple registrations.   |
| Last keepalive received                           | The amount of time since the last keepalive (seconds).  |

show statistics tfo

**Table 3-110 Field Descriptions for the show statistics tfo Command (continued)**

| Field  | Description   |
|--|---|
| Last registration occurred                     | The amount of time since the TFO component registered with the Policy Engine (seconds). Most likely causes are: <ul style="list-style-type: none"> <li>• WAE was rebooted</li> <li>• Configuration change with TFO enabled</li> <li>• Restart of the TFO component by the Node Manager</li> </ul>   |
| Hits   | Number of connections that had a configured policy that specified the use of TFO .  |
| Updated Released                               | Number of hits that were released during Auto-Discovery and did not make use of the TFO component.  |
| Active Connections                             | Number of hits that represent either active connections using the TFO component or connections that are still in the process of performing Auto-Discovery.  |
| Completed Connections                          | Number of hits that have made use of the TFO component and have completed.  |
| Drops  | Number of hits that attempted use of the TFO component but were rejected for some reason. A separate hit and drop will be tallied for each TCP SYN packet received for a connection. This includes the original SYN and any retries.  |
| Rejected Connection Counts Due To:<br>(Total:) | <ul style="list-style-type: none"> <li>• The number of all of the reject reasons that represent hits that were not able to use TFO. Reject reasons include the following:               <ul style="list-style-type: none"> <li>• Not registered</li> <li>• Keepalive timeout</li> <li>• No license</li> <li>• Load level not within range</li> <li>• Connection limit exceeded</li> <li>• Rate limit exceeded (a new connection exceeded the number of connections allowed within the time window)</li> <li>• Minimum TFO not available</li> <li>• Resource manager (minimum resources not available)</li> <li>• Global config optimization disabled</li> <li>• TFO limit exceeded (systemwide connection limit reached)</li> <li>• Server-side invoked</li> <li>• DM deny (Policy Engine dynamic match deny rule matched)</li> <li>• No DM accept was matched</li> </ul> </li> </ul> |
| Auto-Discovery Statistics                      |   |
| Connections queued for accept                  | Number of connections added to the TFO connection accept queue by auto discovery.   |

**Table 3-110 Field Descriptions for the show statistics tfo Command (continued)**

| Field                     | Description   |
|---------------------------|---|
| Accept queue add failures | Number of connections that could not be added to the TFO connection accept queue due to a failure. The failure could possibly be due to queue overflow. |
| AO discovery successful   | Number of times TFO discovery was successful.   |
| AO discovery failure      | Number of times TFO discovery failed.   |

**Related Commands** [show statistics connection closed](#)

---

show statistics udp

## 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  
central-manager

---

**Examples** Table 3-111 describes the fields shown in the **show statistics udp** command display.

**Table 3-111 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**

|                           |   |
|---------------------------|---|
| <b>Syntax Description</b> | <b>gre</b><br>Displays WCCP generic routing encapsulation packet-related statistics.  |
| <b>Defaults</b>           | No default behavior or values.  |
| <b>Command Modes</b>      | EXEC  |
| <b>Device Modes</b>       | application-accelerator   |
| <b>Usage Guidelines</b>   | <p>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.</p> <p>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.</p> <p>After receiving the redirected packet, the WAE does the following:</p> <ol style="list-style-type: none"> <li>1. Strips the GRE layer from the packet.</li> <li>2. Decides whether it should accept this redirected packet and process the request for the content as follows:           <ol style="list-style-type: none"> <li>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 TCP SYN packet of the client was trying to reach.</li> <li>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).</li> </ol> </li> </ol> <p>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.</p> |
| <b>Examples</b>           | Table 3-112 describes the fields shown in the <b>show statistics wccp gre</b> command display.  |

```
show statistics wccp
```

**Table 3-112 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 IP header of the redirected packet 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.<br><br><b>Note</b> 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 3-112 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 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. |

show statistics wccp

**Table 3-112 Field Descriptions for the show statistics wccp gre Command (continued)**

| Field                                       | Description  |
|---|--|
| 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. |
| 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 <b>wccp access-list</b> 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**
- (config) **wccp router-list**
- (config) **wccp shutdown**
- (config) **wccp tcp-promiscuous mask**

# 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  
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 3-113 describes the fields shown in the **show statistics windows-domain** command display.

**Table 3-113 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. |
| Number of authorization success responses | Number of authorization success responses. |

show statistics windows-domain

**Table 3-113 Field Descriptions for the show statistics windows-domain Command (continued)**

| Field                                  | Description                             |
|--|---|
| 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 statistics windows-print requests

To display Windows print acceleration statistics for a WAE, use the **show statistics windows-print requests** EXEC command.

**show statistics windows-print requests**

**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 statistics windows-print requests** command to view the Windows print traffic details.

**Examples** Table 3-114 describes the fields shown in the **show statistics windows-print requests** command display.

**Table 3-114 Field Descriptions for the show statistics windows-print requests Command**

| Field                                   | Description   |
|---|---|
| Statistics gathering period             | Number of hours, minutes, seconds, and milliseconds of the statistics gathering period.         |
| Documents spooled                       | Number of documents spooled.  |
| Pages spooled                           | Number of pages spooled.  |
| Total commands                          | Total number of print commands.   |
| Remote commands                         | Number of print commands that were not handled from the local cache.                            |
| ALL_COMMANDS                            | All the print commands combined.  |
| 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.                                   |
| Bind, ClosePrinter, EnumJobs, and so on | Statistics for individual print commands. Each has the same fields as the ALL_COMMANDS section. |

■ show statistics windows-print requests

---

**Related Commands** [\(config\) accelerator windows-print](#)

# show synq list

To display the connections for the SynQ module, use the **show synq list** EXEC command.

```
show synq list [l {begin regex [regex] | exclude regex [regex] | include regex [regex]}] [l {begin regex [regex] | exclude regex [regex] | include regex [regex]}]
```

## Syntax Description

|                      |   |
|----------------------|---|
|                      | (Optional) Output modifier.   |
| <b>begin regex</b>   | Begins with the line that matches the regular expression. You can enter multiple expressions. |
| <b>exclude regex</b> | Excludes lines that match the regular expression. You can enter multiple expressions.         |
| <b>include regex</b> | Includes lines that match the regular expression. You can enter multiple expressions.         |

## Defaults

No default behavior or values.

## Command Modes

EXEC

## Device Modes

application-accelerator

## Usage Guidelines

Use the **show synq list** command to list connections that are currently being tracked in the SynQ module.

## Examples

The following is sample output from the **show synq list** command:

```
WAE# show synq list
Src-IP:Src-Port      Dest-IP:Dest-Port      Timeout (msec)      Rexmit cnt
```

## Related Commands

[show statistics synq](#)

---

 show sysfs volumes

# 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.

---

**Defaults** No default behavior or values.

---

**Command Modes** EXEC

---

**Device Modes** application-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 3-115 describes the fields shown in the **show sysfs volumes** command display.

**Table 3-115 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  
central-manager

**Examples** Table 3-116 describes the fields shown in the **show tacacs** command display.

**Table 3-116 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 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.  |
| Password type   | Mechanism for password authentication. By default, the Password Authentication Protocol (PAP) is the mechanism for password authentication.   |

**show tacacs****Table 3-116 Field Descriptions for the show tacacs Command (continued)**

| Field  | Description  |
|--------|--|
| Server | Hostname or IP address of the TACACS+ server.              |
| Status | Indicates whether server is the primary or secondary host. |

**Related Commands**

[clear arp-cache](#)  
[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  
central-manager

**Examples** Table 3-117 describes the fields shown in the **show tcp** command display. This command displays the settings configured with the **tcp** global configuration command.

**Table 3-117 Field Descriptions for the show tcp Command**

| Field   | Description   |
|---|---|
| <b>TCP Configuration</b>                      |   |
| 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.                            |
| <b>TCP memory_limit</b>                       |   |
| Low water mark                                | Lower limit (in MB) of memory pressure mode, below which TCP enters into normal memory allocation mode.   |
| 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.   |

■ show tcp

---

**Related Commands**

[clear arp-cache](#)  
[show statistics tcp](#)  
[\(config\) tcp](#)

# show tech-support

To view information necessary for Cisco TAC to assist you, use the **show tech-support** EXEC command.

**show tech-support [page]**

|   |   |
|---|---|
| <b>Syntax Description</b>   | <b>page</b><br>(Optional) Displays command output page by page.   |
| <b>Defaults</b>   | No default behavior or values.  |
| <b>Command Modes</b>  | EXEC  |
| <b>Device Modes</b>   | application-accelerator<br>central-manager  |
| <b>Usage Guidelines</b>   | Use the <b>show tech-support</b> command to view system information necessary for Cisco TAC to assist you with a WAAS device. We recommend that you log the output to a disk file. (See the <a href="#">(config) logging console</a> command.)  |
| <b>Examples</b>   | The following is sample output from the <b>show tech-support</b> command:   |
|  <b>Note</b> | Because the <b>show tech-support</b> command output can be long, excerpts are shown in this example.  |
|   | <pre> 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 ... </pre> |

show tech-support

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 wccp
show alarms all
show statistics auto-discovery
show statistics filtering
show statistics ip
show statistics icmp
show statistics netstat
show statistics peer
show statistics tfo
show policy-engine status
show policy-engine application
show disks SMART-info
show disks SMART-info details
show disks failed-sectors
```

---

**show telnet**

## 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** No default behavior or values.

---

**Command Modes** EXEC

---

**Device Modes** application-accelerator  
central-manager

---

**Examples** The following is sample output from the **show telnet** command. It shows 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 tcp

To display global Traffic Flow Optimization (TFO) TCP buffer information for a WAE, use the **show tfo tcp** EXEC command.

**show tfo tcp**

**SyntaxDescription** This command has no arguments or keywords.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator

**Examples** The following is sample output from the **show tfo tcp** command. It displays TCP buffer information for the WAE.

```
WAE# show tfo tcp
Buffer Sizing Status:
Configured:
Adaptive buffer sizing : disabled
Maximum receive buffer size : 4096 KB
Maximum send buffer size : 4096 KB
Fix buffer sizes:
Optimized side receive buffer size : 1024 KB
Optimized side send buffer size : 1024 KB
Original side receive buffer size : 512 KB
Original side send buffer size : 512 KB
Default:
Fixed buffer sizes:
Optimized side receive buffer size : 32 KB
Optimized side send buffer size : 32 KB
Original side receive buffer size : 32 KB
Original side send buffer size : 32 KB
Adaptive buffer sizes :
Maximum receive buffer size : 4096 KB
Maximum send buffer size : 4096 KB
```

**Related Commands**

- [show statistics tfo](#)
- [show statistics auto-discovery](#)
- [show statistics connection closed](#)
- [show statistics filtering](#)
- [\(config\) tfo tcp adaptive-buffer-sizing](#)

■ **show transaction-logging**

# 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-logging** EXEC command to display information about the current configuration of transaction logging on a WAE. Transaction log file information is displayed for TFO transactions and video accelerator transactions.



**Note** For security reasons, passwords are never displayed in the output of the **show transaction-logging** EXEC command.

**Examples**

The following is sample output from the **show transaction-logging** command. It lists information about the current configuration of transaction logging on a WAE.

```
WAAE# show transaction-logging
Flow transaction log configuration:
-----
Flow Logging is disabled.
Flow Archive interval: every-day every 1 hour
Flow Maximum size of archive file: 2000000 KB

Exporting files to ftp servers is disabled.
File compression is disabled.
Export interval: every-day every 1 hour
Accelerator video windows-media transaction log configuration:
-----
Accelerator video windows-media logging is disabled.
Accelerator video windows-media archive interval: every-day every 1 hour
Accelerator video windows-media maximum size of archive file: 2000000 KB

Exporting files to ftp servers is disabled.
File compression is disabled.
Export interval: every-day every 1 hour
```

**Related Commands**

[clear arp-cache](#)  
[transaction-log](#)  
[\(config\) transaction-logs](#)

---

**show user**

## 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}**

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | <b>uid number</b> Displays user information based on the identification number of the user (0–65535).<br><b>username name</b> Displays user information based on the name of the user. |
|---------------------------|--|

---

**Command Default** No default behavior or values.

---

**Command Modes** EXEC

---

**Device Modes** application-accelerator  
central-manager

---

**Examples** Table 3-118 describes the fields shown in the **show user** command display.

**Table 3-118 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 arp-cache](#)  
[show users administrative](#)  
[\(config\) username](#)

# show users administrative

To display users with administrative privileges to the WAAS device, use the **show users administrative** EXEC command.

**show users administrative [history | locked-out | logged-in]**

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | <b>administrative</b> Displays a list of users defined on the device.<br><b>history</b> Displays a historical list of user log-ins.<br><b>locked-out</b> Displays a list of locked out users.<br><b>logged-in</b> Displays a list of users that are logged in. |
|---------------------------|--|

|                 |                                |
|-----------------|--------------------------------|
| <b>Defaults</b> | No default behavior or values. |
|-----------------|--------------------------------|

|                      |      |
|----------------------|------|
| <b>Command Modes</b> | EXEC |
|----------------------|------|

|                     |  |
|---------------------|--|
| <b>Device Modes</b> | application-accelerator<br>central-manager |
|---------------------|--|

|                 |   |
|-----------------|---|
| <b>Examples</b> | <a href="#">Table 3-119</a> describes the fields shown in the <b>show users administrative history</b> command display. |
|-----------------|---|

**Table 3-119 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. |

[Table 3-120](#) describes the fields shown in the **show users administrative logged-in** command display.

**Table 3-120 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. |

**show users administrative****Table 3-120 Field Descriptions for the show users administrative logged-in Command**

| Field           | Description   |
|-----------------|---|
| 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.            |

**Related Commands**

[clear arp-cache](#)  
[\(config\) 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]**

|                           |   |
|---------------------------|---|
| <b>Syntax Description</b> | <b>last</b> (Optional) Displays the version information for the last saved image.<br><b>pending</b> (Optional) Displays the version information for the pending upgraded image. |
|---------------------------|---|

|                 |                                |
|-----------------|--------------------------------|
| <b>Defaults</b> | No default behavior or values. |
|-----------------|--------------------------------|

|                      |      |
|----------------------|------|
| <b>Command Modes</b> | EXEC |
|----------------------|------|

|                     |  |
|---------------------|--|
| <b>Device Modes</b> | application-accelerator<br>central-manager |
|---------------------|--|

|                 |  |
|-----------------|--|
| <b>Examples</b> | Table 3-121 describes the fields shown in the <b>show version</b> command display. |
|-----------------|--|

**Table 3-121 Field Descriptions for the show version Command**

| Field   | Description   |
|---|---|
| Cisco Wide Area Application Services Software (WAAS)                                  | Software application, copyright, release, and build information.  |
| Copyright (c) year by Cisco Systems, Inc.   |   |
| Cisco Wide Area Application Services Software Release XXX (build bXXX month day year) |   |
| Version   | Version number of the software that is running on the device.     |
| Compiled hour:minute:second month day year by cnbuild                                 | Comple 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 virtual-blade**

## show virtual-blade

To display virtual blade information on your WAE device, use the **show virtual-blade** EXEC command.

```
show virtual-blade [[virtual-blade-number [blockio | interface int_name]] | vmstat]]
```

### Syntax Description

|                             |  |
|-----------------------------|--|
| <b>blockio</b>              | Displays the disk statistics.  |
| <b>interface int_name</b>   | Displays the network interface statistics for the specified interface. |
| <b>virtual-blade-number</b> | Specifies an individual virtual blade for which to view information.   |
| <b>vmstat</b>               | Displays the virtual blade process statistics for all virtual blades.  |

### Command Default

No default behavior or values.

### Command Modes

EXEC

### Device Modes

application-accelerator

### Examples

The following is sample output from the **show virtual-blade** command. It displays general virtual blade information.

```
WAE# show virtual-blade
Virtual-blade resources:
  VB Memory: 1000MiB configured, 3072MiB available.
  VB Disk space: 40GiB configured, 180GiB available.
  VB Image space /local1/vbs: 128MiB used, 125644MiB available
  CPU(s) assigned: 2
Virtual-blade(s) state:
  virtual-blade 1 is running
```

The following is sample output from the **show virtual-blade** command. It displays information for a specific virtual blade (virtual blade 1 in the example).

```
WAE# show virtual-blade 1
virtual-blade 1
config:
  description Windows 2008 Server
  device cpu qemu64
  device nic rtl8139
  device disk IDE
  device keyboard us
  memory 1000
  disk 40
  no boot fd-image
  boot cd-image /local1/vbs/WoW_1.0.2.iso
  boot from cd-rom
  interface 1 bridge GigabitEthernet 1/0 mac-address 00:16:3E:97:6F:84
  no vnc
  autostart
state:
  running
```

```

serial console session inactive
vnc server disabled
current cd /local1/vbs/WoW_1.0.2.iso
current floppy [not inserted]

```

Table 3-122 describes the fields shown in the general **show virtual-blade** display.

**Table 3-122 Field Descriptions for the General show virtual-blade Command**

| Field               | Description   |
|---------------------|---|
| VB Memory           | The amount of WAAS system memory assigned to all virtual blades, and the amount of memory remaining.  |
| VB Disk Space       | The amount of WAAS system disk space assigned to all virtual blades, and the amount of disk space remaining.  |
| VB Image space      | The location and amount of virtual blade image space assigned to the virtual blade, and the amount of disk space remaining.                                   |
| CPU(s) Assigned     | CPU numbers of the CPUs assigned for use by virtual blades. (For example, if 2 is shown, that means that CPU number 2 is assigned for use by virtual blades.) |
| Virtual Blade State | The state of each defined virtual blade (running or stopped).   |

Table 3-123 describes the fields shown in the **show virtual-blade** command display for a specific virtual blade.

**Table 3-123 Field Descriptions for the Specific show virtual-blade Command**

| Field            | Description   |
|------------------|---|
| virtual blade    | Virtual blade number.   |
| description      | Description of the virtual blade.   |
| device           | Device emulation parameters used by the virtual blade.  |
| memory           | Memory allocated to the virtual blade, in MB.   |
| disk             | Disk space allocated to the virtual blade, in GB.   |
| no boot fd-image | Floppy disk image from which the virtual blade is configured to boot. In this case, it shows that the virtual blade is not configured to boot from the floppy disk image. |
| boot cd-image    | CD-ROM image from which the virtual blade is configured to boot. Appears only if boot cd-image is configured.   |
| boot from        | Boot source location.   |
| interface        | Interface bridging configuration.   |
| no vnc           | Shows that the VNC server is disabled. (This line does not appear when the VNC server is enabled.)  |
| autostart        | Shows that the virtual blade is configured to start automatically.  |
| state            | State of the virtual blade (running or stopped) and other runtime information.  |

#### Related Commands

[\(config\) virtual-blade](#)

■ show virtual-blade

```
(config-vb) autostart
(config-vb) boot
(config-vb) description
(config-vb) device
(config-vb) disk
(config-vb) interface
(config-vb) memory
(config-vb) vnc
```

## 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 status
```

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | <b>wide-area-engines</b> Displays which WAEs are seen by which routers.<br><b>flows</b> Displays WCCP packet flows.<br><b>tcp-promiscuous</b> Displays TCP-PROMISCUOUS caching service packet flows.<br><b>summary</b> (Optional) Displays summarized information about TCP-PROMISCUOUS caching service packet flows.<br><b>gre</b> Displays WCCP generic routing encapsulation packet-related information.<br><b>masks</b> Displays WCCP mask assignments for a given service.<br><b>routers</b> Displays routers seen and not seen by this WAE.<br><b>services</b> Displays WCCP services configured.<br><b>detail</b> (Optional) Displays details of services.<br><b>status</b> Displays version of WCCP that is enabled and running. |
|---------------------------|--|

|                 |                                |
|-----------------|--------------------------------|
| <b>Defaults</b> | No default behavior or values. |
|-----------------|--------------------------------|

|                      |      |
|----------------------|------|
| <b>Command Modes</b> | EXEC |
|----------------------|------|

|                     |                         |
|---------------------|-------------------------|
| <b>Device Modes</b> | application-accelerator |
|---------------------|-------------------------|

|                 |   |
|-----------------|---|
| <b>Examples</b> | Table 3-124 describes the fields shown in the <b>show wccp gre</b> command display. |
|-----------------|---|

show wccp

**Table 3-124 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 IP header of the redirected packet 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.<br><br><b>Note</b> 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 3-124 Field Descriptions for the show 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.  |

show wccp

**Table 3-124 Field Descriptions for the show 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 the IP address of a client, the WAE can receive packets with the client IP (which is different from the IP address of the WAE) 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 <b>wccp access-list</b> 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.  |

The following is sample output from the **show wccp services** command:

```
WAE# show wccp services
```

```
Services configured on this File Engine
    TCP Promiscuous 61
    TCP Promiscuous 62
```

The following is sample (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 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 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 is sample 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
```

■ **show wccp**

```
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 is sample output from the **show wccp status** command:

```
WAE# show wccp status
WCCP version 2 is enabled and currently active
```

---

#### Related Commands

- [\*\*\(config\) wccp access-list\*\*](#)
- [\*\*\(config\) wccp flow-redirect\*\*](#)
- [\*\*\(config\) wccp router-list\*\*](#)
- [\*\*\(config\) wccp shutdown\*\*](#)
- [\*\*\(config\) wccp tcp-promiscuous mask\*\*](#)
- [\*\*\(config\) 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.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator  
central-manager

**Examples** Table 3-125 describes the fields shown in the **show windows-domain** command display.

**Table 3-125 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  |   |

■ **show windows-domain**

**Table 3-125 Field Descriptions for the show windows-domain Command (continued)**

| Field             | Description  |
|-------------------|--|
| 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]**

|                           |                 |   |
|---------------------------|-----------------|---|
| <b>Syntax Description</b> | <b>poweroff</b> | (Optional) Turns off the power after closing all applications and operating system. |
|---------------------------|-----------------|---|

|                 |                                |
|-----------------|--------------------------------|
| <b>Defaults</b> | No default behavior or values. |
|-----------------|--------------------------------|

|                      |      |
|----------------------|------|
| <b>Command Modes</b> | EXEC |
|----------------------|------|

|                     |  |
|---------------------|--|
| <b>Device Modes</b> | application-accelerator<br>central-manager |
|---------------------|--|

|                         |   |
|-------------------------|---|
| <b>Usage Guidelines</b> | 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 3-126 describes the shutdown-only operation and the shutdown poweroff operation for a WAAS device.

**Table 3-126 Description of the shutdown Command Operations**

| Activity                                      | Process   |
|---|---|
| User performs a shutdown operation on the WAE | Shutdown poweroff<br>WAE# <b>shutdown poweroff</b>  |
| 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 how to close all applications and stop all system activities using the **shutdown** command:

```
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 how to close all applications, stop all system activities, and then turn off power to the WAAS device using the **shutdown poweroff** command:

```
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.

```
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 mibvar] [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]]]}}
```

**snmp trigger delete mibvar**

| Syntax Description     |   |
|------------------------|---|
| <b>create mibvar</b>   | Configures a threshold for a MIB object. Specifies the name of the MIB object that you want to monitor or the MIB object for which you want to remove a monitoring threshold. |
| <b>wildcard</b>        | (Optional) Treats the specified MIB variable name as having a wildcard.   |
| <b>wait-time</b>       | (Optional) Number of seconds, 60–600, to wait between trigger samples.  |
| <b>absent</b>          | (Optional) Applies the absent existence test.   |
| <b>LINE</b>            | (Optional) Description of the threshold being created.  |
| <b>mibvar1 mibvar1</b> | (Optional) Adds a MIB object to the notification.   |
| <b>mibvar2 mibvar2</b> | (Optional) Adds a MIB object to the notification.   |
| <b>mibvar3 mibvar3</b> | (Optional) Adds a MIB object to the notification.   |
| <b>equal</b>           | Applies the equality threshold test.  |
| <b>absolute value</b>  | (Optional) Specifies an absolute value sample type.   |

|                     |  |
|---------------------|--|
| <b>delta value</b>  | Specifies a delta sample type.           |
| <b>falling</b>      | Applies the falling threshold test.      |
| <b>greater-than</b> | Applies the greater-than threshold test. |
| <b>less-than</b>    | Applies the less-than threshold test.    |
| <b>on-change</b>    | Applies the changed existence test.      |
| <b>present</b>      | Applies the present test.                |
| <b>rising</b>       | Applies the rising threshold test.       |
| <b>delete</b>       | Removes a threshold for a MIB object.    |

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator  
central-manager

**Usage Guidelines** Using the **snmp trigger** EXEC 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.

**snmp trigger**

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-server 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**

- [show snmp](#)
- [\(config\) 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](#)
- [\(config\) snmp-server notify inform](#)

```
(config) snmp-server user  
(config) snmp-server view  
write
```

## 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*

|   |                |  |
|---|----------------|--|
| <b>Syntax Description</b>   | <i>options</i> | Options to use with the <b>ssh EXEC</b> command. For more information about the possible options, see RFC 4254 at <a href="http://www.rfc-archive.org/getrfc.php?rfc=4254">http://www.rfc-archive.org/getrfc.php?rfc=4254</a> .  |
| <b>Defaults</b>   |                | By default, the Secure Shell (SSH) feature is disabled on a WAAS device.   |
| <b>Command Modes</b>  |                | EXEC   |
| <b>Device Modes</b>   |                | application-accelerator<br>central-manager   |
| <b>Usage Guidelines</b>   |                | 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. |
|  <b>Note</b> |                | The Telnet daemon can still be used with the WAAS device. SSH does not replace Telnet.   |
| <b>Related Commands</b>   |                | (config) <b>sshd</b><br>(config) <b>ssh-key-generate</b>   |

# tcpdump

To dump network traffic, use the **tcpdump** EXEC command.

**tcpdump [LINE]**

|                           |             |   |
|---------------------------|-------------|---|
| <b>Syntax Description</b> | <b>LINE</b> | (Optional) Dump options. For more information see the “Usage Guidelines” section. |
|---------------------------|-------------|---|

|                 |                                |
|-----------------|--------------------------------|
| <b>Defaults</b> | No default behavior or values. |
|-----------------|--------------------------------|

|                      |      |
|----------------------|------|
| <b>Command Modes</b> | EXEC |
|----------------------|------|

|                     |  |
|---------------------|--|
| <b>Device Modes</b> | application-accelerator<br>central-manager |
|---------------------|--|

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

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).

Use the **-h** option to view the options available, as shown in the following example:

```
WAE# tcpdump -h
tcpdump version 3.8.1 (jlemon)
libpcap version 0.8
Usage: tcpdump [-aAdDef1LnNOpqRStuUvxX] [-c count] [-C file_size]
               [-E algo:secret] [-F file] [-i interface] [-r file]
               [-s snaplen] [-T type] [-w file] [-y datalinktype]
               [ expression ]
```

|                 |  |
|-----------------|--|
| <b>Examples</b> | The following example shows how to start a network traffic dump to a file named <i>tcpdump.txt</i> : |
|-----------------|--|

```
WAE# tcpdump -w tcpdump.txt
```

|                         |   |
|-------------------------|---|
| <b>Related Commands</b> | <a href="#">less</a><br><a href="#">ping</a><br><a href="#">tethereal</a> |
|-------------------------|---|

■ **tcpdump**

**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**

|                   |  |
|-------------------|--|
| <i>hostname</i>   | Hostname of the network device.                              |
| <i>ip-address</i> | IP address of the network device.                            |
| <i>portnum</i>    | (Optional) Port number (1–65535). Default port number is 23. |

---

**Defaults**

The default port number is 23.

**Command Modes**

EXEC

**Device Modes**

application-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 how to log in to a WAAS device using the Telnet client in several ways:

```
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]}
```

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | <b>length</b> <i>length</i> Sets the length of the display on the terminal (0–512). Setting the length to 0 means there is no pausing.<br><b>monitor</b> Copies the debug output to the current terminal.<br><b>disable</b> (Optional) Disables monitoring at this specified terminal. |
|---------------------------|--|

|                 |                          |
|-----------------|--------------------------|
| <b>Defaults</b> | The default is 24 lines. |
|-----------------|--------------------------|

|                      |      |
|----------------------|------|
| <b>Command Modes</b> | EXEC |
|----------------------|------|

|                     |  |
|---------------------|--|
| <b>Device Modes</b> | application-accelerator<br>central-manager |
|---------------------|--|

|                         |  |
|-------------------------|--|
| <b>Usage Guidelines</b> | When 0 is entered as the <i>length</i> parameter, the output to the screen does not pause. For all nonzero values of <i>length</i> , the -More- prompt is displayed when the number of output lines matches the specified <i>length</i> number. The -More- prompt is considered a line of output. To view the next screen, press the <b>Spacebar</b> . To view one line at a time, press the <b>Enter</b> 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.

|                 |  |
|-----------------|--|
| <b>Examples</b> | The following example shows how to set the number of lines to display to 20: |
|-----------------|--|

```
WAE# terminal length 20
```

The following example shows how to configure the terminal for no pausing:

```
WAE# terminal length 0
```

|                         |                           |
|-------------------------|---------------------------|
| <b>Related Commands</b> | All <b>show</b> commands. |
|-------------------------|---------------------------|

# test

To perform diagnostic tests and display the results, use the **test** EXEC command.

```
test self-diagnostic [system | basic | connectivity | interfaces | tfo | wccp | inline | wafs ] | all
```

| Syntax Description | <b>self-diagnostic</b> | Performs self-diagnostics tests.   |
|--------------------|------------------------|--|
|                    | <b>system</b>          | (Optional) Checks the device status, presence of core files, and alarms.   |
|                    | <b>basic</b>           | (Optional) Checks the device network configuration.  |
|                    | <b>connectivity</b>    | (Optional) Checks if the external hosts required for device operation are reachable by sending ICMP ping packets.  |
|                    | <b>interfaces</b>      | (Optional) Checks the operation of physical interfaces, including ports on the Cisco WAE Inline Network Adapter.   |
|                    | <b>tfo</b>             | (Optional) Checks the traffic optimization configuration settings and operation. (Applies only to application accelerator devices.)  |
|                    | <b>wccp</b>            | (Optional) Checks the WCCP configuration settings and operation. (Applies only to application accelerator devices.)  |
|                    | <b>inline</b>          | (Optional) Checks the inline group configuration settings and operation. (Applies only to application accelerator devices that have the Cisco WAE Inline Network Adapter installed.) |
|                    | <b>wafs</b>            | (Optional) Checks the WAFS configuration settings and operation. (Applies only to application accelerator devices.)  |
|                    | <b>all</b>             | (Optional) Runs all of the diagnostic tests.   |

**Defaults** No default behavior or values.

**Command Modes** EXEC mode

**Device Modes** application-accelerator  
central-manager

**Usage Guidelines** If you use the **test self-diagnostic** command with the **all** option, all applicable tests are performed. You can specify one or more test options to perform just those tests.

The last diagnostic test report is stored on the device in the following file: /local1/diagnostic\_report.txt.

**Examples** The following example shows how to perform the basic, connectivity, interfaces, and WCCP tests:

```
WAE# test self-diagnostic basic connectivity interfaces wccp
```

Table 3-127 describes the error messages that can be returned by the **test self-diagnostics** command.

**Table 3-127 Error Codes Returned by the test self-diagnostics Command**

| Test         | Error Code       | Description  |
|--------------|------------------|--|
| system       | HAS_COREDUMP     | Core files are present.  |
|              | HAS_ALARM        | Critical or major alarms are pending.  |
| basic        | NO_PRIM_IFACE    | The primary interface is not configured.   |
|              | NO_PRIM_ADDR     | The primary interface has no IP address configured.  |
|              | NO_HOSTNAME      | The hostname is not configured.  |
|              | NO_NAMESERVER    | The name servers are not configured.   |
|              | NO_DOMAIN        | The domain name is not configured.   |
|              | NO_DEFAULT_GW    | The default gateway is not configured.   |
|              | NO_CM_ADDR       | The WAAS Central Manager IP address is not configured.   |
|              | NO_NTP_CFG       | The NTP server is not configured.  |
| connectivity | UNREACHABLE      | The default gateway, name servers, NTP servers, authentication servers (RADIUS, TACACS, or Windows domain), or WAAS Central Manager are unreachable. |
|              | UNRESOLVABLE     | The fully qualified domain name of the device cannot be resolved.  |
|              | WINS_UNAVAILABLE | The WINS server is unreachable or not operational and cannot resolve the device netbios name.  |
| interfaces   | IFACE_DOWN       | The interface is in shutdown mode. If all interfaces are shut down, the test will fail.  |
|              | IFACE_BW         | The interface is configured or negotiated to use 10-MB speed instead of a faster speed.  |
|              | IFACE_HD         | The interface is configured or negotiated to use half duplex instead of full duplex.   |
|              | IFACE_ERRORS     | The interface has packet errors on more than 1 percent of received or sent packets.  |
|              | IFACE_COLLISIONS | The interface has packet collisions on more than 1 percent of sent packets.  |
| tfo          | TFO_DISABLED     | TFO is disabled.   |
|              | TFO_NO_DRE       | DRE is disabled.   |
|              | TFO_NO_LZ        | Compression is disabled.   |
|              | TFO_NOAOACCL     | An application accelerator in the policy engine is not enabled to accelerate traffic.  |
|              | PE_OTHER         | Unclassified traffic is configured to pass through.  |
|              | TFO_NOPT         | Traffic that is configured to be optimized is being passed through.  |
| wccp         | NO_RTRCFG        | WCCP is enabled but TCP promiscuous mode is not configured.  |
|              | NO_RTRLIST       | The router list specified in WCCP configuration is not configured.   |
|              | UNREACHABLE      | Configured WCCP routers are unreachable or other WAEs in the WCCP farm are unreachable.  |
|              | NO_WCCP_RTRS     | The WAE and WCCP routers cannot communicate with each other.   |
|              | NO_INTERCEPT     | The WAE is not receiving intercepted traffic.  |

**Table 3-127 Error Codes Returned by the test self-diagnostics Command (continued)**

| <b>Test</b> | <b>Error Code</b> | <b>Description</b>   |
|-------------|-------------------|--|
| inline      | INLINE_NO_INT     | Traffic interception is not configured on the inlineGroup interface.                         |
|             | INLINE_SHUTDOWN   | The inlineGroup interface is shut down.  |
|             | INLINE_BYPASS     | The inlineGroup interface is in bypass mode.   |
|             | INLINE_INTRCPT    | The inlineGroup interface is not intercepting traffic.                                       |
| wafs        | NO_CONNECTIVITY   | The edge and core WAEs do not have connectivity defined or the peer devices are unreachable. |
|             | UNREACHABLE       | The WAFS connectivity peers are unreachable.   |
|             | NO_WAFS_CONN      | The WAFS transport is not established.   |

# tethereal

To analyze network traffic from the command line, use the **tethereal** EXEC command.

**tethereal [LINE]**

|                           |  |  |
|---------------------------|--|--|
| <b>Syntax Description</b> | <b>LINE</b>  | (Optional) Options. For more information see the “Usage Guidelines” section. |
| <b>Defaults</b>           | No default behavior values.  |  |
| <b>Command Modes</b>      | EXEC   |  |
| <b>Device Modes</b>       | application-accelerator<br>central-manager   |  |
| <b>Usage Guidelines</b>   | Tethereal 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, Tethereal also provides facilities for decoding packets.  |  |
| <b>Examples</b>           | The following example shows how to display the options available with the WAAS <b>tethereal</b> command:   |  |
|                           | <pre>WAE# tethereal -h This is GNU tethereal 0.10.6 (C) 1998-2004 Gerald Combs &lt;gerald@ethereal.com&gt; Compiled with GLib 1.2.9, with libpcap 0.6, with libz 1.1.3, without libpcre, 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.  tethereal [ -vh ] [ -DlNpqSVx ] [ -a &lt;capture autostop condition&gt; ] ... [ -b &lt;number of ring buffer files&gt;[:&lt;duration&gt;] ] [ -c &lt;count&gt; ] [ -d &lt;layer_type&gt;==&lt;selector&gt;,&lt;decode_as_protocol&gt; ] ... [ -f &lt;capture filter&gt; ] [ -F &lt;output file type&gt; ] [ -i &lt;interface&gt; ] [ -N &lt;resolving&gt; ] [ -o &lt;preference setting&gt; ] ... [ -r &lt;infile&gt; ] [ -R &lt;read filter&gt; ] [ -s &lt;snaplen&gt; ] [ -t &lt;time stamp format&gt; ] [ -T pdml ps psml text ] [ -w &lt;savefile&gt; ] [ -y &lt;link type&gt; ] [ -z &lt;statistics string&gt; ]  Valid file type arguments to the "-F" flag: libpcap - libpcap (tcpdump, Ethereal, etc.) rh6_llibpcap - 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</pre> |  |

```
netmon1 - Microsoft Network Monitor 1.x
netmon2 - Microsoft Network Monitor 2.x
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 - Accelgent 5Views capture
niobserverv9 - Network Instruments Observer version 9
default is libpcap
```

---

Related Commands[tcpdump](#)

**traceroute**

# traceroute

To trace the route between a WAAS device to a remote host, use the **traceroute** EXEC command.

**traceroute {hostname | ip-address}**

|                           |   |                 |                      |                   |                            |
|---------------------------|---|-----------------|----------------------|-------------------|----------------------------|
| <b>Syntax Description</b> | <table border="0"> <tr> <td><i>hostname</i></td><td>Name of remote host.</td></tr> <tr> <td><i>ip-address</i></td><td>IP address of remote host.</td></tr> </table> | <i>hostname</i> | Name of remote host. | <i>ip-address</i> | IP address of remote host. |
| <i>hostname</i>           | Name of remote host.  |                 |                      |                   |                            |
| <i>ip-address</i>         | IP address of remote host.  |                 |                      |                   |                            |

**Defaults** No default behavior values.

**Command Modes** EXEC

**Device Modes** application-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 shows how to trace 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 force {archive | export} {flow | accelerator video windows-media}
```

| Syntax Description      | <b>archive</b> Forces the archiving of the transaction log file.<br><b>export</b> Forces the archived transaction log files to be exported.<br><b>flow</b> Forces the archiving or exporting of the Traffic Flow Optimization (TFO) transaction log file.<br><b>accelerator video windows-media</b> Forces the archiving or exporting of the video accelerator transaction log file. |
|-------------------------|--|
| <b>Defaults</b>         | No default behavior values.  |
| <b>Command Modes</b>    | EXEC   |
| <b>Device Modes</b>     | application-accelerator  |
| <b>Examples</b>         | <p>The following example shows how to force the archiving of the TFO transaction log file on the WAE:</p> <pre>WAE# <b>transaction-log force archive flow</b></pre> <p>The following example shows how to force the exporting of the video transaction file on the WAE:</p> <pre>WAE# <b>transaction-log force export accelerator video windows-media</b></pre>                      |
| <b>Related Commands</b> | <a href="#">(config) transaction-logs</a><br><a href="#">show transaction-logging</a>  |

**type**

## type

To display a file, use the **type** EXEC command.

**type** *filename*

|                           |   |               |
|---------------------------|---|---------------|
| <b>Syntax Description</b> | <i>filename</i>   | Name of file. |
| <b>Defaults</b>           | No default behavior or values.  |               |
| <b>Command Modes</b>      | EXEC  |               |
| <b>Device Modes</b>       | application-accelerator<br>central-manager  |               |
| <b>Usage Guidelines</b>   | Use the <b>type</b> command to display the contents of a file within any file directory on a WAAS device. The <b>type</b> command may be used to monitor features such as transaction logging or system logging (syslog). |               |
| <b>Examples</b>           | The following example shows how to display the contents of the <i>syslog.txt</i> file:<br><br>WAE# <b>type /local1/syslog.txt</b>   |               |
| <b>Related Commands</b>   | <a href="#">cpfile</a><br><a href="#">dir</a><br><a href="#">lls</a><br><a href="#">ls</a><br><a href="#">pwd</a><br><a href="#">rename</a>   |               |

# 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** EXEC command.

**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).   |
| <b>follow</b>              | (Optional) Displays the end of the file continuously as new lines are added to the file.                                       |
| <b> </b>                   | (Optional) Displays contents of the file according to the <b>begin</b> , <b>exclude</b> , and <b>include</b> output modifiers. |
| <b>begin</b> <i>LINE</i>   | Identifies the line at which to begin file display. Specifies a regular expression to match in the file.                       |
| <b>exclude</b> <i>LINE</i> | Indicates lines that are to be excluded from the file display. Specifies a regular expression to match in the file.            |
| <b>include</b> <i>LINE</i> | Indicates lines that are to be included in the file display. Specifies a regular expression to match in the file.              |

**Defaults** The last ten lines are shown.

**Command Modes** EXEC

**Device Modes** application-accelerator  
central-manager

**Usage Guidelines** The **type-tail** 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 shows how to look 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
```

type-tail

```

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
r-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-11 java: %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] Destinatio
n IP [port] = 32.60.43.2 [53775] }returned error: -1 errno 9

```

The following example shows how to follow the *syslog.txt* file as it grows:

```
WAE# type-tail /local1/syslog.txt follow
```

# virtual-blade

To change the virtual blade CD-ROM, save or delete the memory state, open or clear a Telnet session, or start and stop a virtual blade, use the **virtual-blade** EXEC command.

```
virtual-blade {bladenum} {cd {cd-rom | disk pathname | eject} | kill-save-state | save | session [clear] | start [delay] | stop [timeout]}
```

|                             |  |
|-----------------------------|--|
| <b>Syntax Description</b>   |  |
| <i>bladenum</i>             | Number of the virtual blade. Valid values are 1 through 4.   |
| <b>cd</b>                   | Changes the virtual blade CD-ROM.  |
| <b>cd-rom</b>               | Uses the WAE CD-ROM drive.   |
| <b>disk <i>pathname</i></b> | Specifies a CD-ROM image file located on the WAE hard drive. This file is located in the <i>/local1/vbs</i> directory. |
| <b>eject</b>                | Ejects the disk from the WAE CD-ROM drive.   |
| <b>kill-save-state</b>      | Deletes the saved virtual blade memory state.  |
| <b>save</b>                 | Saves the current memory state of the virtual blade.   |
| <b>session</b>              | Opens a telnet session to the remote host/port.  |
| <b>clear</b>                | (Optional) Cancels the telnet session to the remote host/port.   |
| <b>start</b>                | Starts the specified virtual blade.  |
| <i>delay</i>                | Specifies the startup delay for the virtual blade being started. Valid values are 1 through 60 seconds.                |
| <b>stop</b>                 | Stops the specified virtual blade.   |
| <i>timeout</i>              | Specifies the shutdown timeout delay for the virtual blade being stopped. Valid values are 0 through 900 seconds.      |

|                 |                                |
|-----------------|--------------------------------|
| <b>Defaults</b> | No default behavior or values. |
|-----------------|--------------------------------|

|                      |      |
|----------------------|------|
| <b>Command Modes</b> | EXEC |
|----------------------|------|

|                     |                         |
|---------------------|-------------------------|
| <b>Device Modes</b> | application-accelerator |
|---------------------|-------------------------|

|                         |   |
|-------------------------|---|
| <b>Usage Guidelines</b> | The <b>virtual-blade</b> EXEC command is used to execute general operations on a virtual blade. The <b>virtual-blade <i>n</i> cd</b> command changes the source of the virtual blade operating system image or ejects the CD. The <b>virtual-blade <i>n</i> save</b> command saves a snapshot of the current virtual blade memory state and saves it to <i>/local1/vbs</i> . The <b>virtual-blade <i>n</i> kill-save-state</b> command deletes the memory snapshot. The <b>virtual-blade <i>n</i> start</b> and <b>virtual-blade <i>n</i> stop</b> commands allow you to activate and deactivate the virtual blade. Each command has an optional delay. |
|-------------------------|---|

|                 |   |
|-----------------|---|
| <b>Examples</b> | The following example shows how to start virtual blade 1 immediately: |
|-----------------|---|

**virtual-blade**

```
WAE# virtual-blade 1 start
```

The following example shows how to stop virtual blade 1 after a 3 minute timeout period:

```
WAE# virtual-blade 1 stop 180
```

The following example shows how to eject the CD in the WAE CD-ROM drive:

```
WAE# virtual-blade 1 cd eject
```

---

**Related Commands**

[\(config\) virtual-blade](#)  
[\(config-vb\) boot](#)  
[\(config-vb\) device](#)  
[\(config-vb\) disk](#)  
[\(config-vb\) interface](#)  
[\(config-vb\) memory](#)

# 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

|   |  |
|---|--|
| <b>backup-config</b><br><i>filename</i>             | Copies current WAFS-related configuration information to a file. 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.                    |
| <b>restore-config</b><br><i>filename</i>            | Loads saved WAFS-related configuration information from a file. 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. |
| <b>sysreport</b>                                    | Deprecated; use <b>copy sysreport</b> .  |
| <b>date-range</b> <i>from_date to_date filename</i> | (Optional) Displays the range of time that the system report is to cover. Specifies start date, end date, and 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 shows how to create a backup file of the WAFS configuration information:

```
WAE# wafs ?
```

**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 shows how to restore 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  
central-manager

**Usage Guidelines** Use the **whoami** command to display the username of the current user.

**Examples** The following example shows how to display 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 | tdbbackup | tdbdump | testparm | wbinfo}
```

| Syntax Description |   |
|--------------------|---|
| <b>diagnostics</b> | Enables selection of Windows domain diagnostic utilities.                                   |
| <b>findsmb</b>     | Displays the utility for troubleshooting NetBIOS name resolution and browsing.              |
| <b>getent</b>      | Displays the utility to get unified list of both local and PDC users and groups.            |
| <b>net</b>         | Displays the utility for administration of remote CIFS servers.                             |
| <b>nmblookup</b>   | Displays the utility for troubleshooting NetBIOS name resolution and browsing.              |
| <b>smbclient</b>   | Displays the utility for troubleshooting the Windows environment and integration.           |
| <b>smbstatus</b>   | Displays the utility for inspecting the Samba server status, connected clients, and so on.  |
| <b>smbtree</b>     | Displays the utility for inspecting the Windows network neighborhood structure and content. |
| <b>tdbbackup</b>   | Displays the utility for backing up, verifying and restoring Samba database files.          |
| <b>tdbdump</b>     | Displays the utility for inspecting the Samba database files.                               |
| <b>testparm</b>    | Displays the utility to validate <i>smb.conf</i> file correctness.                          |
| <b>wbinfo</b>      | Displays the utility for Winbind and domain integration troubleshooting.                    |

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Device Modes** application-accelerator  
central-manager

**Usage Guidelines** Use the **windows-domain** command to activate the selected Windows domain diagnostic utility.

**Examples** The following example shows how to display 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 how to display 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 how to display 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 how to display 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 how to use 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 |  |
|--------------------|--|
| <b>erase</b>       | (Optional) Erases startup configuration from NVRAM.  |
| <b>memory</b>      | (Optional) Writes the configuration to NVRAM. This is the default location for saving startup information. |
| <b>mib-data</b>    | (Optional) Saves MIB persistent configuration data to disk.  |
| <b>terminal</b>    | (Optional) Writes the configuration to a terminal session.   |

**Defaults** The configuration is written to NVRAM by default.

**Command Modes** EXEC

**Device Modes** application-accelerator  
central-manager

**Usage Guidelines** Use the **write** 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 shows how to save the current startup configuration to memory:

```
WAE# write memory
```

**Related Commands** [copy running-config](#)  
[copy startup-config](#)  
[show running-config](#)  
[show startup-config](#)

# Global 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** global configuration command. To unconfigure AAA, use the **no** form of this command.

```
aaa accounting commands {0 | 15} default {start-stop | stop-only | wait-start} tacacs
```

```
no aaa accounting commands {0 | 15} default {start-stop | stop-only | wait-start} tacacs
```

```
aaa accounting exec default {start-stop | stop-only | wait-start} tacacs
```

```
no aaa accounting exec default {start-stop | stop-only | wait-start} tacacs
```

```
aaa accounting system default {start-stop | stop-only} tacacs
```

```
no aaa accounting system default {start-stop | stop-only} tacacs
```

|                           |   |
|---------------------------|---|
| <b>Syntax Description</b> |   |
| <b>commands</b>           | Configures accounting for all commands at the specified privilege level.  |
| <b>0</b>                  | Specifies user privilege level for a normal user.   |
| <b>15</b>                 | Specifies user privilege level for an administrative user.  |
| <b>default</b>            | Sets AAA accounting to use the default accounting list.   |
| <b>start-stop</b>         | 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.                                   |
| <b>stop-only</b>          | Sends a stop accounting notice at the end of the process requested by the user.   |
| <b>wait-start</b>         | 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.<br>A stop accounting notice is also sent but does not need acknowledgement. |
| <b>tacacs</b>             | Enables use of TACACS+ for accounting.  |
| <b>exec</b>               | 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.   |
| <b>system</b>             | Enables accounting for all system-level events not associated with users, such as reloads.  |

|                 |  |
|-----------------|--|
| <b>Defaults</b> | AAA accounting is disabled by default. |
|-----------------|--|

|                      |                      |
|----------------------|----------------------|
| <b>Command Modes</b> | global configuration |
|----------------------|----------------------|

(config) aaa accounting

---

|                     |  |
|---------------------|--|
| <b>Device Modes</b> | application-accelerator<br>central-manager |
|---------------------|--|

---

|                 |  |
|-----------------|--|
| <b>Examples</b> | The following example shows how to configure TACACS+ on the WAAS device, specify 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 request that the 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 example shows 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 example shows 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 example shows 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, CESM_PARSER, PARSER_ALL, CESM_350232,  
"CLI_LOG %s: %s \n", __FUNCTION__, pd->command_line);
```

---

**Related Commands**

[show aaa accounting](#)

(config) accelerator cifs

## (config) accelerator cifs

To enable the CIFS application accelerator, use the **accelerator cifs** global configuration command. To disable the CIFS application accelerator, use the **no** form of this command.

```
accelerator cifs {[double-byte-unicode] | enable | dynamic-share share | clear cache |
    cache server-rename oldname newname | exception {coredump | debug | no-coredump}}}

no accelerator cifs {[double-byte-unicode] | enable | dynamic-share share | clear cache |
    cache server-rename oldname newname | exception {coredump | debug | no-coredump}}
```

| Syntax Description                                   |  |
|--|--|
| <b>double-byte-unicode</b>                           | Enables support for double-byte Unicode languages for Windows 98 clients.                          |
| <b>enable</b>  | Enables the CIFS traffic accelerator.  |
| <b>dynamic-share share</b>                           | Enables support for CIFS dynamic shares and specifies a path in the format:<br>cifs://server/share |
| <b>clear cache</b>                                   | Clears the CIFS application accelerator cache and restarts the accelerator.                        |
| <b>cache server-rename</b><br><i>oldname newname</i> | Renames a CIFS file server for the cached data.  |
| <b>exception</b>                                     | (Optional) Configures the action to be taken if an exception occurs.                               |
| <b>coredump</b>                                      | Writes a core file (default).  |
| <b>debug</b>   | Hangs the system until it is explicitly restarted.   |
| <b>no-coredump</b>                                   | Restarts the accelerator and does not write a core file.   |

### Defaults

The CIFS accelerator is enabled by default and will start automatically if the Enterprise license is installed. The default exception action is coredump.

### Command Modes

global configuration

### Device Modes

application-accelerator

### Usage Guidelines

Use the **accelerator cifs enable** command to enable the acceleration of CIFS traffic with the transparent CIFS accelerator (not the legacy mode of acceleration).

The CIFS application accelerator requires that the WINS server be configured. Use the **windows-domain wins-server** global configuration command to configure the WINS server.

To configure prepositioning directives, use the **accelerator cifs preposition** global configuration command.

Use the **accelerator cifs dynamic-share** command to define a dynamic share, which allows multiple users to access the same share but then be automatically mapped to a different directory based on the user's credentials. Defining a dynamic share allows each user to see a different view of the share, and allows the operation of Access Based Enumeration, if configured on Windows Server.

Use the **accelerator cifs cache server-rename** command to rename the data in the cache if the name of a file server changed and you do not want to lose the cached data for the server. The renaming applies to prepositioned files and files cached on demand.

**Note**

Do not specify the name of another existing cached file server as the new name. If you do specify an existing name as the new name, the cached contents of this file server are overwritten with the cached contents of the file server you are renaming.

**Examples**

The following example shows how to enable the CIFS application accelerator:

```
WAE(config)# accelerator cifs enable
```

**Related Commands**

[show accelerator](#)

[show statistics accelerator](#)

[\(config\) windows-domain](#)

(config) accelerator cifs preposition

# (config) accelerator cifs preposition

To configure a CIFS application accelerator preposition directive, use the **accelerator cifs preposition** global configuration command. To disable the application accelerator, use the **no** form of this command.

**accelerator cifs preposition [remove] *directive\_id***

**no accelerator cifs preposition [remove] *directive\_id***

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | <b>remove</b> (Optional) Deletes a preposition directive.<br><b><i>directive_id</i></b> ID of an existing preposition directive that you want to change or delete, or a new directive that you want to create. |
|---------------------------|--|

|                 |                                |
|-----------------|--------------------------------|
| <b>Defaults</b> | No default behavior or values. |
|-----------------|--------------------------------|

|                      |                      |
|----------------------|----------------------|
| <b>Command Modes</b> | global configuration |
|----------------------|----------------------|

|                     |                         |
|---------------------|-------------------------|
| <b>Device Modes</b> | application-accelerator |
|---------------------|-------------------------|

|                         |   |
|-------------------------|---|
| <b>Usage Guidelines</b> | Use the <b>accelerator cifs preposition</b> command to create and edit preposition directives to be used with the transparent CIFS accelerator. A preposition directive defines a set of files that are to be prepositioned about the WAE device. |
|-------------------------|---|

The **accelerator cifs preposition** command invokes the preposition configuration submode. For details on the commands available in this submode to configure a preposition directive, see the “[Preposition Configuration Mode Commands](#)” section.

|                 |   |
|-----------------|---|
| <b>Examples</b> | The following example shows how to create a new CIFS preposition directive with ID 3: |
|-----------------|---|

```
WAE(config)# accelerator cifs preposition 3
WAE(config-preposition)
```

|                         |  |
|-------------------------|--|
| <b>Related Commands</b> | <a href="#">show accelerator</a><br><a href="#">show statistics accelerator</a><br><a href="#">(config) windows-domain</a> |
|-------------------------|--|

# (config) accelerator epm

To enable the Endpoint Mapper (EPM) application accelerator, use the **accelerator epm** global configuration command. To disable the EPM application accelerator, use the **no** form of this command.

**accelerator cifs preposition [remove] directive\_id**

**no accelerator cifs preposition [remove] directive\_id**

## Syntax Description

|                    |  |
|--------------------|--|
| <b>enable</b>      | (Optional) Enables the EPM application accelerator.                  |
| <b>exception</b>   | (Optional) Configures the action to be taken if an exception occurs. |
| <b>coredump</b>    | Writes a core file (default).  |
| <b>debug</b>       | Hangs the system until it is explicitly restarted.                   |
| <b>no-coredump</b> | Restarts the accelerator and does not write a core file.             |

## Defaults

The EPM accelerator is enabled by default and will start automatically if the Enterprise license is installed. The default exception action is coredump.

## Command Modes

global configuration

## Device Modes

application-accelerator

## Usage Guidelines

Use the **accelerator epm enable** command to enable the acceleration of EPM traffic. The EPM accelerator must be enabled for the MAPI accelerator to operate.

## Examples

The following example shows how to enable the EPM application accelerator:

```
WAE(config)# accelerator epm enable
```

## Related Commands

[\(config\) accelerator mapi](#)  
[show accelerator](#)  
[show statistics accelerator](#)

---

```
(config) accelerator http
```

## (config) accelerator http

To enable the HTTP application accelerator, use the **accelerator http** global configuration command. To disable the HTTP application accelerator, use the **no** form of this command.

```
accelerator http {enable | exception {coredump | debug | no-coredump}}
```

```
no accelerator http {enable | exception {coredump | debug | no-coredump}}
```

| Syntax Description |  |
|--------------------|--|
| <b>enable</b>      | (Optional) Enables the HTTP application accelerator.                 |
| <b>exception</b>   | (Optional) Configures the action to be taken if an exception occurs. |
| <b>coredump</b>    | Writes a core file (default).  |
| <b>debug</b>       | Hangs the system until it is explicitly restarted.                   |
| <b>no-coredump</b> | Restarts the accelerator and does not write a core file.             |

---

### Defaults

The HTTP accelerator is enabled by default and will start automatically if the Enterprise license is installed. The default exception action is coredump.

---

**Command Modes** global configuration

---

**Device Modes** application-accelerator

---

**Examples** The following example shows how to enable the HTTP application accelerator:

```
WAE(config)# accelerator http enable
```

---

**Related Commands**
[show accelerator](#)  
[show statistics accelerator](#)

# (config) accelerator mapi

To enable the MAPI application accelerator, use the **accelerator mapi** global configuration command. To disable the MAPI application accelerator, or one of its options, use the **no** form of this command.

```
accelerator mapi {enable | read-opt | write-opt | exception {coredump | debug | no-coredump}}
```

```
no accelerator mapi {enable | read-opt | write-opt | exception {coredump | debug | no-coredump}}
```

| Syntax Description |   |
|--------------------|---|
| <b>enable</b>      | Enables the MAPI traffic accelerator.   |
| <b>read-opt</b>    | Enables the read-ahead optimization of the MAPI traffic for mail reading.         |
| <b>write-opt</b>   | Enables the asynchronous write optimization of the MAPI traffic for mail sending. |
| <b>exception</b>   | (Optional) Configures the action to be taken if an exception occurs.              |
| <b>coredump</b>    | Writes a core file (default).   |
| <b>debug</b>       | Hangs the system until it is explicitly restarted.                                |
| <b>no-coredump</b> | Restarts the accelerator and does not write a core file.                          |

## Defaults

The MAPI accelerator is enabled by default and will start automatically if the Enterprise license is installed. The read optimization (**read-opt**) and write optimization (**write-opt**) features are enabled by default when the MAPI accelerator is enabled. The default exception action is coredump.

## Command Modes

global configuration

## Device Modes

application-accelerator

## Usage Guidelines

Use the **accelerator mapi enable** command to enable MAPI acceleration. This feature supports Microsoft Outlook 2000–2007 clients. Secure connections that use message authentication (signing) or encryption are not accelerated and MAPI over HTTP is not accelerated.

You must enable the EPM accelerator before the MAPI accelerator can operate.

## Examples

The following example shows how to enable the MAPI application accelerator:

```
WAE(config)# accelerator mapi enable
```

## Related Commands

[\(config\) accelerator epm](#)

[show accelerator](#)

[show statistics accelerator](#)

(config) accelerator nfs

## (config) accelerator nfs

To enable the NFS application accelerator, use the **accelerator nfs** global configuration command. To disable the NFS application accelerator, use the **no** form of this command.

```
accelerator nfs {enable | exception {coredump | debug | no-coredump}}
```

```
no accelerator nfs {enable | exception {coredump | debug | no-coredump}}
```

| Syntax Description |  |
|--------------------|--|
| <b>enable</b>      | (Optional) Enables the EPM application accelerator.                  |
| <b>exception</b>   | (Optional) Configures the action to be taken if an exception occurs. |
| <b>coredump</b>    | Writes a core file (default).  |
| <b>debug</b>       | Hangs the system until it is explicitly restarted.                   |
| <b>no-coredump</b> | Restarts the accelerator and does not write a core file.             |

---

### Defaults

The NFS accelerator is enabled by default and will start automatically if the Enterprise license is installed. The default exception action is coredump.

---

**Command Modes** global configuration

---

**Device Modes** application-accelerator

---

**Examples** The following example shows how to enable the NFS application accelerator:

```
WAE(config)# accelerator nfs enable
```

---

**Related Commands**
[show accelerator](#)  
[show statistics accelerator](#)

# (config) accelerator ssl

To enable the SSL application accelerator, use the **accelerator ssl** global configuration command. To disable the SSL application accelerator, use the **no** form of this command.

```
accelerator ssl {enable | exception {coredump | debug | no-coredump}}
```

```
no accelerator ssl {enable | exception {coredump | debug | no-coredump}}
```

| Syntax Description | <b>enable</b> (Optional) Enables the EPM application accelerator.<br><b>exception</b> (Optional) Configures the action to be taken if an exception occurs.<br><b>coredump</b> Writes a core file (default).<br><b>debug</b> Hangs the system until it is explicitly restarted.<br><b>no-coredump</b> Restarts accelerator and does not write a core file. |
|--------------------|---|
|--------------------|---|

|                 |  |
|-----------------|--|
| <b>Defaults</b> | The SSL accelerator is enabled by default and will start automatically if the Enterprise license is installed. The default exception action is coredump. |
|-----------------|--|

|                      |                      |
|----------------------|----------------------|
| <b>Command Modes</b> | global configuration |
|----------------------|----------------------|

|                     |                         |
|---------------------|-------------------------|
| <b>Device Modes</b> | application-accelerator |
|---------------------|-------------------------|

|                         |  |
|-------------------------|--|
| <b>Usage Guidelines</b> | Use the <b>accelerator ssl enable</b> command to enable the acceleration of SSL traffic. To undo this command, for example to disable SSL acceleration after you have enabled it, use the <b>no</b> version of this command. |
|-------------------------|--|

|                 |  |
|-----------------|--|
| <b>Examples</b> | The following example shows how to enable the SSL application accelerator: |
|-----------------|--|

```
WAE(config)# accelerator ssl enable
```

|                         |   |
|-------------------------|---|
| <b>Related Commands</b> | <a href="#">show accelerator</a><br><a href="#">show statistics accelerator</a><br><a href="#">crypto delete</a><br><a href="#">crypto export</a><br><a href="#">crypto generate</a><br><a href="#">crypto import</a><br><a href="#">(config) crypto pki</a><br><a href="#">(config) crypto ssl</a> |
|-------------------------|---|

■ (config) accelerator ssl

(config-ca) ca-certificate  
(config-ca) description  
(config-ca) revocation-check

# (config) accelerator video

To enable the video application accelerator, use the **accelerator video** global configuration command. To disable the video application accelerator, use the **no** form of this command.

```
accelerator video {enable | unaccelerated-traffic type {all | overload} action drop |
    max-initial-setup-delay seconds |
    windows-media {client idle-timeout seconds | log-forwarding enable}}
```

```
no accelerator video {enable | unaccelerated-traffic type {all | overload} action drop |
    max-initial-setup-delay seconds |
    windows-media {client idle-timeout seconds | log-forwarding enable}}
```

```
accelerator video exception {coredump | debug | no-coredump}
```

```
no accelerator video exception {coredump | debug | no-coredump}
```

| Syntax Description                     |  |
|--|--|
| <b>enable</b>                          | Enables the video traffic accelerator.   |
| <b>unaccelerated-traffic type</b>      | Configures the handling of video traffic that is not being accelerated due to overload or unsupported transport or format, including Windows Media video on demand traffic and all RTSP traffic that is not for Windows Media.   |
| <b>all</b>                             | Selects all video traffic that is not being accelerated due to overload or unsupported transport or format, including Windows Media video on demand traffic and all RTSP traffic that is not for Windows Media.  |
| <b>overload</b>                        | Selects video traffic that is not being accelerated due to an overload condition.  |
| <b>action drop</b>                     | Drops the specified type of video traffic that is not being accelerated. The connection is actually reset. If you do not specify this action, the default is to handle such traffic with the negotiated TCP optimization policy.   |
| <b>max-initial-setup-delay seconds</b> | Sets the maximum number of seconds to wait for the first message from the client and the first response from the server, after the connection is accepted by the video accelerator, and before timing out the connection. Valid values range from 10–180 seconds. The default is 60. |
| <b>windows-media</b>                   | Configures Windows Media-specific settings.  |
| <b>client idle-timeout seconds</b>     | Sets the maximum number of seconds to wait after the initial client request, while the client connection is idle, before timing out the connection. Valid values range from 30–300 seconds. The default is 60.   |
| <b>log-forwarding enable</b>           | Enables forwarding of Windows Media logs to the upstream Windows Media Server. Log forwarding is enabled by default.   |
| <b>exception</b>                       | (Optional) Configures the action to be taken if an exception occurs.   |
| <b>coredump</b>                        | Writes a core file (default).  |
| <b>debug</b>                           | Hangs the system until it is explicitly restarted.   |
| <b>no-coredump</b>                     | Restarts the accelerator and does not write a core file.   |

## Defaults

The video accelerator is enabled by default and will start automatically if both the Enterprise and Video licenses are installed. The default exception action is coredump.

(config) accelerator video

---

**Command Modes** global configuration

---

**Device Modes** application-accelerator

---

**Usage Guidelines** Use the **accelerator video enable** command to enable the acceleration of Windows Media live streaming video traffic that uses the RTSP.

You can configure the video accelerator to discard unaccelerated video traffic by using the **unaccelerated-traffic type {all | overload} action drop** option. If you do not specify this option, the unaccelerated video traffic is handled with the negotiated TCP optimization policy.

---

**Examples** The following example shows how to enable the video application accelerator:

```
WAE(config)# accelerator video enable
```

---

**Related Commands** [\*\*show accelerator\*\*](#)[\*\*show statistics accelerator\*\*](#)

# (config) accelerator windows-print

To enable the Windows print accelerator, use the **accelerator windows-print** global configuration command. To disable the Windows print accelerator, use the **no** form of this command.

**accelerator windows-print enable**

**no accelerator windows-print enable**

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

**Defaults** The Windows print accelerator is enabled by default and will start automatically if the Enterprise license is installed.

**Command Modes** global configuration

**Device Modes** application-accelerator

**Examples** The following example shows how to enable the Windows print accelerator:

```
WAE(config)# accelerator windows-print enable
```

**Related Commands** [show statistics windows-print requests](#)

(config) alarm overload-detect

## (config) alarm overload-detect

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

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

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

|                           |   |   |
|---------------------------|---|---|
| <b>Syntax Description</b> | <b>clear 1-999</b><br><b>raise 10-1000</b><br><b>enable</b> | Specifies the number of alarms per second 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.<br><br><b>Note</b> The <b>alarm overload-detect clear</b> value must be less than the <b>alarm overload-detect raise</b> value.<br>(Optional) Specifies the number of alarms per second at which the WAAS device enters an alarm overload state and SNMP traps and alarm notifications to your network management station (NMS) are suspended.<br>Enables the detection of alarm overload situations. |
|---------------------------|---|---|

### Defaults

**clear:** 1 alarm per second  
**raise:** 10 alarms per second

### Command Modes

global configuration

### Device Modes

application-accelerator  
 central-manager

### Usage Guidelines

In the alarm overload state, applications continue to raise alarms and these alarms are recorded within the WAAS device. Use the **show alarms** and **show alarms history** EXEC commands to display all the alarms in the alarm overload state.

### Examples

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

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

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

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

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

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

**Related Commands** [show alarms](#)

(config) asset

## (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***

**no asset tag *name***

|                           |   |                          |
|---------------------------|---|--------------------------|
| <b>Syntax Description</b> | <b>tag <i>name</i></b>  | Sets the asset tag name. |
| <b>Defaults</b>           | No default behaviors or values.   |                          |
| <b>Command Modes</b>      | global configuration  |                          |
| <b>Device Modes</b>       | application-accelerator<br>central-manager  |                          |
| <b>Examples</b>           | The following example shows how to configure a tag name for the asset tag string on a WAAS device:<br><br>WAE(config)# <b>asset tag entitymib</b> |                          |

# (config) authentication configuration

To specify administrative login authorization parameters for a WAAS device, use the **authentication configuration** 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]
```

```
no authentication {configuration {local | radius | tacacs | windows-domain}}
    enable [primary | secondary | tertiary | quaternary]
```

| Syntax Description    |  |
|-----------------------|--|
| <b>configuration</b>  | Sets the administrative login authorization (configuration) parameters for the WAAS device.                                      |
| <b>local</b>          | Selects the local database method for the WAAS device.   |
| <b>radius</b>         | Selects the RADIUS method for the WAAS device.   |
| <b>tacacs</b>         | Selects the TACACS+ method for the WAAS device.  |
| <b>windows-domain</b> | Selects the Windows domain controller method for the WAAS device.  |
| <b>enable</b>         | Enables the specified methods for the WAAS device.   |
| <b>primary</b>        | (Optional) Specifies the first method that the WAAS device should use.   |
| <b>secondary</b>      | (Optional) Specifies the second method that the WAAS device should use.  |
| <b>tertiary</b>       | (Optional) Specifies the third method that the WAAS device should use if the primary and secondary methods fail.                 |
| <b>quaternary</b>     | (Optional) Specifies the fourth method that the WAAS device should use if the primary, secondary, and tertiary methods all fail. |

**Defaults** The local authentication method is enabled by default.

**Command Modes** global configuration

**Device Modes** application-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.



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*.

**(config) authentication configuration**

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. The 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 the local method 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 a 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 a 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 the Windows Domain Login Authentication

You can enable the 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 **windows-domain wins-server** global configuration command. (See the [\(config\) windows-domain](#) command.)


**Note**


---

WAAS supports authentication by a Windows domain controller running only on Windows Server 2000 or Windows Server 2003.

---



---

**Examples**

The following example shows how to query the secondary authentication database if the primary authentication server is unreachable. This feature is referred to as the failover server-unreachable feature.

```
WAE(config)# authentication fail-over server-unreachable
```

If you enable the failover server-unreachable feature on the WAAS device, only two login authentication schemes (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. In the following example, 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 authentication methods are specified because the failover 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
```

(config) authentication configuration

**Note**

If you enable 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 failover 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 enable 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 content-request

# (config) authentication content-request

To authenticate a request for content, use the **authentication content-request** global configuration mode command. To selectively disable options, use the **no** form of this command.

**authentication content-request windows-domain-ctrl disconnected-mode enable**

**no authentication content-request windows-domain-ctrl disconnected-mode enable**

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | <b>content-request</b> Authenticates a request for content.<br><b>Note</b> This option is available in the application-accelerator device mode only. |
|                           | <b>windows-domain-ctrl</b> Selects a Windows domain controller for domain server authentication.   |
|                           | <b>disconnected-mode enable</b> Enables authentication in the disconnected mode.   |

**Defaults** The local authentication method is enabled by default.

**Command Modes** global configuration

**Device Modes** application-accelerator

**Usage Guidelines** The **authentication** command configures both the authentication and authorization methods that govern login and configuration access to the WAAS device.



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. The 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 the local method 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 a 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 a 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.)

(config) authentication content-request

### 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 the Windows Domain Login Authentication

You can enable the 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 **windows-domain wins-server** global configuration command. (See the [\(config\) windows-domain](#) command.)



**Note** WAAS supports authentication by a Windows domain controller running only on Windows Server 2000 or Windows Server 2003.

### Examples

The following example shows how to query the secondary authentication database if the primary authentication server is unreachable. This feature is referred to as the failover server-unreachable feature.

```
WAE(config)# authentication fail-over server-unreachable
```

If you enable the failover server-unreachable feature on the WAAS device, only two login authentication schemes (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. In the following example, 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 authentication methods are specified because the failover 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 enable 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 failover 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 enable 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 fail-over

## (config) authentication fail-over

To specify authentication failover if the primary authentication server is unreachable, use the **authentication fail-over** global configuration mode command. To selectively disable options, use the **no** form of this command.

**authentication fail-over server-unreachable**

**no authentication fail-over server-unreachable**

|                           |                                     |   |
|---------------------------|-------------------------------------|---|
| <b>Syntax Description</b> | <b>fail-over server-unreachable</b> | Specifies that the WAAS device is to query the secondary authentication database if the primary authentication server is unreachable. |
|---------------------------|-------------------------------------|---|

**Defaults** The local authentication method is enabled by default.

**Command Modes** global configuration

**Device Modes** application-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.



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. The 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 the local method 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 a 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 a 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

(config) authentication fail-over

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 the Windows Domain Login Authentication

You can enable the 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 **windows-domain wins-server** global configuration command. (See the [\(config\) windows-domain](#) command.)



**Note**

WAAS supports authentication by a Windows domain controller running only on Windows Server 2000 or Windows Server 2003.

### Examples

The following example shows how to query the secondary authentication database if the primary authentication server is unreachable. This feature is referred to as the failover server-unreachable feature.

```
WAE(config)# authentication fail-over server-unreachable
```

If you enable the failover server-unreachable feature on the WAAS device, only two login authentication schemes (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. In the following example, 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 authentication methods are specified because the failover 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 enable 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 failover 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 enable 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 login

# (config) authentication login

To set the administrative login authentication parameters for a WAAS device, use the **authentication login** global configuration mode command. To selectively disable options, use the **no** form of this command.

```
authentication login {local | radius | tacacs | windows-domain}
enable [primary | secondary | tertiary| quaternary]
```

```
no authentication login {local | radius | tacacs | windows-domain}
enable [primary | secondary | tertiary| quaternary]
```

| Syntax Description |  |
|--------------------|--|
|                    | <b>login</b> Sets the administrative login authentication parameters for the WAAS device.  |
|                    | <b>local</b> Selects the local database method for the WAAS device.  |
|                    | <b>radius</b> Selects the RADIUS method for the WAAS device.   |
|                    | <b>tacacs</b> Selects the TACACS+ method for the WAAS device.  |
|                    | <b>windows-domain</b> Selects the Windows domain controller method for the WAAS device.  |
|                    | <b>enable</b> Enables the specified methods for the WAAS device.   |
|                    | <b>primary</b> (Optional) Specifies the first method that the WAAS device should use.  |
|                    | <b>secondary</b> (Optional) Specifies the second method that the WAAS device should use.   |
|                    | <b>tertiary</b> (Optional) Specifies the third method that the WAAS device should use if the primary and secondary methods fail.                   |
|                    | <b>quaternary</b> (Optional) Specifies the fourth method that the WAAS device should use if the primary, secondary, and tertiary methods all fail. |

---

**Defaults** The local authentication method is enabled by default.

---

**Command Modes** global configuration

---

**Device Modes** application-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.



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. The 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 the local method 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 a 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 a 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.

(config) authentication login

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 the Windows Domain Login Authentication

You can enable the 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 **windows-domain wins-server** global configuration command. (See the **(config) windows-domain** command.)


**Note**

WAAS supports authentication by a Windows domain controller running only on Windows Server 2000 or Windows Server 2003.

**Examples**

The following example shows how to query the secondary authentication database if the primary authentication server is unreachable. This feature is referred to as the failover server-unreachable feature.

```
WAE(config)# authentication fail-over server-unreachable
```

If you enable the failover server-unreachable feature on the WAAS device, only two login authentication schemes (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. In the following example, 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 authentication methods are specified because the failover 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 enable 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 failover 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 enable 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](#)

■ (config) authentication login

```
show statistics tacacs  
(config) tacacs  
windows-domain  
(config) windows-domain
```

# (config) authentication strict-password-policy

To activate the strong password policy on a WAAS device, use the **authentication strict-password-policy** global configuration command. To deactivate the strong password policy and use the standard password policy on a WAAS device, use the **no** form of this command.

**authentication strict-password-policy**

**no authentication strict-password-policy**

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

**Defaults** The strong password policy is enabled on the WAAS device.

**Command Modes** global configuration

**Device Modes** application-accelerator  
central-manager

**Usage Guidelines** When you enable the strong password policy, your user passwords must meet the following requirements:

- The password must be 8 to 31 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.
- Each new password must be different from the previous 12 passwords. User passwords expire within 90 days.
- The password cannot contain the characters ‘ “ | (apostrophe, double quote, or pipe) or any control characters.

When you disable the strong password policy, user passwords must meet the following requirements:

- The password must have 1 to 31 characters.
- 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 you enable the strong password policy, existing standard-policy passwords will still work. However, these passwords are subject to expiration under the strong password policy.

```
■ (config) authentication strict-password-policy
```

---

**Examples**

The following example shows how to enable the strong password policy:

```
WAE(config)# authentication strict-password-policy
```

The following example shows how to disable the strong password policy:

```
WAE(config)# no authentication strict-password-policy
```

---

**Related Commands**

[clear users](#)

[\(config\) authentication configuration](#)

# (config) 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 **auto-discovery** global configuration command. To disable auto-discovery, use the **no** form of this command.

```
auto-discovery blacklist {enable | hold-time minutes}
```

```
no auto-discovery blacklist {enable | hold-time minutes}
```

|                           |   |
|---------------------------|---|
| <b>Syntax Description</b> | <b>blacklist</b> Specifies the TFO auto-discovery blacklist server configuration.<br><b>enable</b> Enables the TFO auto-discovery blacklist operation.<br><b>hold-time minutes</b> Specifies the maximum time to hold the blacklisted server address in the cache. The range is 1–10080 minutes. The default is 60 minutes. |
|---------------------------|---|

**Defaults**      The default auto-discovery blacklist hold time is 60 minutes.

**Command Modes**      global configuration

**Device Modes**      application-accelerator

**Usage Guidelines**      Use the **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 TCP packets with options 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.

**Examples**      The following example shows how to enable TFO auto-discovery blacklist using the **auto-discovery** command:

```
WAE(config)# auto-discovery blacklist enable
```

**Related Commands**      [show statistics auto-discovery](#)

(config) auto-register

## (config) auto-register

To enable the discovery of a Fast Ethernet or Gigabit Ethernet WAE and its automatic registration with the WAAS Central Manager through the 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]**

**no 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.   |
|--------------------|----------------------------------|---|
|                    | <b>FastEthernet slot/port</b>    | (Optional) Selects a Fast Ethernet interface for automatic registration using DHCP. Slot number and port number of the Fast Ethernet interface. Valid slot values are from 0 to 3.  |
|                    | <b>GigabitEthernet slot/port</b> | (Optional) Selects a Gigabit Ethernet interface for automatic registration using DHCP. Slot number and port number of the Gigabit Ethernet interface. Valid slot values are 1 or 2. |

**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 that run the WAAS software (with the exception of the WAAS Central Manager) automatically discover the WAAS Central Manager and register with it. You do not have to do any manual configuration on the device. Once the WAE is registered, you can approve the device and configure it remotely using the WAAS Central Manager GUI.

You can use the **auto-register enable** command to allow 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.



**Note** You must disable autoregistration when both device interfaces are configured as port-channel interfaces.

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 DHCP that is used for autoregistration is *not* the same as the interface-level DHCP that is configurable through the **ip address dhcp** interface configuration command.

To assign a static IP address using the **interface GigabitEthernet slot/port** command, you must first disable the automatic registration of devices through DHCP by using the **no auto-register enable** command.

---

**Examples**

The following example shows how to enable autoregistration on GigabitEthernet port 2/0:

```
WAE(config)# auto-register enable GigabitEthernet 2/0
```

The following example shows how to disable 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

# (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]}}
```

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

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | <b>enable</b> Enables banner support on the WAE.<br><b>exec</b> Configures an EXEC banner.<br><b>message text</b> (Optional) Specifies a message to be displayed when an EXEC process is created. The message text is on a single line (980 characters maximum). The WAE translates the \n portion of the message to a new line when the banner is displayed to the user.<br><b>login</b> Configures a login banner.<br><b>motd</b> Configures an MOTD banner. |
|---------------------------|--|

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

**Command Modes** global configuration

**Usage Guidelines** 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 you enter when 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#
```

■ (config) banner

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}
```

```
no bypass static {clientip | any-client} {serverip | any-server}
```

| Syntax Description |   |
|--------------------|---|
| <b>static</b>      | Adds a static entry to the bypass list.                               |
| <b>clientip</b>    | Requests from this IP address bypass the WAE.                         |
| <b>any-client</b>  | Bypasses the traffic from any client destined to a particular server. |
| <b>serverip</b>    | Requests from this IP address bypass the WAE.                         |
| <b>any-server</b>  | 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** 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.



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 shows how to force 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 shows how to force all traffic destined to a specified server to bypass the WAE:

```
WAE(config)# bypass static any-client 172.16.7.52
```

The following example shows how to force 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
```

**(config) bypass**

| 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** global configuration command. To disable CDP, use the **no** form of this command.

```
cdp {enable | holdtime seconds | timer seconds}
no cdp {enable | holdtime seconds | timer seconds}
```

| Syntax Description | <b>enable</b>           | Enables CDP globally.  |
|--------------------|-------------------------|--|
|                    | <b>holdtime seconds</b> | Sets the length of time in seconds (10–255) that a receiver keeps CDP packets before they are discarded. The default is 180 seconds. |
|                    | <b>timer seconds</b>    | Interval between the CDP advertisements in seconds (5–254). The default is 60 seconds.   |

| Defaults | <b>holdtime:</b> 180 seconds |
|----------|------------------------------|
|          | <b>timer:</b> 60 seconds     |

| Command Modes | global configuration |
|---------------|----------------------|
|---------------|----------------------|

| Device Modes | application-accelerator |
|--------------|-------------------------|
|              | central-manager         |

| Examples | The following example shows that when 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: |
|----------|--|
|          | <pre>WAE(config)# cdp enable WAE(config)# cdp holdtime 10 WAE(config)# cdp timer 15</pre>  |

| Related Commands | <a href="#">(config-if) cdp</a> |
|------------------|---------------------------------|
|                  | <a href="#">clear arp-cache</a> |
|                  | <a href="#">show cdp</a>        |

(config) central-manager

## (config) central-manager

To specify the WAAS Central Manager 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}
no central-manager {address {hostname | ip-address} | role {primary | standby} | ui port
port-num}}
```

| Syntax Description          |  |
|-----------------------------|--|
| <b>address</b>              | 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.   |
| <b>role</b>                 | Configures the WAAS Central Manager role to either primary or standby.   |
| <b>primary</b>              | Configures the WAAS Central Manager to be the primary WAAS Central Manager for the WAEs that are registered with it. |
| <b>standby</b>              | Configures the WAAS Central Manager to be the standby WAAS Central Manager for the WAEs that are registered with it. |
| <b>ui</b>                   | Configures the WAAS Central Manager GUI port address.  |
| <b>port</b> <i>port-num</i> | Configures the WAAS Central Manager GUI port (1–65535). The default is port 8443.                                    |


**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.

|                      |  |
|----------------------|--|
| <b>Defaults</b>      | The WAAS Central Manager GUI is preconfigured to use port 8443.  |
| <b>Command Modes</b> | global configuration   |
| <b>Device Modes</b>  | application-accelerator<br>central-manager   |
| <b>Examples</b>      | The following example shows how to specify 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 shows how to specify that 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 shows how to configure a new GUI port to access the WAAS Central Manager GUI:

```
WAE(config)# central-manager ui port 8550
```

The following example shows how to configure 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

## (config) clock

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

```
clock {timezone timezone hoursoffset [minutesoffset]} |
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} }

no clock {timezone timezone hoursoffset [minutesoffset]} |
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} }
```

| Syntax Description                |  |
|-----------------------------------|--|
| <b>timezone</b> <i>timezone</i>   | Configures the name of the standard time zone and hours offset from UTC  |
| <b>hoursoffset</b>                | (–23 to +23). See “ <a href="#">Usage Guidelines</a> ” section tables.   |
| <b>minutesoffset</b>              | (Optional) Minutes offset (see the table below in the “ <a href="#">Usage Guidelines</a> ” section) from UTC (0–59). |
| <b>summertime</b> <i>timezone</i> | Configures the name of the summer or daylight saving time zone.  |
| <b>date</b>                       | Configures the absolute summer time.   |
| <b>startday</b>                   | Date (1–31) to start.  |
| <b>startmonth</b>                 | Month (January through December) to start.   |
| <b>startyear</b>                  | Year (1993–2032) to start.   |
| <b>starthour</b>                  | Hour (0–23) to start in hour:minute (hh:mm) format.  |
| <b>endday</b>                     | Date (1–31) to end.  |
| <b>endmonth</b>                   | Month (January through December) to end.   |
| <b>endyear</b>                    | Year (1993–2032) to end.   |
| <b>endhour</b>                    | Hour (0–23) to end in hour:minute (hh:mm) format.  |
| <b>offset</b>                     | Minutes offset (see the table below in the “ <a href="#">Usage Guidelines</a> ” section) from UTC (0–59).            |
| <b>recurring</b>                  | Configures the recurring summer time.  |
| <b>1-4</b>                        | Configures the starting week number 1–4.   |
| <b>startweekday</b>               | Day of the week (Monday–Friday) to start.  |
| <b>endweekday</b>                 | Weekday (Monday–Friday) to end.  |
| <b>first</b>                      | Configures the summer time to recur beginning the first week of the month.   |
| <b>last</b>                       | Configures the summer time to recur beginning the last week of the month.  |

| Defaults      | No default behavior or values. |
|---------------|--------------------------------|
| Command Modes | global configuration           |

**Device Modes**

application-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.

**Note**

Unexpected time changes can result in unexpected system behavior. We recommend reloading the system after changing the system clock.

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 *O O* 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 O O
```

**Note**

The time zone entry is case sensitive and must be specified in the exact notation listed in [Table 3-1](#). When you use a time zone entry from the time zone table, the system is automatically adjusted for daylight saving time.

**Table 3-1 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              |
| Asia/Baku            | +4              |
| Asia/Bangkok         | +7              |
| Asia/Colombo         | +6              |

(config) clock

**Table 3-1** Time Zone—Offsets from UTC (continued)

| Time Zone           | Offset from UTC |
|---------------------|-----------------|
| 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              |
| Europe/London       | 0               |
| Europe/Moscow       | +3              |
| Europe/Paris        | +1              |

**Table 3-1 Time Zone—Offsets from UTC (continued)**

| Time Zone         | Offset from UTC |
|-------------------|-----------------|
| 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 shows how to specify 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 shows how to negate the time zone setting on the WAAS device:

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

The following example shows how to configure 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

## (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
```

```
no cms {database maintenance {full {enable | schedule weekday at time} } |
         regular {enable | schedule weekday at time} } | enable
```

```
cms rpc timeout {connection 5-1800 | incoming-wait 10-600 | transfer 10-7200}
```

```
no cms rpc timeout {connection 5-1800 | incoming-wait 10-600 | transfer 10-7200}
```

| Syntax Description | <b>database maintenance</b> | Configures the embedded database clean or reindex maintenance routine.  |
|--------------------|-----------------------------|---|
|                    | <b>full</b>                 | Configures the full maintenance routine and cleans the embedded database tables.  |
|                    | <b>enable</b>               | Enables the specified routine or process to be performed on the embedded database tables.   |
|                    | <b>schedule weekday</b>     | Sets the schedule for performing the maintenance routine to a day of the week.<br><br>every-day Every day<br>Mon every Monday<br>Tue every Tuesday<br>Wed every Wednesday<br>Thu every Thursday<br>Fri every Friday<br>Sat every Saturday<br>Sun every Sunday                         |
|                    | <b>at time</b>              | Sets the maintenance schedule time of day to start the maintenance routine (0-23:0-59) (hh:mm).<br><br>at Maintenance time of day<br>Mon every Monday<br>Tue every Tuesday<br>Wed every Wednesday<br>Thu every Thursday<br>Fri every Friday<br>Sat every Saturday<br>Sun every Sunday |
|                    | <b>regular</b>              | Configures the regular maintenance routine and reindexes the embedded database tables.  |
|                    | <b>rpc timeout</b>          | Configures the timeout values for remote procedure call connections.  |
|                    | <b>connection 5-1800</b>    | Specifies the maximum time to wait when making a connection. The timeout period is in seconds. The default for the WAAS Central Manager is 30 seconds; the default for a WAE is 180 seconds.  |

---

|                             |  |
|-----------------------------|--|
| <b>incoming-wait</b> 10-600 | Specifies the maximum time to wait for a client response. The timeout period is in seconds. The default is 30 seconds.         |
| <b>transfer</b> 10-7200     | Specifies the maximum time to allow a connection to remain open. The timeout period is 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

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 shows how to schedule 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
```

```
■ (config) cms
```

**Related Commands**

- [cms](#)
- [show cms](#)

## (config) crypto pki

To configure public key infrastructure (PKI) encryption parameters on a WAAS device, use the **crypto pki** global configuration command. To negate these actions, use the **no** form of this command.

```
crypto pki {ca certificate-authority-name | global-settings}
```

| Syntax Description | ca                                | Configures encryption certificate authority information. Using this command enables certificate authority configuration mode. See <a href="#">PKI Certificate Authority Configuration Mode Commands, page -695</a> . |
|--------------------|-----------------------------------|--|
|                    | <i>certificate-authority-name</i> | The name of the certificate authority that you want to edit.   |
|                    | global-settings                   | Configures PKI encryption global settings. Using this command enables PKI global settings configuration mode. See <a href="#">PKI Certificate Authority Configuration Mode Commands, page -695</a> .                 |

**Defaults** There are no default arguments or values for this command.

**Command Modes** global configuration

**Device Modes** application-accelerator  
central-manager

**Usage Guidelines** Use the **crypto pki** global configuration command to enter CA configuration mode or PKI global settings configuration mode.

**Examples** The following example puts WAAS into CA configuration mode, editing the “my-ca” certification authority. The mode change is indicated by the system prompt:

```
WAE(config)# crypto pki my-ca
WAE(config-ca) #
```

**Related Commands**
[\(config\) crypto ssl](#)
[\(config-ca\) ca-certificate](#)
[\(config-ca\) description](#)
[\(config-ca\) revocation-check](#)

(config) crypto ssl

# (config) crypto ssl

To configure secure sockets layer (SSL) encryption parameters on a WAAS device, use the **crypto ssl** global configuration command. To negate these actions, use the **no** form of this command.

```
crypto ssl {cipher list cipher-list-name | management-service | services}
```

| Syntax Description |                           |  |
|--------------------|---------------------------|--|
|                    | <b>cipher-list</b>        | Configures the SSL cipher suite list. Using this command enables cipher list configuration mode. See the <a href="#">SSL Cipher List Configuration Mode Commands</a> . |
|                    | <i>cipher-list-name</i>   | The name of the SSL cipher list that you want to edit.   |
|                    | <b>management-service</b> | Configures SSL management services. Using this command enables SSL management configuration mode.  |
|                    | <b>services</b>           | Configures SSL services. Using this command enables SSL global configuration mode.   |

**Defaults** There are no default arguments or values for this command.

**Command Modes** global configuration

**Device Modes** application-accelerator  
central-manager

**Usage Guidelines** Use the **crypto ssl** global configuration command to enter SSL cipher list configuration mode, SSL management services configuration mode, or SSL global settings configuration mode.

**Examples** The following example puts the WAAS device into SSL cipher list configuration mode, editing the myList cipher suite list. The mode change is indicated by the system prompt:

```
WAE(config)# crypto ssl cipher-list myList
WAE(config-cipher-list) #
```

**Related Commands** [\(config\) crypto pki](#)  
[\(config-cipher-list\) cipher](#)

# (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 | central-manager}**

**no device mode {application-accelerator | central-manager}**

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | <b>application-accelerator</b> Configures the WAAS device to function as a WAAS Accelerator. All of your Edge WAEs and Core WAEs should be operating in this mode.<br><b>central-manager</b> 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  
central-manager

**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
```

To change the device mode from central-manager to application-accelerator, you must first use the **cms deregister** 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, as shown in the following example:

```
WAE# cms deregister
WAE(config)# device mode application-accelerator
WAE# copy running-config startup-config
```

**Related Commands** [show device-mode](#)

(config) directed-mode

## (config) directed-mode

To configure the mode by which traffic is sent between two WAEs, use the **directed-mode** global configuration command. To configure the WAAS device not to use directed mode, use the **no** form of this command.

**directed-mode enable [port *udp-port*]**

**no directed-mode enable [port *udp-port*]**

|                             |  |               |                        |                             |  |
|-----------------------------|--|---------------|------------------------|-----------------------------|--|
| <b>Syntax Description</b>   | <table border="0"> <tr> <td><b>enable</b></td><td>Enables directed mode.</td></tr> <tr> <td><b>port <i>udp-port</i></b></td><td>Sets the UDP port number to use to send traffic between two WAEs.<br/>The default port is 4050.</td></tr> </table> | <b>enable</b> | Enables directed mode. | <b>port <i>udp-port</i></b> | Sets the UDP port number to use to send traffic between two WAEs.<br>The default port is 4050. |
| <b>enable</b>               | Enables directed mode.   |               |                        |                             |  |
| <b>port <i>udp-port</i></b> | Sets the UDP port number to use to send traffic between two WAEs.<br>The default port is 4050.   |               |                        |                             |  |

**Defaults** The default communication mode to a peer WAE is transparent mode (not directed mode).

**Command Modes** global configuration

**Device Modes** application-accelerator

**Examples** The following example shows how to configure a WAE for directed mode on the default UDP port of 4050:

```
WAE(config)# directed-mode enable
```

**Related Commands**
[show statistics auto-discovery](#)  
[show statistics connection closed](#)

## (config) disk disk-name

To disable the disk for online removal, use the **disk disk-name** global configuration command. To reenable the disk, use the **no** form of this command.

**disk disk-name diskxx shutdown [force]**

**no disk disk-name diskxx shutdown [force]**

| Syntax Description | <b>diskxx</b> Name of the disk (disk00-disk05).<br><b>shutdown</b> Disables the disk for maintenance.<br><b>force</b> (Optional) Forces a disk to be reenabled when used with the <b>no</b> form of this command.<br>This option is not available on RAID-5 systems. |
|--------------------|--|
|--------------------|--|

**Defaults** Disks are enabled.

**Command Modes** global configuration

**Device Modes** application-accelerator  
central-manager

**Usage Guidelines** This command is not available on the WAE-7341 and WAE-7371 models. Instead, use the **disk disk-name diskxx replace** EXEC mode command.

You can replace a failed disk or perform a 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 a scheduled disk maintenance, or 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.)



**Note** The **show disks failed-disk-id** EXEC command is not available on WAE-7341 and WAE-7371 models.

**Examples** The following example shows how to disable disk00 for online removal using the **disk disk-name** command:

```
WAE(config)# disk disk-name disk00 shutdown
```

**Related Commands** [\(config\) disk error-handling](#)

■ (config) disk disk-name

(config) disk logical shutdown  
disk  
show disks

# (config) disk encrypt

To enable disk encryption, use the **disk encrypt** global configuration command. To disable disk encryption, use the **no** form of this command.

**disk encrypt enable**

**no disk encrypt enable**

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

**Defaults** Disk encryption is disabled by default.

**Command Modes** global configuration

**Device Modes** application-accelerator

**Usage Guidelines** To view the encryption status details, use the **show disks details** EXEC command. While the file system is initializing, you will see the following message: “System initialization is not finished, please wait...” You may also view the disk encryption status to check whether a disk is enabled or disabled in the Central Manager GUI, Device Home window.

**Examples** The following example shows how to enable disk encryption using the **disk encrypt** command:

```
WAE(config)# disk encrypt enable
```

**Related Commands**

[disk](#)

[show disks](#)

(config) disk error-handling

## (config) disk error-handling

To configure how disk errors are handled on a WAAS device, use the **disk error-handling** global configuration command. To disable automatic remapping of disk errors, use the **no** form of this command.

**disk error-handling remap**

**no disk error-handling remap**

|                           |              |  |
|---------------------------|--------------|--|
| <b>Syntax Description</b> | <b>remap</b> | Sets the disk to attempt to remap disk errors automatically. |
|---------------------------|--------------|--|

**Defaults** The disk is configured to remap disk errors automatically.

**Command Modes** global configuration

**Device Modes** application-accelerator  
central-manager

**Examples** The following example shows how to disable automatic remapping of disk errors:

```
WAE(config)# no disk error-handling remap
```

**Related Commands** [disk](#)  
[show disks](#)

# (config) disk logical shutdown

To shut down the RAID-5 logical disk drive, use the **disk logical shutdown** global configuration command. To reenable the RAID-5 logical disk drive, use the **no** form of this command.

**disk logical shutdown**

**no disk logical shutdown [force]**

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | force<br><br>(Optional) Forces RAID Logical drive to be reenabled when used with the <b>no</b> form of this command. |
|---------------------------|--|

|                 |  |
|-----------------|--|
| <b>Defaults</b> | The RAID-5 array is configured by default. |
|-----------------|--|

|                      |                      |
|----------------------|----------------------|
| <b>Command Modes</b> | global configuration |
|----------------------|----------------------|

|                     |                         |
|---------------------|-------------------------|
| <b>Device Modes</b> | application-accelerator |
|---------------------|-------------------------|

|                         |   |
|-------------------------|---|
| <b>Usage Guidelines</b> | This command is supported on WAE-7341, WAE-7371, and WAE-674 models only.<br><br>Use this command to operate the WAE in diskless mode. In diskless mode, the partitions and disks are not mounted and cannot be used.<br><br>You must reload the device for this command to take effect.<br><br>After a multiple disk failure or RAID controller failure, and after the drives are replaced and the RAID disk is rebuilt, the logical disk may remain in the error state. To reenable the disk, use the <b>no disk logical shutdown force</b> command, then reload the WAE. |
|-------------------------|---|

|                 |  |
|-----------------|--|
| <b>Examples</b> | The following example shows how shutdown the RAID-5 logical disk drive using the <b>disk logical shutdown</b> command: |
|-----------------|--|

```
WAE(config)# disk logical shutdown
```

|                         |   |
|-------------------------|---|
| <b>Related Commands</b> | <a href="#">(config) disk disk-name</a> |
|-------------------------|---|

(config) egress-method

## (config) egress-method

To configure the egress method for intercepted connections, use the **egress-method** global configuration command. To unconfigure the egress method, use the **no** form of this command.

```
egress-method {ip-forwarding | negotiated-return | generic-gre} intercept-method wccp
```

```
no egress-method {ip-forwarding | negotiated-return | generic-gre} intercept-method wccp
```

| Syntax Description       |  |
|--------------------------|--|
| <b>ip-forwarding</b>     | Configures the IP forwarding egress method.                                  |
| <b>negotiated-return</b> | Configures the WCCP negotiated return egress method.                         |
| <b>generic-gre</b>       | Configures the generic GRE egress method.                                    |
| <b>intercept-method</b>  | Chooses for which interception method the egress method is being configured. |
| <b>wccp</b>              | Configures the egress method for WCCP interception.                          |

**Defaults** The default egress method is IP forwarding.

**Command Modes** global configuration

**Device Modes** application-accelerator

**Examples** 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
```

The following example shows how to configure the interception and egress method for the generic GRE egress method from the CLI by configuring an intercepting router list, and then configuring the generic GRE egress method:

```
WAE(config)# wccp router-list 1 192.168.68.98
WAE(config)# egress-method generic-gre intercept-method wccp
```

The router list must contain the IP address of each intercepting router. Multicast addresses are not supported. Additionally, you must configure a GRE tunnel interface on each router.

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 statistics connection egress-methods** EXEC command.

To view information about the generic GRE egress method, use the **show generic-gre** EXEC command.

To clear statistics information for the generic GRE egress method, use the **clear statistics generic-gre** EXEC command.

**Related Commands**

[clear arp-cache](#)  
[debug egress-method](#)  
[show egress-methods](#)  
[show tfo tcp](#)  
[\(config\) wccp tcp-promiscuous mask](#)

**(config) end**

## (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  
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.

In addition, you can press **Ctrl-Z** to exit 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*

**no exec-timeout** *timeout*

| Syntax Description | <i>timeout</i> | Timeout in minutes (0–44640). A value of 0 sets the logout timeout to infinite. |
|--------------------|----------------|---|
|--------------------|----------------|---|

|          |                            |
|----------|----------------------------|
| Defaults | The default is 15 minutes. |
|----------|----------------------------|

|               |                      |
|---------------|----------------------|
| Command Modes | global configuration |
|---------------|----------------------|

|              |  |
|--------------|--|
| Device Modes | application-accelerator<br>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 <b>exec-timeout</b> command. When the <b>exec-timeout</b> interval elapses, the WAAS device automatically closes the Telnet or SSH session. |
|------------------|--|

|          |  |
|----------|--|
| Examples | The following example shows how to configure a timeout of 100 minutes: |
|----------|--|

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

The following example shows how to negate the configured timeout of 100 minutes and revert to the default value of 15 minutes:

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

|                  |  |
|------------------|--|
| Related Commands | <a href="#">(config) telnet enable</a> |
|------------------|--|

(config) exit

## (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  
central-manager

**Usage Guidelines** This command is equivalent to pressing **Ctrl-Z** or entering the **end** command.

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

```
WAE(config)# exit
WAE#
```

**Related Commands** [\(config\) end](#)

# (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}
```

```
no flow monitor tcpstat-v1 {enable | host ip_address}
```

| Syntax Description | <b>tcpstat-v1</b> Sets the tcpstat-v1 collector configuration.<br><b>enable</b> Enables flow monitoring.<br><b>host ip_address</b> Specifies the 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 information about how 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>.

**Examples** The following example shows how to enable flow monitoring using the **flow monitor** command:

```
WAE(config)# flow monitor tcpstat-v1 enable
```

**Related Commands** [debug flow](#)

(config) help

# (config) help

To obtain online help for the command-line interface, use the **help** global configuration command. To disable help, use the **no** form of this command.

**help**

**no 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  
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 use the backspace key 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
```

**Related Commands** [show running-config](#)

(config) hostname

## (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**

**no hostname name**

---

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

---

|                 |  |
|-----------------|--|
| <b>Defaults</b> | The default hostname is the model number of the WAAS device (for example WAE-511, WAE-611, or WAE-7326). |
|-----------------|--|

|                      |                      |
|----------------------|----------------------|
| <b>Command Modes</b> | global configuration |
|----------------------|----------------------|

|                     |  |
|---------------------|--|
| <b>Device Modes</b> | application-accelerator<br>central-manager |
|---------------------|--|

|                         |  |
|-------------------------|--|
| <b>Usage Guidelines</b> | 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: @, #, \$, %, ^, &, \*, (), |, \", /, <>.

|                 |   |
|-----------------|---|
| <b>Examples</b> | The following example shows how to change the hostname of the WAAS device to <i>sandbox</i> : |
|-----------------|---|

```
WAE-511(config)# hostname sandbox
Sandbox(config)#
```

The following example shows how to remove the hostname:

```
Sandbox(config)# no hostname
WAE-511(config)#
```

---

|                         |  |
|-------------------------|--|
| <b>Related Commands</b> | <a href="#">dnslookup</a><br><a href="#">(config) ip</a><br><a href="#">(config-if) ip</a> |
|-------------------------|--|

**show hosts**

(config) inetd

## (config) inetd

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}

no inetd enable {ftp | rcp}
```

|                           |                       |
|---------------------------|-----------------------|
| <b>Syntax Description</b> |                       |
| <b>enable</b>             | Enables services.     |
| <b>ftp</b>                | Enables FTP services. |
| <b>rcp</b>                | Enables RCP services. |

---

**Defaults** FTP is enabled; RCP is disabled.

---

**Command Modes** global configuration

---

**Device Modes** application-accelerator  
central-manager

---

**Usage Guidelines** Inetd (an Internet daemon) 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 shows how to enable an FTP service session on the WAAS device:

```
WAE(config)# inetd enable ftp
```

The following example shows how to disable FTP services:

```
WAE(config)# no inetd enable ftp
```

---

**Related Commands** [show inetd](#)

## (config) inline vlan-id-connection-check

To enable VLAN ID checking on intercepted traffic, use the **inline vlan-id-connection-check** global configuration command. To disable VLAN ID checking, use the **no** form of this command.

**inline vlan-id-connection-check**

**no inline vlan-id-connection-check**

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

**Defaults** VLAN ID checking is enabled.

**Command Modes** global configuration

**Device Modes** application-accelerator  
central-manager

**Examples** The following example shows how to enable VLAN ID checking of the intercepted traffic on the WAAS device:

```
WAE(config)# inline vlan-id-connection-check
```

The following example shows how to disable VLAN ID checking:

```
WAE(config)# no inline vlan-id-connection-check
```

**Related Commands** [\(config\) interface GigabitEthernet](#)  
[\(config-if\) encapsulation dot1Q](#)

(config) interface GigabitEthernet

# (config) interface GigabitEthernet

To configure a Gigabit Ethernet 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 1 [primary]]
```

```
no 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 1 [primary]]
```

## Syntax Description

|  |  |
|--|--|
| <b>GigabitEthernet</b>   | Selects a Gigabit Ethernet interface to configure (slot and port number).  |
| <i>slot/port</i>   | 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 (/).  |
| <b>autosense</b>   | (Optional) Sets the GigabitEthernet interface to automatically sense the interface speed.  |
| <b>bandwidth</b>   | (Optional) Sets the bandwidth of the specified interface.  |
| <b>10</b>  | Sets the bandwidth of the interface to 10 megabits per second (Mbps).  |
| <b>100</b>   | Sets the bandwidth of the interface to 100 Mbps.   |
| <b>1000</b>  | Sets the bandwidth of the interface to 1000 Mbps. This option is not available on all ports and is the same as autosense.  |
| <b>cdp enable</b>  | (Optional) Enables Cisco Discovery Protocol (CDP) on the specified interface.  |
| <b>channel-group 1</b>   | (Optional) Assigns the interface EtherChannel to group 1.  |
| <b>description</b> <i>text</i>   | Enters a description of the interface.   |
| <b>full-duplex</b>   | (Optional) Sets the interface to full-duplex operation.  |
| <b>half-duplex</b>   | (Optional) Sets the interface to half-duplex operation.  |
| <b>Note</b> We strongly recommend that you do not use half duplex on the WAE, routers, switches, or other devices. |  |
| <b>ip</b>  | (Optional) Enables IP configuration commands for the interface.  |
| <b>access-group</b>  | 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.                                       |

|  |   |
|--|---|
| <b>in</b>                                | Applies the specified ACL to inbound packets on the current interface.  |
| <b>out</b>                               | Applies the specified ACL to outbound packets on the current interface.   |
| <b>address</b> <i>ip-address netmask</i> | Sets the interface IP address and netmask.  |
| <b>secondary</b>                         | (Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address. |
| <b>dhcp</b>                              | (Optional) Sets the IP address to the address that is negotiated over Dynamic Host Configuration Protocol (DHCP).   |
| <b>client-id</b> <i>id</i>               | (Optional) Specifies the client identifier.   |
| <b>hostname</b> <i>name</i>              | (Optional) Specifies the hostname.  |
| <b>mtu</b> <i>mtusize</i>                | (Optional) Sets the interface Maximum Transmission Unit (MTU) size in bytes (88–1500).  |
| <b>shutdown</b>                          | (Optional) Shuts down this interface.   |
| <b>standby</b> <b>1</b>                  | (Optional) Sets the standby group number to 1.  |
| <b>primary</b>                           | (Optional) Sets this interface as the active interface in the standby group.  |

**Defaults**

The first attached interface in a standby group is defined as the active interface. There are no other default behaviors or values.

**Command Modes**

global configuration

**Device Modes**

application-accelerator  
central-manager

**Usage Guidelines**

Although the CLI contains the **no interface** option, you cannot apply the **no** command to an interface. The software displays the following error message: Removing of physical interface is not permitted.

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, 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.

(config) interface GigabitEthernet



**Note** When you use the **ip address** command to change the IP address of an interface that has been shut down, it automatically brings up that interface by default.

### 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 they are configured on the same subnet.

You can assign up to four secondary addresses to an interface. These addresses become active only after you configure the primary address. 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. 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

When you configure a WAAS device initially, you can configure a static IP address or use 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.

You can enable an interface for DHCP 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. You can configure DHCP servers to identify the client identifier and the hostname that the WAAS device is sending and then send 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.

### Configuring a Standby Group

You can associate an interface with a standby group by using the **standby 1** interface configuration command. To make an interface the active interface in a standby group, use the **standby 1 primary** interface configuration command. If you have already associated an interface with a standby group but have not made it the primary interface, you cannot specify the command again to add the primary designation. First, remove the interface from the standby group, then reassign it, specifying the **primary** option at the same time.

A physical interface can be a member of a standby group or a port channel, but not both.

You cannot assign an IP address to both a standby group and a port channel. Only one virtual interface can be configured with an IP address.

### Examples

The following example shows how to configure 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 shows how to enable a shut down interface:

```
WAE(config)# no interface GigabitEthernet 1/0 shutdown
```

The following example shows how to create 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 shows how to remove 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 shows how to add 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 shows how to remove 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 shows how to assign a secondary IP address on a Gigabit Ethernet interface on a WAAS device:

```
WAE# configure
WAE(config)# interface GigabitEthernet 1/0
WAE(config-if)# ip address 10.10.10.10 255.0.0.0 secondary
```

```
■ (config) interface GigabitEthernet
```

The following example shows how to configure a description for a Gigabit Ethernet interface:

```
WAE(config)# interface GigabitEthernet 1/0
WAE(config-if)# description This is a GigabitEthernet interface.
```

---

**Related Commands**

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

# (config) interface InlineGroup

To configure an InlineGroup 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 InlineGroup slot/grpnumber [autosense | bandwidth {10 | 100 | 1000} |
    failover timeout {1 | 3 | 5} | full-duplex | half-duplex | inline [vlan {all | native | vlan_list}] |
shutdown]

no 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]
```

| Syntax Description    |  |
|-----------------------|--|
| <b>InlineGroup</b>    | Sets the 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). |
| <b>slot/grpnumber</b> |  |
| <b>autosense</b>      | (Optional) Sets the Gigabit Ethernet interface to automatically sense the interface speed.   |
| <b>bandwidth</b>      | (Optional) Sets the bandwidth of the specified interface.  |
| <b>10</b>             | Sets the bandwidth of the interface to 10 megabits per second (Mbps).  |
| <b>100</b>            | Sets the bandwidth of the interface to 100 Mbps.   |
| <b>1000</b>           | Sets the bandwidth of the interface to 1000 Mbps. This option is not available on all ports and is the same as autosense.                                      |
| <b>failover</b>       | (Optional) Modifies failover parameters.   |
| <b>timeout</b>        | (Optional) Sets the maximum time for the inline group of interfaces to transfer traffic to another port in the group after a failover event.                   |
| <b>1</b>              | Number of seconds before a failover occurs.  |
| <b>3</b>              | Number of seconds before a failover occurs.  |
| <b>5</b>              | Number of seconds before a failover occurs.  |
| <b>full-duplex</b>    | (Optional) Sets the interface to full duplex.  |
| <b>half-duplex</b>    | (Optional) Sets the interface to half duplex.  |
|                       | <b>Note</b> We strongly recommend that you do not use half duplex on the WAE, routers, switches, or other devices.   |
| <b>inline</b>         | (Optional) Enables inline interception for an InlineGroup of interfaces.   |
| <b>vlan</b>           | (Optional) Modifies the VLAN list parameters.  |
| <b>all</b>            | Applies the command to all tagged and untagged packets.  |
| <b>native</b>         | Specifies untagged packets.  |
| <b>vlan_list</b>      | Comma-separated list of VLAN IDs. Restricts the inline feature to the specified set of VLANs.  |
| <b>shutdown</b>       | (Optional) Shuts down this interface.  |

## Defaults

No default behavior or values.

(config) interface InlineGroup

**Command Modes** global configuration

**Device Modes** application-accelerator  
central-manager

**Usage Guidelines** 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 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 on the WAE, routers, switches, or other devices. Use of half-duplex impedes system 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.

**Related Commands** [show interface](#)

[show running-config](#)

[show startup-config](#)

# (config) interface PortChannel

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

```
interface PortChannel 1 [description text | ip {access-group {acl-num | acl_name} {in | out} | address ip-address netmask] | shutdown]
```

```
no interface PortChannel 1 [description text | ip {access-group {acl-num | acl_name} {in | out} | address ip-address netmask] | shutdown]
```

| Syntax Description               |  |
|----------------------------------|--|
| <b>PortChannel 1</b>             | Configures an EtherChannel.  |
| <b>description <i>text</i></b>   | (Optional) Enters a description of the interface.  |
| <b>ip</b>                        | (Optional) Enables IP configuration commands for the interface.  |
| <b>access-group</b>              | Configures access control for IP packets on this interface using an 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.   |
| <b>in</b>                        | Applies the specified ACL to inbound packets on the current interface.   |
| <b>out</b>                       | Applies the specified ACL to outbound packets on the current interface.  |
| <b>address <i>ip-address</i></b> | Sets the interface IP address and netmask.   |
| <i>netmask</i>                   |  |
| <b>shutdown</b>                  | (Optional) Shuts down this interface.  |
| <b>Defaults</b>                  | No default behavior or values.   |
| <b>Command Modes</b>             | global configuration   |
| <b>Device Modes</b>              | application-accelerator<br>central-manager   |
| <b>Usage Guidelines</b>          | 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 the current link status of each interface. You must configure EtherChannel on the switch or router if you configure it on the WAE.<br><br>You cannot remove an EtherChannel that is configured as the primary interface on a WAE. |

(config) interface PortChannel



**Note** You cannot use the inline Ethernet interfaces that are located on the WAE inline network adapter to form an EtherChannel.



**Note** No two interfaces can have IP addresses in the same subnet.

**Examples**

The following example shows how to create 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 shows how to remove 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
```

**Related Commands**

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

# (config) interface standby

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

**interface Standby 1 {description *text* | ip address *ip\_address netmask* | shutdown}**

**no interface Standby 1 {description *text* | ip address *ip\_address netmask* | shutdown}**

| Syntax Description |  |
|--------------------|--|
|                    | <b>Standby 1</b> Configures a standby interface.   |
|                    | <b>description <i>text</i></b> Enters a description of the interface.                              |
|                    | <b>ip address <i>ip_address netmask</i></b> Specifies the IP address and netmask of the interface. |
|                    | <b>shutdown</b> Shuts down this interface.   |

|          |                                |
|----------|--------------------------------|
| Defaults | No default behavior or values. |
|----------|--------------------------------|

|               |                      |
|---------------|----------------------|
| Command Modes | global configuration |
|---------------|----------------------|

|              |  |
|--------------|--|
| Device Modes | application-accelerator<br>central-manager |
|--------------|--|

|                  |  |
|------------------|--|
| Usage Guidelines | A standby interface cannot be removed if it is configured as the system primary interface. |
|------------------|--|



No two interfaces can have IP addresses in the same subnet.

|                  |  |
|------------------|--|
| Related Commands | <a href="#">show interface</a><br><a href="#">show running-config</a><br><a href="#">show startup-config</a> |
|------------------|--|

(config) ip

## (config) ip

To change the 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 | domain-name name1 name2 name3 |
      ip host hostname ip-address | ip name-server ip-addresses |
      ip path-mtu-discovery enable | ip route dest_addrs net_addrs gateway_addrs }

no ip { default-gateway ip-address | domain-name name1 name2 name3 |
        ip host hostname ip-address | ip name-server ip-addresses |
        ip path-mtu-discovery enable | ip route dest_addrs net_addrs gateway_addrs }
```

|                           |   |
|---------------------------|---|
| <b>Syntax Description</b> | <b>default-gateway</b> <i>ip-address</i> Specifies the IP address of the default gateway (if not routing IP).<br><b>domain-name</b> <i>name1</i> Specifies domain names (up to three can be specified).<br><i>name2 name3</i> |
|                           | <b>host</b> <i>hostname ip-address</i> Adds an entry to the /etc/hosts file on the device, mapping the specified hostname to the specified IP address of the host.  |
|                           | <b>name-server</b> <i>ip-addresses</i> Specifies the address of the name server and IP addresses of the name servers (up to a maximum of eight).  |
|                           | <b>path-mtu-discovery</b> Enables RFC 1191 Path Maximum Transmission Unit (MTU) discovery.<br><b>enable</b>   |
|                           | <b>route</b> <i>dest_addrs net_addrs</i> Specifies the net route (destination route address, netmask address, and gateway address).   |

**Defaults** No default behavior or values.

**Command Modes** global configuration

**Device Modes** application-accelerator  
central-manager

**Usage Guidelines** To define a default gateway, use the **ip default-gateway** command. You can only configure one default gateway. 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. You can enter up to three domain names. 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.

To add an entry to the /etc/hosts file on the device, mapping a hostname to an IP address, use the **ip host** command. A given hostname can be mapped only to a single IP address, while an IP address can have multiple hostnames mapped to it, each one through a separate issuance of this command. To remove the entry from the /etc/hosts file, use the **no** form of this command. You can use the **show hosts** EXEC command to display the contents of the /etc/hosts file.

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 autodiscovery discovers the MTU and automatically sets the correct value. Use the **ip path-mtu-discovery enable** command to start this autodiscovery utility. By default, this feature is enabled. When this feature is disabled, the sending device uses a packet size that is smaller than 576 bytes and the next hop MTU. Existing connections are not affected when this feature is turned on or off.

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 shows how to configure a default gateway for the WAAS device:

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

The following example shows how to configure 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 shows how to configure a default domain name for the WAAS device:

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

The following example shows how to add an entry to the /etc/hosts file on the WAAS device:

```
WAE(config)# ip host corp-B7 10.11.12.140
```

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

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

---

**Related Commands**

[show hosts](#)

[show ip routes](#)

(config) ip access-list

## (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 command. To disable an access list, use the **no** form of this command.

**ip access-list {standard | extended} {acl-name | acl-num}**

**no ip access-list {standard | extended} {acl-name | acl-num}**

|                    |   |   |
|--------------------|---|---|
| Syntax Description | <b>standard</b><br><br><b>extended</b><br><br><i>acl-name</i><br><br><i>acl-num</i> | <p>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:<br/>         WAE(config-std-nacl)#</p> <p>See the “<a href="#">Standard ACL Configuration Mode Commands</a>” 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)#.</p> <p>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:<br/>         WAE(config-ext-nacl) #</p> <p>See the “<a href="#">Extended ACL Configuration Mode Commands</a>” 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) #.</p> <p>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.</p> <p>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.</p> |
|--------------------|---|---|

### Defaults

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

### Command Modes

global configuration

### Device Modes

application-accelerator  
central-manager

**Usage Guidelines**

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, use the **exit** command at the ACL configuration mode prompt.

To create an entry, use a the **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. You must include at least one **permit** entry to create a valid access list.

**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.

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 limit 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 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:

```
...
!
interface GigabitEthernet 1/0
 ip address 10.1.1.50 255.255.0.0
```

■ **(config) ip access-list**

```
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 arp-cache](#)

[\(config-if\) 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 this command.

```
kerberos {local-realm kerberos-realm | realm {dns-domain | host} kerberos-realm |
           server kerberos-realm {hostname | ip-address} [port-number]}
```

```
no kerberos {local-realm kerberos-realm | realm {dns-domain | host} kerberos-realm |
              server kerberos-realm {hostname | ip-address} [port-number]}
```

| Syntax Description    | <b>local-realm</b><br><i>kerberos-realm</i> | Displays the default Kerberos realm (IP address or name in uppercase letters) for WAAS. Configures a switch to authenticate users defined in the Kerberos database. The default value is a null string. |
|-----------------------|---|---|
| <b>realm</b>          |   | Maps a hostname or DNS domain name to a Kerberos realm.   |
| <i>dns-domain</i>     |   | DNS domain name to map to the Kerberos realm.   |
|                       |   | <b>Note</b> The name must begin with a leading dot (.)  |
| <i>host</i>           |   | Host IP address or name to map to Kerberos host realm.  |
| <i>kerberos-realm</i> |   | Kerberos realm (IP address or name in uppercase letters). The default value is a null string.   |
| <b>server</b>         |   | Specifies the Key Distribution Center (KDC) to use in a given Kerberos realm and, optionally, the port number that 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.  |

|                 |  |
|-----------------|--|
| <b>Defaults</b> | kerberos-realm: NULL string<br>port-number: 88 |
|-----------------|--|

|                      |                      |
|----------------------|----------------------|
| <b>Command Modes</b> | global configuration |
|----------------------|----------------------|

|                     |  |
|---------------------|--|
| <b>Device Modes</b> | application-accelerator<br>central-manager |
|---------------------|--|

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

(config) kerberos



**Note** Your Windows domain server must have a Reverse DNS Zone configured for this command to execute successfully.

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. To disable access to the kernel debugger, use the **no** form of this command.

**kernel kdb**

**no kernel kdb**

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | This command has no arguments or keywords. |
|---------------------------|--|

|                 |   |
|-----------------|---|
| <b>Defaults</b> | The kernel debugger is disabled by default. |
|-----------------|---|

|                      |                      |
|----------------------|----------------------|
| <b>Command Modes</b> | global configuration |
|----------------------|----------------------|

|                     |  |
|---------------------|--|
| <b>Device Modes</b> | application-accelerator<br>central-manager |
|---------------------|--|

|                         |  |
|-------------------------|--|
| <b>Usage Guidelines</b> | Once enabled, kdb is automatically activated if kernel problems occur, or you can manually activate it from the local console for the WAAS device. 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 the **go** command 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 the **reboot** command, 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 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.

|                 |   |
|-----------------|---|
| <b>Examples</b> | The following example shows how to enable, and then disable, access to the kernel debugger: |
|-----------------|---|

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

|                         |                                       |
|-------------------------|---------------------------------------|
| <b>Related Commands</b> | <a href="#">(config) kernel kdump</a> |
|-------------------------|---------------------------------------|

---

```
(config) kernel kdump
```

## (config) kernel kdump

To enable the kernel crash dump mechanism, use the **kernel kdump enable** global configuration command. To disable the kernel crash dump mechanism, use the **no** form of this command.

**kernel kdump enable**

**no kernel kdump enable**

---

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

---

**Defaults** The kernel crash dump mechanism is enabled by default.

---

**Command Modes** global configuration

---

**Device Modes** application-accelerator  
central-manager

---

**Usage Guidelines** A kernel crash dump file is stored in the following disk location:  
*/local/local1/crash/timestamp/vmcore*

The analysis of the kernel crash dump file is stored in the following file:  
*/local/local1/crash/timestamp/analysis.txt*

---

**Examples** The following example shows how to enable, and then disable, the kernel crash dump mechanism:

```
WAE(config)# kernel kdump enable
WAE(config)# no kernel kdump enable
```

---

**Related Commands** [\(config\) kernel kdb](#)  
[show kdump](#)

## (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 this command.

**line console carrier-detect**

**no line console carrier-detect**

|                           |   |
|---------------------------|---|
| <b>Syntax Description</b> |   |
| <b>console</b>            | Configures the console terminal line settings.                                    |
| <b>carrier-detect</b>     | Sets the device to check the carrier detect signal before writing to the console. |

|                 |                                |
|-----------------|--------------------------------|
| <b>Defaults</b> | No default behavior or values. |
|-----------------|--------------------------------|

|                      |                      |
|----------------------|----------------------|
| <b>Command Modes</b> | global configuration |
|----------------------|----------------------|

|                     |  |
|---------------------|--|
| <b>Device Modes</b> | application-accelerator<br>central-manager |
|---------------------|--|

|                 |  |
|-----------------|--|
| <b>Examples</b> | The following example shows how to set the WAAS device to check for the carrier detect signal: |
|-----------------|--|

```
WAE(config)# line console carrier-detect
```

(config) logging console

# (config) logging console

To set system logging to console, use the **logging console** global configuration command. To disable logging functions, use the **no** form of this command.

**logging console {enable | priority *loglevel*}**

**no logging console {enable | priority *loglevel*}**

| Syntax Description      | <b>console</b> Sets system logging to a console.<br><b>enable</b> Enables system logging.<br><b>priority <i>loglevel</i></b> Sets which priority level messages to send. Use one of the following keywords: <ul style="list-style-type: none"> <li>• <b>alert</b>—Immediate action needed. Priority 1.</li> <li>• <b>critical</b>—Immediate action needed. Priority 2.</li> <li>• <b>debug</b>—Debugging messages. Priority 7.</li> <li>• <b>emergency</b>—System is unusable. Priority 0.</li> <li>• <b>error</b>—Error conditions. Priority 3.</li> <li>• <b>information</b>—Informational messages. Priority 6.</li> <li>• <b>notice</b>—Normal but significant conditions. Priority 5.</li> <li>• <b>warning</b>—Warning conditions. Priority 4.</li> </ul> |
|-------------------------|---|
| <b>Defaults</b>         | Logging: on<br>Priority of message for console: warning<br>Log file: /local1/syslog.txt   |
| <b>Command Modes</b>    | global configuration  |
| <b>Device Modes</b>     | application-accelerator<br>central-manager  |
| <b>Usage Guidelines</b> | Use the <b>logging</b> command to set specific parameters of the system log file.<br>You can configure logging to send various levels of messages to the console using the <b>logging console priority</b> option.  |
| <b>Examples</b>         | The following example shows how to send messages that have a priority code of “error” (Level 3) to the console:<br><pre>WAE(config)# logging console priority error</pre>   |

The following example shows how to disable sending of messages that have a priority code of “error” (Level 3) to the console:

```
WAE(config)# no logging console error
```

---

**Related Commands**

[clear arp-cache](#)

[show logging](#)

(config) logging disk

# (config) logging disk

To system logging to a disk file, use the **logging disk** global configuration command. To disable logging functions, use the **no** form of this command.

```
logging disk {enable | filename filename | priority loglevel | recycle size}
```

```
no logging disk {enable | filename filename | priority loglevel | recycle size}
```

| Syntax Description       |  |
|--------------------------|--|
| <b>disk</b>              | Sets system logging to a disk file.  |
| <b>enable</b>            | Enables system logging.  |
| <b>filename filename</b> | Sets the name of the syslog file.  |
| <b>priority loglevel</b> | Sets which priority level messages to send. Use one of the following keywords: <ul style="list-style-type: none"> <li>• <b>alert</b>—Immediate action needed. Priority 1.</li> <li>• <b>critical</b>—Immediate action needed. Priority 2.</li> <li>• <b>debug</b>—Debugging messages. Priority 7.</li> <li>• <b>emergency</b>—System is unusable. Priority 0.</li> <li>• <b>error</b>—Error conditions. Priority 3.</li> <li>• <b>information</b>—Informational messages. Priority 6.</li> <li>• <b>notice</b>—Normal but significant conditions. Priority 5.</li> <li>• <b>warning</b>—Warning conditions. Priority 4.</li> </ul> |
| <b>recycle size</b>      | Overwrites <i>syslog.txt</i> when it surpasses the recycle size (1000000–50000000 bytes).  |

|                 |  |
|-----------------|--|
| <b>Defaults</b> | Logging: on<br>Priority of message for disk log file: debug<br>Log file: /local1/syslog.txt<br>Log file recycle size: 10,000,000 bytes |
|-----------------|--|

|                      |                      |
|----------------------|----------------------|
| <b>Command Modes</b> | global configuration |
|----------------------|----------------------|

|                     |  |
|---------------------|--|
| <b>Device Modes</b> | application-accelerator<br>central-manager |
|---------------------|--|

|                         |   |
|-------------------------|---|
| <b>Usage Guidelines</b> | Use the <b>logging</b> command to set specific parameters of the system log file. |
|-------------------------|---|

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.

---

**Examples**

The following example shows how to send messages that have a priority code of “error” (Level 3) to a file:

```
WAE(config)# logging disk priority error
```

---

**Related Commands**

[clear arp-cache](#)  
[show logging](#)

■ (config) logging facility

# (config) logging facility

To set the facility parameter for system logging, use the **logging facility** global configuration command. To disable logging functions, use the **no** form of this command.

**logging facility** *facility*

**no logging facility** *facility*

---

|                           |                                 |  |
|---------------------------|---------------------------------|--|
| <b>Syntax Description</b> | <b>facility</b> <i>facility</i> | Sets the facility parameter for syslog messages. Use one of the following keywords:  |
|                           |                                 | <ul style="list-style-type: none"> <li>• <b>auth</b>—Authorization system</li> <li>• <b>daemon</b>—System daemons</li> <li>• <b>kernel</b>—Kernel</li> <li>• <b>local0</b>—Local use</li> <li>• <b>local1</b>—Local use</li> <li>• <b>local2</b>—Local use</li> <li>• <b>local3</b>—Local use</li> <li>• <b>local4</b>—Local use</li> <li>• <b>local5</b>—Local use</li> <li>• <b>local6</b>—Local use</li> <li>• <b>local7</b>—Local use</li> <li>• <b>mail</b>—Mail system</li> <li>• <b>news</b>—USENET news</li> <li>• <b>syslog</b>—Syslog itself</li> <li>• <b>user</b>—User process</li> <li>• <b>uucp</b>—UUCP system</li> </ul> |

---

**Defaults** Logging: on

**Command Modes** global configuration

**Device Modes** application-accelerator  
central-manager

**Examples** The following example shows how to set the facility parameter to authorization system for syslog messages:

```
WAE(config)# logging facility auth
```

**Related Commands**

[clear arp-cache](#)  
[show logging](#)

(config) logging host

# (config) logging host

To configure system logging to a remote host, use the **logging host** global configuration command. To disable logging functions, use the **no** form of this command.

```
logging host {hostname | ip-address} [port port_num | priority loglevel | rate-limit message_rate]
```

```
no logging host {hostname | ip-address} [port port_num | priority loglevel | rate-limit  
message_rate]
```

| Syntax Description                       |  |
|--|--|
| <b>host</b>                              | Sets system logging to a remote host.  |
| <i>hostname</i>                          | Hostname of the remote syslog host. Specify up to four remote syslog hosts.<br><br><b>Note</b> To specify more than one syslog host, use multiple command lines; specify one host per command.   |
| <i>ip-address</i>                        | IP address of the remote syslog host. Specify up to four remote syslog hosts.<br><br><b>Note</b> To specify more than one syslog host, use multiple command lines; specify one host per command.   |
| <b>port port_num</b>                     | (Optional) Specifies the port to be used when logging to a host. The default port is 514.  |
| <b>priority loglevel</b>                 | Sets which priority level messages to send. Use one of the following keywords: <ul style="list-style-type: none"> <li>• <b>alert</b>—Immediate action needed. Priority 1.</li> <li>• <b>critical</b>—Immediate action needed. Priority 2.</li> <li>• <b>debug</b>—Debugging messages. Priority 7.</li> <li>• <b>emergency</b>—System is unusable. Priority 0.</li> <li>• <b>error</b>—Error conditions. Priority 3.</li> <li>• <b>information</b>—Informational messages. Priority 6.</li> <li>• <b>notice</b>—Normal but significant conditions. Priority 5.</li> <li>• <b>warning</b>—Warning conditions. Priority 4.</li> </ul> |
| <b>rate-limit</b><br><i>message_rate</i> | (Optional) Sets the rate limit (in messages per second) for sending messages to a host. Rate limit is 0-10000 (in messages per second). Setting the rate limit to 0 disables rate limiting.  |

|                      |  |
|----------------------|--|
| <b>Defaults</b>      | Logging: on<br>Priority of message for a host: warning |
| <b>Command Modes</b> | global configuration                                   |
| <b>Device Modes</b>  | application-accelerator<br>central-manager             |

**Usage Guidelines**

Use the **logging** command to set specific parameters of the system log file.

To configure the WAAS device to send varying levels of event messages to an external syslog host, use the **logging host** option.

You can configure a WAAS device to send varying levels of messages to up to four remote syslog hosts using the **logging host hostname** command.

**Examples**

The following example shows how 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 arp-cache](#)

[show logging](#)

(config) ntp

## (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]
```

```
no 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]
```

|                                   |  |
|-----------------------------------|--|
| <b>Syntax Description</b>         |  |
| <b>authenticate</b>               | (Optional) Authenticates the NTP server.   |
| <b>authentication-key</b>         | (Optional) Sets the NTP authentication key value. Must be from 0 to 4294967295.                  |
| <b>md5 encryption-type</b>        | (Optional) Sets the MD5 cryptographic hash function. The MD5 encryption type must be set to 0.   |
| <b>server</b>                     | (Optional) 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 that provides the clock synchronization (maximum of 4). |
| <i>hostnames</i>                  | (Optional) Hostname of the time server that provides the clock synchronization (maximum of 4).   |
| <b>server-with-authentication</b> | (Optional) Sets the authentication NTP server IP address for the WAAS device.                    |
| <b>key authentication-key</b>     | (Optional) Sets the NTP authentication key value. Must be from 0 to 4294967295.                  |

|                      |  |
|----------------------|--|
| <b>Defaults</b>      | The default NTP version number is 3.       |
| <b>Command Modes</b> | global configuration                       |
| <b>Device Modes</b>  | application-accelerator<br>central-manager |

|   |   |
|---|---|
| <b>Usage Guidelines</b>   |   |
|  <b>Note</b> | Unexpected time changes can result in unexpected system behavior. We recommend reloading the system after enabling an NTP server. |

**Examples**

The following example shows how to specify 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
```

**clock**

**(config) clock**

**show clock**

**show ntp**

(config) policy-engine application classifier

# (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. 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}}}]

no policy-engine application classifier classifier-name
```

|                           |   |
|---------------------------|---|
| <b>Syntax Description</b> | <b>classifier classifier-name</b> Classifier name (up to 30 characters). The name must start with a letter representing the application class.<br><b>list</b> (Optional) Lists the conditions contained in the specified classifier.<br><b>match</b> (Optional) Specifies the criteria for matching traffic.<br><b>all</b> Matches any type of traffic.<br><b>dst</b> Specifies the criteria for identifying the destination host.<br><b>host hostname</b> Specifies the hostname of the system that is the source or destination of the traffic.<br><b>ip ip_address</b> Specifies the IP address of the system that is the source or destination of the traffic.<br><b>port</b> Specifies the criteria for identifying the port or ports used by the source or destination hosts.<br><b>eq port</b> Specifies the source or destination port number.<br><b>range port1 port2</b> Specifies a range of source or destination port numbers.<br><b>src</b> Specifies the criteria for identifying the source host. |
|---------------------------|---|

|                      |                      |
|----------------------|----------------------|
| <b>Command Modes</b> | global configuration |
|----------------------|----------------------|

|                     |                         |
|---------------------|-------------------------|
| <b>Device Modes</b> | application-accelerator |
|---------------------|-------------------------|

|                         |  |
|-------------------------|--|
| <b>Usage Guidelines</b> | 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 match conditions. |
|-------------------------|--|

You cannot delete a classifier if any policies are using it. When creating a new application classifier or adding an existing application classifier, the WAAS CLI enters into a submode allowing you to specify one or more conditions. However, if the condition specified matches an already existing condition in the classifier conditions list, no action is taken. You can delete a condition by using the **no** form of this command. When creating a new classifier, you must add at least one condition.



|             |  |
|-------------|--|
| <b>Note</b> | 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*.



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](#)  
[\(config\) 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

# (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} [accelerate {cifs | http | mapi | MS-port-mapper | nfs | video}] [set-dscp dscp-marking] |  
  
    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} [accelerate {cifs | http | mapi | MS-port-mapper | nfs | video}] [set-dscp dscp-marking]}  
  
no policy-engine application map adaptor EPM epm-map disable line-number
```

| Syntax Description |  |   |
|--------------------|--|---|
|                    | <b>EPM</b> <i>epm-map</i>                | Specifies the messaging Application Programming Interface (MAPI) or Universal Unique ID (UUID). |
|                    | <b>delete</b> <i>line-number</i>         | Deletes the application policy map specified by the line number.                                |
|                    | <b>disable</b> <i>line-number</i>        | Disables the application policy map specified by the line number.                               |
|                    | <b>insert</b>                            | Inserts or adds a new policy map at the specified position.                                     |
|                    | <b>first</b>                             | Inserts the new application policy map at the beginning of the list.                            |
|                    | <b>last</b>                              | Inserts the new application policy map at the end of the list.                                  |
|                    | <b>pos</b> <i>line-number</i>            | Inserts the new application policy map at the specified line number.                            |
|                    | <b>name</b> <i>app-name</i>              | Specifies the name of the application.  |
|                    | <b>All</b>                               | Specifies all traffic.  |
|                    | <b>classifier</b> <i>classifier-name</i> | Specifies the name of the application traffic classifier.                                       |
|                    | <b>disable</b>                           | (Optional) Disables optimization or pass through.   |
|                    | <b>action</b>                            | Specifies whether to optimize the traffic or let it pass through.                               |
|                    | <b>optimize</b>                          | Applies general optimization.   |
|                    | <b>DRE</b>                               | Enables or disables DRE optimization.   |
|                    | <b>yes</b>                               | Enables DRE optimization.   |
|                    | <b>no</b>                                | Disables DRE optimization.  |
|                    | <b>compression</b>                       | Applies Lempel-Ziv (LZ) compression or no compression.  |

|                              |  |
|------------------------------|--|
| <b>LZ</b>                    | Applies LZ compression.  |
| <b>none</b>                  | Applies no compression.  |
| <b>full</b>                  | Applies full generic optimization.   |
| <b>pass-through</b>          | Allows traffic to pass through without any optimization.   |
| <b>accelerate</b>            | (Optional) Accelerates the traffic using a special adapter.  |
| <b>cifs</b>                  | Accelerates the traffic using the CIFS accelerator.  |
| <b>http</b>                  | Accelerates the traffic using the HTTP accelerator.  |
| <b>mapi</b>                  | Accelerates the traffic using the MAPI accelerator.  |
| <b>MS-port-mapper</b>        | Accelerates the traffic using the Microsoft EndPoint Port Mapper (EPM).  |
| <b>nfs</b>                   | Accelerates the traffic using the NFS accelerator.   |
| <b>video</b>                 | Accelerates the traffic using the video accelerator.   |
| <b>set-dscp dscp-marking</b> | (Optional) Sets the DSCP marking value (Table 3-2) to be applied to the traffic classified in the policy. Applies only if the action includes the <b>optimize</b> or <b>accelerate</b> keywords. |
| <b>list</b>                  | Lists the specified application policy maps.   |
| <b>from line-number</b>      | (Optional) Specifies the line number of the first application policy map to list.  |
| <b>to line-number</b>        | (Optional) Specifies the line number of the last application policy map to list.   |
| <b>move</b>                  | Moves the specified application policy map from one line to another.   |

**Command Modes** global configuration

**Device Modes** application-accelerator

**Usage Guidelines**

 **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](#)  
[\(config\) policy-engine application map other optimize DRE](#)  
[\(config\) policy-engine application map other optimize full](#)  
[\(config\) policy-engine application name](#)  
[\(config\) policy-engine application set-dscp](#)

(config) policy-engine application map adaptor WAFS transport

## (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}  
        [accelerate {cifs | http | mapi | MS-port-mapper | nfs | video}] [set-dscp dscp-marking] |  
  
    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} [accelerate {cifs | http | mapi |  
        MS-port-mapper | nfs | video}] [set-dscp dscp-marking]}  
  
no policy-engine application map adaptor WAFS transport disable line-number
```

| Syntax Description                       |  |  |
|--|--|--|
| <b>delete</b> <i>line-number</i>         | Deletes the application policy map specified by the line number.     |  |
| <b>disable</b> <i>line-number</i>        | Disables the application policy map specified by the line number.    |  |
| <b>insert</b>                            | Inserts or adds a new policy map at the specified position.          |  |
| <b>first</b>                             | Inserts the new application policy map at the beginning of the list. |  |
| <b>last</b>                              | Inserts the new application policy map at the end of the list.       |  |
| <b>pos</b> <i>line-number</i>            | Inserts the new application policy map at the specified line number. |  |
| <b>name</b> <i>app-name</i>              | Specifies the name of the application.                               |  |
| <b>All</b>                               | Specifies all traffic.   |  |
| <b>classifier</b> <i>classifier-name</i> | Specifies the name of the application traffic classifier.            |  |
| <b>disable</b>                           | (Optional) Disables optimization or pass through.                    |  |
| <b>action</b>                            | Specifies whether to optimize the traffic or let it pass through.    |  |
| <b>optimize</b>                          | Applies general optimization.  |  |
| <b>DRE</b>                               | Enables or disables DRE optimization.                                |  |
| <b>yes</b>                               | Enables DRE optimization.  |  |
| <b>no</b>                                | Disables DRE optimization.   |  |
| <b>compression</b>                       | Applies Lempel-Ziv (LZ) compression or no compression.               |  |
| <b>LZ</b>                                | Applies LZ compression.  |  |
| <b>none</b>                              | Applies no compression.  |  |
| <b>full</b>                              | Applies full generic optimization.                                   |  |
| <b>pass-through</b>                      | Allows traffic to pass through without any optimization.             |  |

|                              |   |
|------------------------------|---|
| <b>accelerate</b>            | (Optional) Accelerates the traffic using a special adapter.   |
| <b>cifs</b>                  | Accelerates the traffic using the CIFS accelerator.   |
| <b>http</b>                  | Accelerates the traffic using the HTTP accelerator.   |
| <b>mapi</b>                  | Accelerates the traffic using the MAPI accelerator.   |
| <b>MS-port-mapper</b>        | Accelerates the traffic using the Microsoft EndPoint Port Mapper (EPM).   |
| <b>nfs</b>                   | Accelerates the traffic using the NFS accelerator.  |
| <b>video</b>                 | Accelerates the traffic using the video accelerator.  |
| <b>set-dscp dscp-marking</b> | Sets the DSCP marking value ( <a href="#">Table 3-2</a> ) to be applied to the traffic classified in the policy. Applies only if the action includes the <b>optimize</b> or <b>accelerate</b> keywords. |
| <b>list</b>                  | Lists the specified application policy maps.  |
| <b>from line-number</b>      | (Optional) Specifies the line number of the first application policy map to list.   |
| <b>to line-number</b>        | (Optional) Specifies the line number of the last application policy map to list.  |
| <b>move</b>                  | Moves the specified application policy map from one line to another.  |

**Command Modes** global configuration

**Device Modes** application-accelerator

**Usage Guidelines**  **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](#)
- [\(config\) 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 set-dscp](#)

(config) policy-engine application map basic

# (config) policy-engine application map basic

To configure the application policy with the basic policy map, use the **policy-engine application map basic** global configuration command. To disable the EPM service in the application policy configuration, use the **no** form of this command.

```
policy-engine application map basic {
    delete line-number |
    disable line-number |
    insert {first | last | pos line-number} name app-name classifier classifier-name [disable]
        action {optimize {DRE {yes | no} compression {LZ | none} | full} | pass-through}
        [accelerate {cifs | http | mapi | MS-port-mapper | nfs | video}] [set-dscp dscp-marking] |
    list [from line-number [to line-number] | to line-number [from line-number]] |
    move from line-number to line-number |
    name app-name classifier classifier-name {[disable] action {optimize {DRE {yes | no} compression {LZ | none} | full} | pass-through} [accelerate {cifs | http | mapi | MS-port-mapper | nfs | video}] [set-dscp dscp-marking]}}
no policy-engine application map basic disable line-number
```

| Syntax Description                       |  |  |
|--|--|--|
| <b>delete</b> <i>line-number</i>         |  | Deletes the application policy map specified by the line number.     |
| <b>disable</b> <i>line-number</i>        |  | Disables the application policy map specified by the line number.    |
| <b>insert</b>                            |  | Inserts or adds a new policy map at the specified position.          |
| <b>first</b>                             |  | Inserts the new application policy map at the beginning of the list. |
| <b>last</b>                              |  | Inserts the new application policy map at the end of the list.       |
| <b>pos</b> <i>line-number</i>            |  | Inserts the new application policy map at the specified line number. |
| <b>name</b> <i>app-name</i>              |  | Specifies the name of the application traffic classifier.            |
| <b>classifier</b> <i>classifier-name</i> |  | Specifies the name of the application traffic classifier.            |
| <b>disable</b>                           |  | (Optional) Disables optimization or pass-through.                    |
| <b>action</b>                            |  | Specifies whether to optimize the traffic or let it pass through.    |
| <b>optimize</b>                          |  | Applies general optimization.  |
| <b>DRE</b>                               |  | Enables or disables DRE optimization.                                |
| <b>yes</b>                               |  | Enables DRE optimization.  |
| <b>no</b>                                |  | Disables DRE optimization.   |
| <b>compression</b>                       |  | Applies Lempel-Ziv (LZ) compression or no compression.               |
| <b>LZ</b>                                |  | Applies LZ compression.  |
| <b>none</b>                              |  | Applies no compression.  |
| <b>full</b>                              |  | Applies full generic optimization.                                   |
| <b>pass-through</b>                      |  | Allows traffic to pass through without any optimization.             |
| <b>accelerate</b>                        |  | (Optional) Accelerates the traffic using a special adapter.          |

|                              |  |
|------------------------------|--|
| <b>cifs</b>                  | Accelerates the traffic using the CIFS accelerator.  |
| <b>http</b>                  | Accelerates the traffic using the HTTP accelerator.  |
| <b>mapi</b>                  | Accelerates the traffic using the MAPI accelerator.  |
| <b>MS-port-mapper</b>        | Accelerates the traffic using the Microsoft EndPoint Port Mapper (EPM).  |
| <b>nfs</b>                   | Accelerates the traffic using the NFS accelerator.   |
| <b>video</b>                 | Accelerates the traffic using the video accelerator.   |
| <b>set-dscp dscp-marking</b> | (Optional) Sets the DSCP marking value (Table 3-2) to be applied to the traffic classified in the policy. Applies only if the action includes the <b>optimize</b> or <b>accelerate</b> keywords. |
| <b>list</b>                  | Lists the specified application policy maps.   |
| <b>from line-number</b>      | (Optional) Specifies the line number of the first application policy map to list.  |
| <b>to line-number</b>        | (Optional) Specifies the line number of the last application policy map to list.   |
| <b>move</b>                  | Moves the specified application policy map from one line to another.   |

**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.

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.

To view WAFS dynamic accept or deny list entries, use the **show policy-engine application dynamic** command.



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](#)
- [\(config\) 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
```

**show policy-engine application**

# (config) policy-engine application map other optimize DRE

To configure the **optimize DRE** action on nonclassified 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}
[set-dscp dscp-marking]
```

| Syntax Description           |   |
|------------------------------|---|
| <b>yes</b>                   | Applies the <b>optimize DRE</b> action on nonclassified traffic.  |
| <b>no</b>                    | Specifies not to apply the <b>optimize DRE</b> action on nonclassified traffic.   |
| <b>compression</b>           | Applies the specified compression.  |
| <b>LZ</b>                    | Applies the Lempel-Ziv (LZ) compression.  |
| <b>none</b>                  | Applies no compression.   |
| <b>set-dscp dscp-marking</b> | (Optional) Sets the DSCP marking value ( <a href="#">Table 3-2</a> ) to be applied to the traffic classified in the policy. |

**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.



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](#)
- [\(config\) policy-engine application map other optimize full](#)
- [\(config\) policy-engine application map other pass-through](#)

■ (config) policy-engine application map other optimize DRE

(config) policy-engine application name  
(config) policy-engine application set-dscp

# (config) policy-engine application map other optimize full

To configure the application policy on nonclassified 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 [set-dscp dscp-marking]**

|  |  |
|--|--|
| <b>Syntax Description</b>  | <b>set-dscp dscp-marking</b> (Optional) Sets the DSCP marking value ( <a href="#">Table 3-2</a> ) to be applied to the traffic classified in the policy.   |
| <b>Command Modes</b>   | global configuration   |
| <b>Device Modes</b>  | application-accelerator  |
| <b>Usage Guidelines</b>  | Use the <b>policy-engine application map other optimize full</b> global configuration command to configure the application policy on nonclassified traffic with the <b>optimize full</b> action.   |
|  <b>Note</b> | 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> .   |
| <b>Related Commands</b>  | <a href="#">(config) policy-engine application classifier</a><br><a href="#">(config) policy-engine application map adaptor EPM</a><br><a href="#">(config) policy-engine application map adaptor WAFS transport</a><br><a href="#">(config) policy-engine application map basic</a><br><a href="#">(config) policy-engine application map other optimize DRE</a><br><a href="#">(config) policy-engine application map other pass-through</a><br><a href="#">(config) policy-engine application name</a><br><a href="#">(config) policy-engine application set-dscp</a> |

```
■ (config) policy-engine application map other pass-through
```

## (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**

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

**Defaults** No default behavior or values.

**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](#)
- [\(config\) 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 [set-dscp dscp-marking]**

**no policy-engine application name app-name [set-dscp dscp-marking]**

| Syntax Description | <b>application name</b> <i>app-name</i> Application name (up to 30 characters). The name cannot contain spaces or special characters. Specify the reserved name Other to set the DSCP marking value on nonclassified traffic. |
|--------------------|---|
|                    | <b>set-dscp dscp-marking</b> (Optional) Sets the DSCP marking value ( <a href="#">Table 3-2</a> ) to be applied to the application traffic.   |

**Defaults** No default behavior or values.

**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 or to apply a DSCP marking value to the application traffic. You cannot delete an application name if other policies are using this name. Successful deletion clears all statistics that were once associated with this application.



**Note** There is a limitation of 255 different application names.

You cannot delete the application definition named Other.

A DSCP value that you specify in the **policy-engine application name** command applies to all traffic associated with the application, unless it is overridden by a DSCP marking value that you specify in a specific map by one of the **policy-engine application map** commands. If a DSCP marking value is not assigned or defined, the default DSCP marking value (defined by the **policy-engine application set-dscp** command) is applied to traffic.



**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:

■ (config) policy-engine application name

```
WAE(config)# policy-engine application name Payroll
```

The following example shows how to assign a DSCP marking value to traffic associated with the Payroll application:

```
WAE(config)# policy-engine application name Payroll set-dscp cs1
```

---

**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
- (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 set-dscp

To set the default DSCP marking value for use with applications, use the **policy-engine application set-dscp** global configuration command. To set the default DSCP marking value to its default value, use the **no** form of this command.

**policy-engine application set-dscp *dscp-marking***

**no policy-engine application set-dscp *dscp-marking***

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | <b>set-dscp <i>dscp-marking</i></b> Specifies the DSCP marking value, as shown in <a href="#">Table 3-2</a> .  |
| <b>Defaults</b>           | No default behavior or values.   |
| <b>Command Modes</b>      | global configuration   |
| <b>Device Modes</b>       | application-accelerator  |
| <b>Usage Guidelines</b>   | <p>The DSCP field in an IP packet enables different levels of service to be assigned to network traffic. Levels of service are assigned by marking each packet on the network with a DSCP code. DSCP is the combination of IP Precedence and Type of Service (ToS) fields. For more information, see RFC 2474.</p> <p>A DSCP value is assigned in an application definition or an application policy map and applies to all traffic associated with the application or policy map. If a DSCP value is not assigned or defined, the default DSCP value is applied to traffic. The global default DSCP value is copy, which copies the DSCP value from the incoming packet and uses it for the outgoing packet.</p> <p><a href="#">Table 3-2</a> lists the valid DSCP marking values that you can specify.</p> |

**Table 3-2 DSCP Marking Values**

| DSCP Code | Description                                    |
|-----------|--|
| 0 - 63    | Sets packets with a numeric dscp from 0 to 63. |
| af11      | Sets packets with AF11 dscp (001010).          |
| af12      | Sets packets with AF11 dscp (001100).          |
| af13      | Sets packets with AF13 dscp (001110).          |
| af21      | Sets packets with AF21 dscp (010010).          |
| af22      | Sets packets with AF22 dscp (010100).          |
| af23      | Sets packets with AF23 dscp (010110).          |
| af31      | Sets packets with AF31 dscp (011010).          |
| af32      | Sets packets with AF32 dscp (011100).          |
| af33      | Sets packets with AF33 dscp (011110).          |
| af41      | Sets packets with AF41 dscp (100010).          |
| af42      | Sets packets with AF42 dscp (100100).          |

---

```
(config) policy-engine application set-dscp
```

**Table 3-2 DSCP Marking Values (continued)**

| DSCP Code | Description  |
|-----------|--|
| af43      | Sets packets with AF43 dscp (100110).  |
| cs1       | Sets packets with CS1 (precedence 1) dscp (001000).                              |
| cs2       | Sets packets with CS2 (precedence 2) dscp (010000).                              |
| cs3       | Sets packets with CS3 (precedence 3) dscp (011000).                              |
| cs4       | Sets packets with CS4 (precedence 4) dscp (100000).                              |
| cs5       | Sets packets with CS5 (precedence 5) dscp (101000).                              |
| cs6       | Sets packets with CS6 (precedence 6) dscp (110000).                              |
| cs7       | Sets packets with CS7 (precedence 7) dscp (111000).                              |
| copy      | Copies the DSCP value from the incoming packet to the outgoing packet. (default) |
| default   | Sets packets with default dscp (000000).   |
| ef        | Sets packets with EF dscp (101110).  |

---

### Examples

The following example shows how to set the default DSCP marking value to copy:

```
WAE(config)# policy-engine application set-dscp copy
```

---

### Related Commands

[\(config\) policy-engine application name](#)

# (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}**

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | <b>remove-all</b> Removes the application policy configurations and resets other changed configurations.<br>Note: This does not apply to applications defined in the WAAS Central Manager, which are global, including the applications defined in device/device group level. They will be propagated to all devices that are registered with the Central Manager. |
| <b>Defaults</b>           | No default behavior or values.   |
| <b>Command Modes</b>      | global configuration   |
| <b>Device Modes</b>       | application-accelerator  |
| <b>Usage Guidelines</b>   | This action includes but is not limited to the following: <ul style="list-style-type: none"> <li>Remove all application names except “other.”</li> <li>Remove all classifiers.</li> <li>Remove all policy maps.</li> <li>Reset the default action to <b>pass-through</b>.</li> </ul>   |
| <b>Note</b>               | 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> .   |
| <b>Examples</b>           | The following example shows how to remove all application policy configurations on a WAE using the <b>policy-engine config</b> command:<br><pre>WAE#(config) policy-engine config remove-all</pre>   |
| <b>Related Commands</b>   | <a href="#">show policy-engine status</a>  |

■ (config) policy-engine config

```
show statistics auto-discovery  
show statistics connection closed
```

# (config) port-channel

To configure the port channel load-balancing options on a WAAS device, use the **port-channel** global configuration command. To set load balancing on the port channel to its default method, use the **no** form of this command.

**port-channel load-balance {src-dst-ip-port | round-robin}**

**no port-channel load-balance {src-dst-ip-port | round-robin}**

|                           |   |
|---------------------------|---|
| <b>Syntax Description</b> | <b>load-balance</b> Configures the load-balancing method.<br><b>src-dst-ip-port</b> Specifies the load-balancing method based on a combination of source and destination IP addresses/ports. This load-balancing method has replaced the dst-ip method on devices running WAAS version 4.1.3 or later.<br><b>round-robin</b> Specifies the load-balancing method using a round-robin resource allocation. |
|---------------------------|---|

**Defaults** Round-robin is the default load-balancing method.

**Command Modes** global configuration

**Device Modes** application-accelerator  
central-manager

**Usage Guidelines** The **port-channel load-balance** command configures one of two 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 shows how to configure IP load balancing on a port channel and then disable it:

```
WAE(config)# port-channel load-balance src-dst-ip-port
WAE(config)# no port-channel load-balance
```

(config) primary-interface

# (config) primary-interface

To configure the primary interface for a WAAS device, use the **primary-interface** global configuration command. To remove the configured primary interface, use the **no** form of this command.

```
primary-interface {GigabitEthernet 1-2/port | PortChannel 1| Standby 1| inlineGroup slot/grpnumber}
```

```
no primary-interface {GigabitEthernet 1-2/port | PortChannel 1 | Standby 1 | inlineGroup slot/grpnumber}
```

| Syntax Description                |  |
|-----------------------------------|--|
| <b>GigabitEthernet 1-2/port</b>   | Selects a Gigabit Ethernet interface as the primary interface of the WAAS device. Slot number 1 or 2 and port number.  |
| <b>PortChannel 1</b>              | Selects a port channel interface as the primary interface of the WAAS device. (Only one port channel interface is supported.)  |
| <b>Standby 1</b>                  | Selects a standby group as the primary interface of the WAAS device. (Only one standby group is supported.)  |
| <b>inlineGroup slot/grpnumber</b> | Selects an interface on the Cisco WAE Inline Network Adapter as the primary interface of the WAAS device. The group number for the inline feature is either 0 or 1 (each adapter has 2 grouped pairs). |

## Defaults

The default primary interface is the Gigabit Ethernet 1/0 interface. If this interface 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  
central-manager

**Usage Guidelines** You can change the primary interface 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 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
```

The following example shows how to specify the inline interface slot 1, group 0 as the primary interface on a WAAS device:

```
WAE(config)# primary-interface inlineGroup 1/0
```

---

**Related Commands**

[\(config\) interface GigabitEthernet](#)

(config) print-services

# (config) print-services

To enable print services and designate a group name for administrators who are 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}
```

```
no print-services {enable | admin-group admin-group-name | guest-print enable}
```

| Syntax Description | <b>enable</b> Enables print services on the WAAS device.<br><b>admin-group</b> Configures a group of administrators with print services configuration privileges. You can enter a maximum of 127 characters. No spaces are allowed.<br><b>guest-print enable</b> Enables the guest print service. Guest printing allows any user to print to the WAAS print server.<br><b>Note</b> This option is available only in the application-accelerator device mode. |
|--------------------|--|
|--------------------|--|

|                 |  |
|-----------------|--|
| <b>Defaults</b> | By default, print services are disabled and no administrative group is defined ( <i>admin-group-name</i> is null). |
|-----------------|--|

|                      |                      |
|----------------------|----------------------|
| <b>Command Modes</b> | global configuration |
|----------------------|----------------------|

|                     |  |
|---------------------|--|
| <b>Device Modes</b> | application-accelerator<br>central-manager |
|---------------------|--|

|                 |  |
|-----------------|--|
| <b>Examples</b> | The following example shows how to enable print services on a WAAS device: |
|-----------------|--|

```
WAE(config)# print-services enable
```

The following example shows how to add 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 service 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**

[show print-services](#)  
[show running-config](#)  
[show startup-config](#)

(config) radius-server

## (config) radius-server

To configure a set of RADIUS authentication server settings on the WAAS device, use the **radius-server** global configuration command. 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}
```

```
no radius-server {host hostname | hostipaddr [primary] | key keyword | retransmit retries | timeout seconds}
```

| Syntax Description        |   |
|---------------------------|---|
| <b>host hostname</b>      | Specifies a RADIUS server. You can have a maximum of 5 servers.   |
| <b>hostipaddr</b>         | IP address of the RADIUS server.  |
| <b>primary</b>            | (Optional) Sets the server as the primary server.   |
| <b>key keyword</b>        | Specifies the encryption key shared with the RADIUS servers. You can have a maximum of 15 characters.                 |
| <b>retransmit retries</b> | Specifies the number of transmission attempts (1–3) to an active server for a transaction. The default is 2.          |
| <b>timeout seconds</b>    | Specifies the time to wait for a RADIUS server to reply. The range is from 1 to 20 seconds. The default is 5 seconds. |

| Defaults | <b>retransmit retries:</b> 2<br><b>timeout seconds:</b> 5 |
|----------|---|
|----------|---|

| Command Modes | global configuration |
|---------------|----------------------|
|---------------|----------------------|

| Device Modes | application-accelerator<br>central-manager |
|--------------|--|
|--------------|--|

| Usage Guidelines | 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 <a href="#">(config) authentication configuration</a> command.) |
|------------------|--|
|------------------|--|

| Examples | The following example shows how to specify a RADIUS server, specify the RADIUS key, and accept retransmit defaults. You can verify the configuration using the <b>show radius-server</b> 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

## (config) smb-conf

To manually configure the parameters for a WAAS device 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]
no smb-conf section {global | print$ | printers} name attr-name value attr-value [service print]
```

| Syntax Description      |  |
|-------------------------|--|
| <b>global</b>           | Specifies one of the global print parameters.  |
| <b>print\$</b>          | Specifies one of the print\$ parameters.   |
| <b>printers</b>         | Specifies the parameters for one of the printers.  |
| <b>name attr-name</b>   | Specifies the name of the parameter in the specified section that you want to manually configure (up to 80 characters).  |
| <b>value attr-value</b> | Specifies the value of the parameter (up to 255 characters).   |
| <b>service print</b>    | (Optional) Updates the Samba configuration file for print services. Without this option, the <b>smb-conf</b> command updates the Samba configuration file that is used for windows authentication. |

See [Table 3-3](#) for a description of the parameters for the global, print\$, and printers, including the names and default values.

**Defaults** No default behavior or values.

**Command Modes** global configuration

**Device Modes** application-accelerator  
central-manager

**Usage Guidelines** The *smb.conf* file contains a variety of print-related parameters. Global parameters apply to the server. Service level parameters, which define default settings for all other sections and shares, allow you to avoid 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. Print\$ parameters apply to the printers. Printers parameters, which apply to the shares, make it possible to share all printers with a minimal configuration. These parameters apply as defaults to all printers.

[Table 3-3](#) describes the print-related parameters.

**Table 3-3 Print-Related Parameters**

| Parameter Name             | Default Value                                   | Parameter Description   |
|----------------------------|---|---|
| <b>global parameters</b>   |   |   |
| 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  | Parameter that does not enumerate domain users using MSRPC.   |
| winbind enum groups        | no  | Parameter that does not enumerate domain groups using MSRPC.  |
| winbind cache time         | 10  | Time that a domain user or group information remains in the cache before expiring.  |
| winbind use default domain | yes   | Use the default domain for users and groups.  |
| printcap name              | cups  | Use CUPS to determine available printer names.  |
| load printers              | yes   | Automatically creates all available printer shares.   |
| printing                   | cups  | Parameter that uses CUPS-compatible print commands.   |
| cups options               | raw   | Parameter that sets the format of the print output to raw.  |
| force printername          | yes   | Parameter that enforces the same printer name specified in the CUPS GUI to be used as the printer name in Samba.  |
| lpq cache time             | 0   | Cache time for the results of the <b>lpq</b> 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<br>SO_RCVBUF=8192<br>SO_SNDBUF=8192 | Controls on the network layer of the operating system that allows 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  | Parameter that sets <i>nmbd</i> to be a local master browser on a subnet.   |
| domain master              | no  | Parameter that sets <i>nmbd</i> to be a domain master browser for its given workgroup.  |
| preferred master           | no  | Parameter that sets <i>nmbd</i> to be a preferred master browser for its workgroup  |
| dns proxy                  | no  | DNS proxy that 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 the print server (or share) that is visible when a client queries the server. This parameter can also be set by the <b>windows-domain comment</b> command.                                    |

(config) smb-conf

**Table 3-3 Print-Related Parameters (continued)**

| Parameter Name  | Default Value | Parameter Description   |
|-----------------|---------------|---|
| netbios name    | MYFILEENGINE  | Name of the Samba server hosting print services. This parameter can also be set by the <b>windows-domain netbios-name</b> command.  |
| realm           | CISCO         | Active Directory domain name. Always uppercase. This parameter can also be set by the <b>windows-domain realm</b> command.  |
| wins server     | 10.10.10.1    | IP address of the Windows domain server used to authenticate user access to print services. This parameter can also be set by the <b>windows-domain wins-server</b> command.  |
| password server | 10.10.10.10   | Optional IP address of the password server used for authentication of users. This parameter can also be set by the <b>windows-domain password-server</b> command.   |
| security        | domain        | Use Windows domain server for authentication. This parameter can also be set by the <b>windows-domain security</b> 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. The 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                   | Parameter that does not require a password to connect to the printer.                   |
| browsable  | yes                   | Parameter that allows the printer to be visible in the list of printers.                |
| read only  | yes                   | Parameter that prevents users from creating or modifying the printer list.              |
| write list | root                  | Parameter that 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.  |
| browsable | no                        | Parameter that always sets to no if printable = yes. It makes the printer share invisible in the list of available shares. |
| guest ok  | yes                       | Parameter that does not require a password to connect to the printer's service.  |
| writable  | no                        | Parameter that prevents users from creating or modifying files in the print service directory.                             |

**Table 3-3 Print-Related Parameters (continued)**

| Parameter Name | Default Value | Parameter Description  |
|----------------|---------------|--|
| printable      | yes           | Parameter that 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          | Parameter that allows the print administrator (root user) to add drivers and to set the 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

## (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}**

**no snmp-server access-list {num | name}**

---

### Syntax Description

|             |  |
|-------------|--|
| <i>num</i>  | Standard access list number (1–99).                                |
| <i>name</i> | Standard access list name. You can use a maximum of 30 characters. |

---

### Defaults

No default behavior or values.

---

### Command Modes

global configuration

---

### Device Modes

application-accelerator  
central-manager

---

### Examples

The following example shows how to allow the SNMP agent to check against access control list 12 before accepting or dropping packets:

```
WAE(config)# snmp-server access-list 12
```



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**]

**no snmp-server community** *string* [**group** *groupname* | **rw**]

| Syntax Description |                               |  |
|--------------------|-------------------------------|--|
|                    | <b>string</b>                 | Community string that acts like a password and permits access to the SNMP agent. You can use up to a maximum of 64 characters. |
|                    | <b>group</b> <i>groupname</i> | (Optional) Specifies the group name to which the community string belongs. You can use a maximum of 64 characters.             |
|                    | <b>rw</b>                     | (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.

## Command Modes

global configuration

## Device Modes

application-accelerator  
central-manager

## Examples

The following example shows how to enable the SNMP agent and assign the community string comaccess to SNMP:

```
WAE(config)# snmp-server community comaccess
```

The following example shows how to disable the SNMP agent and remove 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](#)

```
■ (config) snmp-server community
```

```
    (config) snmp-server notify inform  
    (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*

**no snmp-server contact** *line*

|                           |   |
|---------------------------|---|
| <b>Syntax Description</b> | <b>contact</b> <i>line</i> Specifies the text for MIB-II object <i>sysContact</i> . This is the identification of the contact person for this managed node.   |
| <b>Command Modes</b>      | global configuration  |
| <b>Device Modes</b>       | application-accelerator<br>central-manager  |
| <b>Defaults</b>           | No system contact string is set.  |
| <b>Usage Guidelines</b>   | The system contact string is the value stored in the MIB-II system group <i>sysContact</i> object.  |
| <b>Examples</b>           | <p>The following example shows how to set a system contact string and then remove it:</p> <pre>WAE(config)# snmp-server contact Dial System Operator at beeper # 27345 WAE(config)# no snmp-server contact</pre>  |
| <b>Related Commands</b>   | <a href="#">(config) snmp-server community</a><br><a href="#">(config) snmp-server enable traps</a><br><a href="#">(config) snmp-server group</a><br><a href="#">(config) snmp-server host</a><br><a href="#">(config) snmp-server location</a><br><a href="#">(config) snmp-server mib</a><br><a href="#">(config) snmp-server notify inform</a><br><a href="#">(config) snmp-server user</a><br><a href="#">(config) snmp-server view</a><br><a href="#">snmp trigger</a> |

---

```
(config) snmp-server enable traps
```

## (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]]
```

```
snmp-server enable traps config | entity | event
```

```
snmp-server enable traps content-engine [disk-fail | disk-read | disk-write | overload-bypass |
    transaction-log]
```

```
snmp-server enable traps snmp [authentication | cold-start]
```

```
snmp-server enable traps wafs [cslog | eslog | mgrlog]
```

### Syntax Description

|                        |   |
|------------------------|---|
| <b>alarm</b>           | (Optional) Enables WAAS alarm traps.                  |
| <b>clear-critical</b>  | (Optional) Enables clear-critical alarm traps.        |
| <b>clear-major</b>     | (Optional) Enables clear-major alarm traps.           |
| <b>clear-minor</b>     | (Optional) Enables clear-minor alarm traps.           |
| <b>raise-critical</b>  | (Optional) Enables raise-critical alarm traps.        |
| <b>raise-major</b>     | (Optional) Enables raise-major alarm traps.           |
| <b>raise-minor</b>     | (Optional) Enables raise-minor alarm traps.           |
| <b>config</b>          | Enables CiscoConfigManEvent traps.                    |
| <b>entity</b>          | Enables SNMP entity traps.                            |
| <b>event</b>           | Enables Event MIB traps.                              |
| <b>content-engine</b>  | Enables SNMP WAAS traps.                              |
| <b>disk-fail</b>       | (Optional) Enables disk failure error traps.          |
| <b>disk-read</b>       | (Optional) Enables disk read error traps.             |
| <b>disk-write</b>      | (Optional) Enables disk write error traps.            |
| <b>overload-bypass</b> | (Optional) Enables WCCP overload bypass error traps.  |
| <b>transaction-log</b> | (Optional) Enables transaction log write error traps. |
| <b>snmp</b>            | (Optional) Enables SNMP-specific traps.               |
| <b>authentication</b>  | (Optional) Enables authentication traps.              |
| <b>cold-start</b>      | (Optional) Enables cold start traps.                  |
| <b>wafs</b>            | Enables all WAFS-specific traps.                      |
| <b>cslog</b>           | (Optional) Enables the CS log traps.                  |
| <b>eslog</b>           | (Optional) Enables the ES log traps.                  |
| <b>mgrlog</b>          | (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  
central-manager

**Usage Guidelines** In the WAAS software 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. You can enable or disable each of these six alarm traps through the WAAS CLI.

To configure traps, you must enter the **snmp-server enable traps** command. If you do not enter the **snmp-server enable traps** command, no traps are sent.

The **snmp-server enable traps** command is used with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP traps. To send traps, you must configure at least one host using the **snmp-server host** command.

To allow a host to receive a trap, you must enable both the **snmp-server enable traps** command and the **snmp-server host** command for that host.

You must enable SNMP with the **snmp-server community** command.

To disable the sending of the MIB-II SNMP authentication trap, you must enter the command **no snmp-server enable traps snmp authentication**.

## Examples

The following example shows how to enable 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 shows how to disable all traps:

```
WAE(config)# no snmp-server enable traps
```

```
■ (config) 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](#)
- (config) [snmp-server notify inform](#)
- (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]}{}

no snmp-server group name {v1 [notify name] [read name] [write name] |
v2c [notify name] [read name] [write name] |
v3 {auth [notify name] [read name] [write name] |
noauth [notify name] [read name] [write name] |
priv [notify name] [read name] [write name]}{}}
```

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> |  |
| <b>group name</b>         | Specifies the SNMP group. You can enter a maximum of 64 characters.  |
| <b>v1</b>                 | Specifies the group using the Version 1 Security Model.  |
| <b>notify name</b>        | (Optional) Specifies a notify view name for the group that enables you to specify a notify, inform, or trap. You can enter a maximum of 64 characters.                 |
| <b>read name</b>          | (Optional) Specifies a read view name for the group that enables you to view only the contents of the agent. You can enter a maximum of 64 characters.                 |
| <b>write</b>              | (Optional) Specifies a write view name for the group that enables you to enter data and configure the contents of the agent. You can enter a maximum of 64 characters. |
| <b>v2c</b>                | Specifies the group using the Version 2c Security Model.   |
| <b>v3</b>                 | Specifies the group using the User Security Model (SNMPv3).  |
| <b>auth</b>               | Specifies the group using the AuthNoPriv Security Level.   |
| <b>noauth</b>             | Specifies the group using the noAuthNoPriv Security Level.   |
| <b>priv</b>               | Specifies the group using the AuthPriv Security Level.   |

**Defaults** The default is that no user security model group is defined.

**Command Modes** global configuration

**Device Modes** application-accelerator  
central-manager

**Usage Guidelines** The maximum number of SNMP groups that can be created is 10.

■ **(config) snmp-server group**

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 shows how to define a user security model group named acme that uses the 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](#)
- [\(config\) snmp-server notify inform](#)
- [\(config\) 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]]]
```

```
no 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. |
| <b>v2c</b>             | (Optional) Specifies the Version 2c Security Model.   |
| <b>retry number</b>    | (Optional) Sets the count for the number of retries (1–10) for the inform request. (The default is 2 tries.)          |
| <b>timeout seconds</b> | (Optional) Sets the timeout for the inform request (1–1000 seconds). The default is 15 seconds.                       |
| <b>v3</b>              | (Optional) Specifies the User Security Model (SNMPv3).  |
| <b>auth</b>            | Sends a notification using the AuthNoPriv Security Level.   |
| <b>noauth</b>          | Sends a notification using the noAuthNoPriv Security Level.   |
| <b>priv</b>            | Sends a 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

central-manager

---

```
(config) snmp-server host
```

**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 enter 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 with the **snmp-server enable traps** command to enable SNMP traps.

You must enable SNMP with the **snmp-server community** command.

**Examples**

The following example shows how to send 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 shows how to remove 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](#)
- [\(config\) snmp-server notify inform](#)
- [\(config\) 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*

**no snmp-server location** *line*

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | <b>location</b> <i>line</i> Specifies text for MIB-II object <i>sysLocation</i> . This string describes the physical location of this node.  |
| <b>Defaults</b>           | No system location string is set.  |
| <b>Command Modes</b>      | global configuration   |
| <b>Device Modes</b>       | application-accelerator<br>central-manager   |
| <b>Usage Guidelines</b>   | The system location string is the value stored in the MIB-II system group system location object. You can see the system location string with the <b>show snmp</b> EXEC command.   |
| <b>Examples</b>           | The following example shows how configure a system location string:<br><pre>WAE(config)# snmp-server location Building 3/Room 214</pre>  |
| <b>Related Commands</b>   | <a href="#">(config) snmp-server community</a><br><a href="#">(config) snmp-server contact</a><br><a href="#">(config) snmp-server enable traps</a><br><a href="#">(config) snmp-server group</a><br><a href="#">(config) snmp-server host</a><br><a href="#">(config) snmp-server mib</a><br><a href="#">(config) snmp-server notify inform</a><br><a href="#">(config) snmp-server user</a><br><a href="#">(config) snmp-server view</a><br><a href="#">snmp trigger</a> |

---

```
(config) snmp-server mib
```

## (config) snmp-server mib

To configure persistence for the SNMP Event MIB, use the **snmp-server mib** global configuration command. To disable the Event MIB, use the **no** form of this command.

**snmp-server mib persist event**

**no snmp-server mib persist event**

|                           |   |
|---------------------------|---|
| <b>Syntax Description</b> | <b>persist</b> Configures MIB persistence.<br><b>event</b> Enables MIB persistence for the Event MIB. |
|---------------------------|---|

---

**Defaults** No default behavior or values.

---

**Command Modes** global configuration

---

**Device Modes** application-accelerator  
central-manager

---

**Usage Guidelines** The Event MIB can set the threshold on any MIB variables supported by the WAAS software and store the threshold permanently on the 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**

The WAAS software supports six generic alarm traps in the CISCO-CONTENT-ENGINE-MIB for SNMP and Node Health Manager integration.

**Examples**

The following example shows how to set 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 user](#)  
[\(config\) snmp-server view](#)  
[snmp trigger](#)

---

```
■ (config) snmp-server notify inform
```

## (config) snmp-server notify inform

To configure the SNMP notify inform request on a 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**

**no snmp-server notify inform**

---

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

---

**Defaults** If you do not enter the **snmp-server notify inform** command, the default is an SNMP trap request.

---

**Command Modes** global configuration

---

**Device Modes** application-accelerator  
central-manager

---

**Examples** The following example shows how to configure 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](#)
- [\(config\) snmp-server user](#)
- [\(config\) snmp-server view](#)
- [snmp trigger](#)

# (config) snmp-server trap-source

To set the source interface from which SNMP traps are sent on a WAAS device, use the **snmp-server trap-source** global configuration command. To remove the trap source configuration, use the **no** form of this command.

```
snmp-server trap-source { GigabitEthernet slot/port | PortChannel 1| Standby grpnumber}
```

```
no snmp-server trap-source { GigabitEthernet slot/port | PortChannel 1| Standby grpnumber}
```

| Syntax Description                         |  |
|--|--|
| <b>GigabitEthernet</b><br><i>slot/port</i> | Selects a Gigabit Ethernet interface to configure as the trap source. The slot range is 1–2; the port must be 0. The slot number and port number are separated with a forward slash character (/). |
| <b>PortChannel 1</b>                       | Selects a port channel to configure as the trap source. There is only port channel 1.  |
| <b>Standby</b> <i>grpnumber</i>            | Selects a standby group to configure as the trap source. The group number range is 1–4.  |

**Defaults** No system trap source is set.

**Command Modes** global configuration

**Device Modes** application-accelerator  
central-manager

**Examples** The following example shows how to configure gigabit Ethernet interface 1/0 as the trap source:

```
WAE(config)# snmp-server trap-source gigabitethernet 1/0
```

**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 mib](#)
- [\(config\) snmp-server notify inform](#)
- [\(config\) snmp-server user](#)
- [\(config\) snmp-server view](#)
- [snmp trigger](#)

(config) snmp-server user

## (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] }]]
```

```
no 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] }]]
```

|                                  |  |
|----------------------------------|--|
| <b>Syntax Description</b>        | <b>user</b> <i>name group</i> Specifies the name and group of the SNMP user. Use letters, numbers, dashes, and underscores, but no blanks. The name specifies 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 for the name. The group specifies the group to which the SNMP user belongs. You can enter a maximum of 64 characters for the group.  |
| <b>auth</b>                      | (Optional) Configures user authentication parameters.  |
| <b>md5</b> <i>password</i>       | Configures HMAC MD5 user authentication password.  |
| <b>priv</b> <i>password</i>      | (Optional) Configures authentication HMAC-MD5 user private password. You can enter a maximum of 256 characters.  |
| <b>sha</b> <i>password</i>       | Configures the HMAC-SHA authentication password. You can enter a maximum of 256 characters.  |
| <b>remote</b> <i>octetstring</i> | (Optional) Specifies the globally unique identifier for a remote SNMP entity (for example, the SNMP network management station) for at least one of the SNMP users.<br><br>To send an SNMPv3 inform message, you must configure at least one SNMPv3 user with a remote SNMP ID option 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. |
| <b>Defaults</b>                  | No default behavior or values.   |
| <b>Command Modes</b>             | global configuration   |
| <b>Device Modes</b>              | application-accelerator<br>central-manager   |

**Examples**

The following example shows how to create an SNMPv3 user account 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](#)  
[\(config\) snmp-server notify inform](#)  
[\(config\) snmp-server view](#)  
[snmp trigger](#)

(config) snmp-server view

## (config) snmp-server view

To define an 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}**

**no snmp-server view *viewname MIBfamily* {excluded | included}**

|                           |   |                           |  |                 |  |                 |                                      |
|---------------------------|---|---------------------------|--|-----------------|--|-----------------|--------------------------------------|
| <b>Syntax Description</b> | <table border="0"> <tr> <td><i>viewname MIBfamily</i></td><td>Name of this family of view subtrees and a subtree of the MIB. You can enter a maximum of 64 characters.</td></tr> <tr> <td><b>excluded</b></td><td>Excludes the MIB family from the view.</td></tr> <tr> <td><b>included</b></td><td>Includes the MIB family in the view.</td></tr> </table> | <i>viewname MIBfamily</i> | Name of this family of view subtrees and a subtree of the MIB. You can enter a maximum of 64 characters. | <b>excluded</b> | Excludes the MIB family from the view. | <b>included</b> | Includes the MIB family in the view. |
| <i>viewname MIBfamily</i> | Name of this family of view subtrees and a subtree of the MIB. You can enter a maximum of 64 characters.  |                           |  |                 |  |                 |                                      |
| <b>excluded</b>           | Excludes the MIB family from the view.  |                           |  |                 |  |                 |                                      |
| <b>included</b>           | Includes the MIB family in the view.  |                           |  |                 |  |                 |                                      |

**Defaults** No default behavior or values.

**Command Modes** global configuration

**Device Modes** application-accelerator  
central-manager

**Examples** The following example shows how to define 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](#)
- [\(config\) snmp-server notify inform](#)
- [\(config\) snmp-server user](#)
- [snmp trigger](#)

## (config) sshd

To enable the SSH daemon on a WAAS device, use the **sshd** global configuration command. 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}}
```

```
no sshd {allow-non-admin-users | enable | password-guesses number | timeout seconds |
version {1 | 2}}
```

|                                |  |
|--------------------------------|--|
| <b>Syntax Description</b>      | <b>allow-non-admin-users</b> Allows nonadministrative users to gain SSH access to the chosen device (or device group). By default, this option is disabled.<br><b>Note</b> Nonadministrative users are nonsuperuser administrators. All nonsuperuser administrators 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. |
| <b>enable</b>                  | Enables the SSH daemon on a WAAS device.   |
| <b>password-guesses number</b> | Specifies the maximum number of allowable password guesses per connection (1–99). The default is 3.  |
| <b>timeout seconds</b>         | Configures the number of seconds for which an SSH session will be active during the negotiation (authentication) phase between the client and server before it times out. The SSH login grace time value in seconds is 1–99999. The default is 300.<br><br>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 a successful login.                 |
| <b>version</b>                 | Configures the SSH version to be supported on the WAAS device.   |
| <b>1</b>                       | Specifies that SSH Version 1 is supported on the WAAS device.  |
| <b>2</b>                       | 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

(config) sshd

central-manager

**Usage Guidelines**

Before you enable the **sshd** command, use the **ssh-key-generate** command to generate a private and a public host key, which the client uses to verify the server 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 you enter the **sshd password-guesses** command and specify *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** You can use the Telnet daemon with the WAAS device. SSH does not replace Telnet.

**Examples**

The following example shows how to enable and configure 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 shows how to disable 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

## (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 this command.

**ssh-key-generate [key-length *length*]**

**no ssh-key-generate [key-length *length*]**

---

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | <b>key-length <i>length</i></b> (Optional) Configures the length of the SSH key. The number of bits is 512–2048. |
|---------------------------|--|

---

|                 |  |
|-----------------|--|
| <b>Defaults</b> | <b>key-length <i>length</i>:</b> 1024 bits |
|-----------------|--|

|                      |                      |
|----------------------|----------------------|
| <b>Command Modes</b> | global configuration |
|----------------------|----------------------|

|                     |  |
|---------------------|--|
| <b>Device Modes</b> | application-accelerator<br>central-manager |
|---------------------|--|

|                         |  |
|-------------------------|--|
| <b>Usage Guidelines</b> | Before you enter the <b>sshd enable</b> command, enter the <b>ssh-key-generate</b> command to generate a private and a public host key, which the client programs use to verify a server 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 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.

|                 |   |
|-----------------|---|
| <b>Examples</b> | The following example shows how to generate 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
```

|                         |                               |
|-------------------------|-------------------------------|
| <b>Related Commands</b> | <a href="#">(config) sshd</a> |
|-------------------------|-------------------------------|

## (config) tacacs

To configure TACACS+ server parameters on a WAAS device, use the **tacacs** global configuration command. To disable individual options, use the **no** form of this command.

```
tacacs {host {hostname | ip-address} [primary] | key keyword | password ascii | retransmit retries | timeout seconds}
no tacacs {host {hostname | ip-address} [primary] | key keyword | password ascii | retransmit retries | timeout seconds}
```

| Syntax Description        |   |
|---------------------------|---|
| <b>host</b>               | Specifies a server address.   |
| <i>hostname</i>           | Hostname of the TACACS+ server.   |
| <i>ip-address</i>         | IP address of the TACACS+ server.   |
| <b>primary</b>            | (Optional) Sets the server as the primary server.   |
| <b>key keyword</b>        | Sets the security word. An empty string is the default.   |
| <b>password ascii</b>     | Specifies ASCII as the TACACS+ password type.   |
| <b>retransmit retries</b> | Sets the number of times that requests are retransmitted to a server. The number of retry attempts allowed is 1–3. The default is 2 retry attempts. |
| <b>timeout seconds</b>    | Sets the number of seconds to wait before a request to a server is timed out. The timeout is 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  
central-manager

**Usage Guidelines** To enable user authentication with a TACACS+ server, use the **authentication** global configuration command. (See the [\(config\) authentication configuration](#) command.)

You can use the TACACS+ remote database 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

(config) tacacs

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.

**Examples**

The following example shows how to configure the key used in encrypting packets:

```
WAE(config)# tacacs key human789
```

The following example shows how to configure the host named spearhead as the primary TACACS+ server:

```
WAE(config)# tacacs host spearhead primary
```

The following example shows how to set the timeout interval for the TACACS+ server:

```
WAE(config)# tacacs timeout 10
```

The following example shows how to set 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 configuration](#)  
[show authentication](#)  
[show statistics authentication](#)  
[show statistics tacacs](#)  
[show tacacs](#)

(config) tcp

## (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 | ecn enable | increase-xmit-timer-value value |
      init-ss-threshold value | keepalive-probe-cnt count | keepalive-probe-interval seconds |
      keepalive-timeout seconds}
```

```
no tcp {cwnd-base segments | ecn enable | increase-xmit-timer-value value |
         init-ss-threshold value | keepalive-probe-cnt count | keepalive-probe-interval seconds |
         keepalive-timeout seconds}
```

### Syntax Description

|   |   |
|---|---|
| <b>cwnd-base segments</b>               | Sets initial send congestion window in segments (1–10).   |
| <b>ecn enable</b>                       | Enables TCP explicit congestion notification.   |
| <b>increase-xmit-timer-value value</b>  | 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.  |
|   | <b>Note</b> Use this keyword with caution. The keyword can improve throughput when TCP is used over slow reliable connections but should never be changed in an unreliable packet delivery environment. |
| <b>init-ss-threshold value</b>          | Sets initial slow-start threshold value.  |
| <b>keepalive-probe-cnt count</b>        | Specifies the length of time that the WAAS device keeps an idle connection open. The number of probe counts is 1–10.  |
| <b>keepalive-probe-interval seconds</b> | Specifies the number of times that the WAAS device retries a connection. The keepalive probe interval is in seconds (1–300).  |
| <b>keepalive-timeout seconds</b>        | Specifies the length of time that the WAAS device keeps a connection open before disconnecting. The keepalive timeout is in seconds (1–3600).   |

### Defaults

**tcp cwnd-base:** 2  
**tcp increase-xmit-timer-value:** 1  
**tcp init-ss-threshold:** 100 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  
central-manager

**Usage Guidelines****Caution**

The following are the usage guidelines for this command:

Be careful using these parameters. In nearly all environments, the default TCP settings are adequate. Fine tuning of TCP settings is for network administrators who are experienced and have a 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 shows how to enable a TCP explicit congestion notification:

```
WAE(config)# tcp ecn enable
```

**Related Commands**

[clear arp-cache](#)  
[show statistics tcp](#)  
[show tcp](#)

(config) telnet enable

## (config) telnet enable

To enable Telnet on a WAAS device, use the **telnet enable** global configuration command. To disable this feature, use the **no** form of this command.

**telnet enable**

**no 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  
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 shows how to enable the use of Telnet on the WAAS device:

```
WAE(config)# telnet enable
```

**Related Commands** **telnet**

**show telnet**

# (config) tfo exception

To configure exception handling for Traffic Flow Optimization (TFO), use the **tfo exception** global configuration command. To disable TFO exception handling configuration, use the **no** form of this command.

```
tfo exception {coredump | debug | no-coredump}
```

```
no tfo exception {coredump | debug | no-coredump}
```

| Syntax Description |  |
|--------------------|--|
| <b>coredump</b>    | Writes a core file (default).                            |
| <b>debug</b>       | Hangs the system until it is explicitly restarted.       |
| <b>no-coredump</b> | Restarts the accelerator and does not write a core file. |

**Defaults** The default is coredump.

**Command Modes** global configuration

**Device Modes** application-accelerator

**Examples** The following example shows how to write TFO exception handling to a core file using the **tfo exception** command:

```
WAE(config)# tfo exception coredump
```

**Related Commands** [\(config\) tfo optimize](#)

(config) tfo optimize

## (config) tfo optimize

To configure a WAE for Traffic Flow Optimization (TFO), use the **tfo optimize** global configuration command. To disable TFO optimization, use the **no** form of this command.

**tfo optimize {DRE {yes | no} compression {LZ | none} | full}**

**no tfo optimize {DRE {yes | no} compression {LZ | none} | full}**

| Syntax Description |  |   |
|--------------------|--|---|
| <b>DRE</b>         |  | Configures TFO optimization with or without Data Redundancy Elimination (DRE).  |
| <b>yes</b>         |  | Enables DRE.  |
| <b>no</b>          |  | Disables DRE.   |
| <b>compression</b> |  | Configures TFO optimization with or without generic compression.  |
| <b>LZ</b>          |  | Configures TFO optimization with Lempel-Ziv (LZ) compression.   |
| <b>none</b>        |  | Configures TFO optimization with no compression.  |
| <b>full</b>        |  | Configures TFO optimization with DRE and LZ compression. Using this keyword is the same as specifying the <b>tfo optimize DRE yes compression LZ</b> command. |

**Defaults** The default TFO optimization on a WAAS device is **tfo optimize full**.

**Command Modes** global configuration

**Device Modes** application-accelerator

**Examples** The following example shows to configures TFO optimization with DRE and full compression using the **tfo optimize** command:

```
WAE(config)# tfo optimize DRE yes compression full
```

**Related Commands** [show statistics tfo](#)

# (config) tfo tcp adaptive-buffer-sizing

To configure a WAE for Traffic Flow Optimization (TFO) with TCP adaptive buffering, use the **tfo tcp adaptive-buffer-sizing** global configuration command. To disable adaptive buffer sizing or to unconfigure the buffer size, use the **no** form of this command.

```
tfo tcp adaptive-buffer-sizing {enable | receive-buffer-max size | send-buffer-max size}
```

```
no tfo tcp adaptive-buffer-sizing {enable | receive-buffer-max size | send-buffer-max size}
```

| Syntax Description | <b>enable</b>                  | Enables TCP adaptive buffer sizing.  |
|--------------------|--------------------------------|--|
|                    | <b>receive-buffer-max size</b> | Sets the maximum size of the receive buffer. Valid values range from 1 to 8192 KB. |
|                    | <b>send-buffer-max size</b>    | Sets the maximum size of the send buffer. Valid values range from 1 to 8192 KB.    |

**Defaults** Adaptive buffering is enabled by default. The default maximum send and receive buffer sizes depend on the WAE device model.

**Command Modes** global configuration

**Device Modes** application-accelerator

**Usage Guidelines** If you would rather use preallocated and unchanging send and receive buffers, you can configure them with the following global configuration commands: **tfo tcp optimized-receive-buffer**, **tfo tcp optimized-send-buffer**, **tfo tcp original-receive-buffer**, and **tfo tcp original-send-buffer**. You can turn off adaptive buffer sizing by using the **no tfo tcp adaptive-buffer-sizing** command.

**Examples** The following example shows how to configure a WAE for Traffic Flow Optimization (TFO) with TCP adaptive buffering using the **tfo tcp adaptive-buffer-sizing** command:

```
WAE(config)# tfo tcp adaptive-buffer-sizing enable
```

**Related Commands**

- [\(config\) tfo tcp optimized-mss](#)
- [\(config\) tfo tcp optimized-receive-buffer](#)
- [\(config\) tfo tcp optimized-send-buffer](#)
- [\(config\) tfo tcp original-receive-buffer](#)
- [\(config\) tfo tcp original-send-buffer](#)
- [show tfo tcp](#)

---

```
(config) tfo tcp keepalive
```

## (config) tfo tcp keepalive

To configure a WAE for Traffic Flow Optimization (TFO) with TCP keepalives, use the **tfo tcp keepalive** global configuration command. To disable TFO TCP keepalives, use the **no** form of this command.

**tfo tcp keepalive**

**no tfo tcp keepalive**

---

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

---

**Defaults** Keepalives are disabled by default.

---

**Command Modes** global configuration

---

**Device Modes** application-accelerator

---

**Usage Guidelines** This command enables TCP keepalives on the TFO optimized sockets (the connection between two peer WAEs).

---

**Examples** The following example shows how to configure a WAE for Traffic Flow Optimization with TCP keepalives using the **tfo tcp keepalive** command:

```
WAE(config)# tfo tcp keepalive
```

---

**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) with an optimized-side TCP maximum segment size, use the **tfo tcp optimized-mss** global configuration command. To disable this function, use the **no** form of this command.

**tfo tcp optimized-mss** *segment-size*

**no tfo tcp optimized-mss** *segment-size*

|                           |   |
|---------------------------|---|
| <b>Syntax Description</b> | <i>segment-size</i> Optimized side TCP max segment size (512–1460). |
|---------------------------|---|

|                 |  |
|-----------------|--|
| <b>Defaults</b> | The default value of the segment size is 1432 bytes. |
|-----------------|--|

|                      |                      |
|----------------------|----------------------|
| <b>Command Modes</b> | global configuration |
|----------------------|----------------------|

|                     |                         |
|---------------------|-------------------------|
| <b>Device Modes</b> | application-accelerator |
|---------------------|-------------------------|

|                         |   |
|-------------------------|---|
| <b>Usage Guidelines</b> | This command sets the TCP maximum segment size on TFO optimized sockets (the connection between two peer WAEs). |
|-------------------------|---|

|                 |   |
|-----------------|---|
| <b>Examples</b> | The following example shows how to configure a WAE for Traffic Flow Optimization with an optimized-side TCP maximum segment size of 512 using the <b>tfo tcp optimized-mss</b> command: |
|-----------------|---|

```
WAE(config)# tfo tcp optimized-mss 512
```

|                         |   |
|-------------------------|---|
| <b>Related Commands</b> | <a href="#">(config) tfo tcp keepalive</a><br><a href="#">(config) tfo tcp optimized-receive-buffer</a><br><a href="#">(config) tfo tcp optimized-send-buffer</a><br><a href="#">(config) tfo tcp original-mss</a><br><a href="#">(config) tfo tcp original-receive-buffer</a><br><a href="#">(config) tfo tcp original-send-buffer</a> |
|-------------------------|---|

---

```
(config) tfo tcp optimized-receive-buffer
```

## (config) tfo tcp optimized-receive-buffer

To configure a WAE for Traffic Flow Optimization (TFO) with an optimized-side receive buffer, use the **tfo tcp optimized-receive-buffer** global configuration command. To disable this function, use the **no** form of this command.

**tfo tcp optimized-receive-buffer *buffer-size***

**no tfo tcp optimized-receive-buffer *buffer-size***

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | <i>buffer-size</i><br>Receive buffer size in kilobytes.  |
| <b>Defaults</b>           | 32 KB  |
| <b>Command Modes</b>      | global configuration   |
| <b>Device Modes</b>       | application-accelerator  |
| <b>Examples</b>           | The following example shows how to configure a WAE for Traffic Flow Optimization with a 32k optimized-side receive buffer using the <b>tfo tcp optimized-receive-buffer</b> command:<br><br><pre>WAE(config)# tfo tcp optimized-receive-buffer 32</pre>  |
| <b>Related Commands</b>   | <a href="#">(config) tfo tcp keepalive</a><br><a href="#">(config) tfo tcp optimized-mss</a><br><a href="#">(config) tfo tcp optimized-send-buffer</a><br><a href="#">(config) tfo tcp original-mss</a><br><a href="#">(config) tfo tcp original-receive-buffer</a><br><a href="#">(config) tfo tcp original-send-buffer</a> |

## (config) tfo tcp optimized-send-buffer

To configure a WAE for Traffic Flow Optimization (TFO) with an optimized-side send buffer, use the **tfo tcp optimized-send-buffer** global configuration command. To disable this function, use the **no** form of this command.

**tfo tcp optimized-send-buffer *buffer-size***

**no tfo tcp optimized-send-buffer *buffer-size***

|                           |   |
|---------------------------|---|
| <b>Syntax Description</b> | <i>buffer-size</i><br>Send buffer size in kilobytes.  |
| <b>Defaults</b>           | 32 KB   |
| <b>Command Modes</b>      | global configuration  |
| <b>Device Modes</b>       | application-accelerator   |
| <b>Usage Guidelines</b>   | The buffer should be equal to or greater than the Bandwidth Delay Product (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 $45 \text{ Mbps} * 0.15 \text{ sec} = 6.75 \text{ Mb}$ , or 0.844 MB (844 KB). In this case, you could set the buffer size to 1024 KB. |
| <b>Examples</b>           | The following example shows how to configure a WAE for Traffic Flow Optimization with a 32k optimized-side send buffer using the <b>tfo tcp optimized-send-buffer</b> command:<br><br>WAE(config)# <b>tfo tcp optimized-send-buffer 32</b>  |
| <b>Related Commands</b>   | <a href="#">(config) tfo tcp keepalive</a><br><a href="#">(config) tfo tcp optimized-mss</a><br><a href="#">(config) tfo tcp optimized-receive-buffer</a><br><a href="#">(config) tfo tcp original-mss</a><br><a href="#">(config) tfo tcp original-receive-buffer</a><br><a href="#">(config) tfo tcp original-send-buffer</a>   |

---

```
(config) tfo tcp original-mss
```

## (config) tfo tcp original-mss

To configure a WAE for Traffic Flow Optimization (TFO) with an unoptimized-side TCP maximum segment size, use the **tfo tcp original-mss** global configuration command. To disable this function, use the **no** form of this command.

**tfo tcp original-mss *segment-size***

**no tfo tcp original-mss *segment-size***

|                           |                     |  |
|---------------------------|---------------------|--|
| <b>Syntax Description</b> | <i>segment-size</i> | Specifies original (end-point) side TCP max segment size (512–1460). |
|---------------------------|---------------------|--|

|                 |            |
|-----------------|------------|
| <b>Defaults</b> | 1432 bytes |
|-----------------|------------|

|                      |                      |
|----------------------|----------------------|
| <b>Command Modes</b> | global configuration |
|----------------------|----------------------|

|                     |                         |
|---------------------|-------------------------|
| <b>Device Modes</b> | application-accelerator |
|---------------------|-------------------------|

|                 |  |
|-----------------|--|
| <b>Examples</b> | The following example shows how to configure a WAE for Traffic Flow Optimization with a 1432 byte unoptimized-side TCP maximum segment size using the <b>tfo tcp original-mss</b> command: |
|-----------------|--|

```
WAE(config)# tfo tcp original-mss 1432
```

|                         |  |
|-------------------------|--|
| <b>Related Commands</b> | <a href="#">(config) tfo tcp keepalive</a><br><a href="#">(config) tfo tcp optimized-mss</a><br><a href="#">(config) tfo tcp optimized-receive-buffer</a><br><a href="#">(config) tfo tcp optimized-send-buffer</a><br><a href="#">(config) tfo tcp original-receive-buffer</a><br><a href="#">(config) tfo tcp original-send-buffer</a> |
|-------------------------|--|

## (config) tfo tcp original-receive-buffer

To configure a WAE for Traffic Flow Optimization (TFO) with an unoptimized-side receive buffer, use the **tfo tcp original-receive-buffer** global configuration command. To disable this function, use the **no** form of this command.

**tfo tcp original-receive-buffer *buffer-size***

**no tfo tcp original-receive-buffer *buffer-size***

|                           |   |
|---------------------------|---|
| <b>Syntax Description</b> | <i>buffer-size</i> Receive buffer size in kilobytes.  |
| <b>Defaults</b>           | 32 KB   |
| <b>Command Modes</b>      | global configuration  |
| <b>Device Modes</b>       | application-accelerator   |
| <b>Examples</b>           | The following example shows how to configure a WAE for Traffic Flow Optimization with a 32k unoptimized-side receive buffer using the <b>tfo tcp original-receive-buffer</b> command:<br><br>WAE(config)# <b>tfo tcp original-receive-buffer 32</b>   |
| <b>Related Commands</b>   | <a href="#">(config) tfo tcp keepalive</a><br><a href="#">(config) tfo tcp optimized-mss</a><br><a href="#">(config) tfo tcp optimized-receive-buffer</a><br><a href="#">(config) tfo tcp optimized-send-buffer</a><br><a href="#">(config) tfo tcp original-mss</a><br><a href="#">(config) tfo tcp original-send-buffer</a> |

---

```
(config) tfo tcp original-send-buffer
```

## (config) tfo tcp original-send-buffer

To configure a WAE for Traffic Flow Optimization (TFO) with an unoptimized-side send buffer, use the **tfo tcp original-send-buffer** global configuration command. To disable this function, use the **no** form of this command.

**tfo tcp original-send-buffer *buffer-size***

**no tfo tcp original-send-buffer *buffer-size***

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | <i>buffer-size</i><br>Send buffer size in kilobytes.   |
| <b>Defaults</b>           | 32 KB  |
| <b>Command Modes</b>      | global configuration   |
| <b>Device Modes</b>       | application-accelerator  |
| <b>Examples</b>           | The following example shows how to configure a WAE for Traffic Flow Optimization with a 32k unoptimized-side receive buffer using the <b>tfo tcp original-send-buffer</b> command:<br><br>WAE(config)# <b>tfo tcp original-send-buffer 32</b>  |
| <b>Related Commands</b>   | <a href="#">(config) tfo tcp keepalive</a><br><a href="#">(config) tfo tcp optimized-mss</a><br><a href="#">(config) tfo tcp optimized-receive-buffer</a><br><a href="#">(config) tfo tcp optimized-send-buffer</a><br><a href="#">(config) tfo tcp original-mss</a><br><a href="#">(config) tfo tcp original-receive-buffer</a> |

# (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 {accelerator video windows-media | flow} enable
transaction-logs flow access-list acl-name
transaction-logs {accelerator video windows-media | flow} archive interval seconds
transaction-logs {accelerator video windows-media | flow} archive interval every-day
{at hour:minute | every hours}
transaction-logs {accelerator video windows-media | flow} archive interval every-hour
{at minute | every minutes}
transaction-logs {accelerator video windows-media | flow} archive interval every-week
[on weekdays at hour:minute]
transaction-logs {accelerator video windows-media | flow} archive max-file-size filesize
transaction-logs {accelerator video windows-media | flow} export compress
transaction-logs {accelerator video windows-media | flow} export enable
transaction-logs {accelerator video windows-media | flow} export ftp-server
{hostname | servipaddrs} login passw directory
transaction-logs {accelerator video windows-media | flow} export interval minutes
transaction-logs {accelerator video windows-media | flow} export interval every-day
{at hour:minute | every hours}
transaction-logs {accelerator video windows-media | flow} export interval every-hour
{at minute | every minutes}
transaction-logs {accelerator video windows-media | flow} export interval every-week
[on weekdays at hour:minute]
transaction-logs {accelerator video windows-media | flow} export sftp-server
{hostname | servipaddrs} login passw directory
```

| Syntax Description                     |  |
|--|--|
| <b>accelerator video windows-media</b> | Specifies the video accelerator transaction log feature for Windows Media transactions.                                |
| <b>flow</b>                            | Specifies the TFO flow transaction log feature.  |
| <b>enable</b>                          | Enables the transaction log feature.   |
| <b>access-list <i>acl-name</i></b>     | Configures an access list name to restrict logged traffic. Only traffic that is included in the access list is logged. |
| <b>archive</b>                         | Configures archive parameters.   |
| <b>interval <i>seconds</i></b>         | Determines how frequently the archive file is to be saved. Value is in seconds (120–604800).                           |

(config) transaction-logs

|                                      |  |
|--------------------------------------|--|
| <b>every-day</b>                     | Archives using intervals of 1 day or less.   |
| <b>at hour:minute</b>                | Specifies the local time at which to archive each day (hh:mm).   |
| <b>every hours</b>                   | Specifies the interval in hours. The interval aligns with midnight. The intervals are as follows:<br>1 Hourly<br>12 Every 12 hours<br>2 Every 2 hours<br>24 Every 24 hours<br>3 Every 3 hours<br>4 Every 4 hours<br>6 Every 6 hours<br>8 Every 8 hours                       |
| <b>every-hour</b>                    | Specifies intervals of 1 hour or less.   |
| <b>at minute</b>                     | Sets the time at each hour. The minute alignment for the hourly task is from 0 to 59.  |
| <b>every minutes</b>                 | Specifies the interval in minutes for hourly task that aligns with the top of the hour. The intervals are as follows:<br>10 Every 10 minutes<br>15 Every 15 minutes<br>2 Every 2 minutes<br>20 Every 20 minutes<br>30 Every 30 minutes<br>5 Every 5 minutes                  |
| <b>every-week</b>                    | Specifies intervals of 1 or more times a week.   |
| <b>on weekdays</b>                   | (Optional) Sets the day of the week and the weekdays on which to perform the task. You can specify one or more weekdays:<br>Fri Every Friday<br>Mon Every Monday<br>Sat Every Saturday<br>Sun Every Sunday<br>Thu Every Thursday<br>Tue Every Tuesday<br>Wed Every Wednesday |
| <b>max-file-size</b> <i>filesize</i> | Specifies the maximum size in kilobytes (1000–2000000) of the archive file to be maintained on the local disk.   |
| <b>export</b>                        | 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.  |
| <b>compress</b>                      | Enables compression of archived log files into a zip format before exporting them to external FTP servers.   |
| <b>ftp-server</b>                    | Sets the FTP server to receive exported archived files.  |
| <i>hostname</i>                      | Hostname of the target server.   |
| <i>servipaddrs</i>                   | IP address of the target server.   |
| <i>login</i>                         | User login to target server (1–10080).   |
| <i>passw</i>                         | User password to target server (less than 40 characters).  |
| <i>directory</i>                     | Target directory path for exported files on the server.  |

|                         |  |
|-------------------------|--|
| <b>interval minutes</b> | Specifies the interval in minutes (1–10080) at which to export a file.                   |
| <b>sftp-server</b>      | Sets the Secure File Transfer Protocol (SFTP) server to receive exported archived files. |

**Defaults**

The default settings for the logging feature are as follows:

**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

**Command Modes**

global configuration

**Device Modes**

application-accelerator

**Related Commands**

[clear arp-cache](#)

[show transaction-logging](#)

[transaction-log](#)

(config) username

# (config) username

To establish username authentication on a WAAS device, use the **username** global configuration command. To disable this feature, use the **no** form of this command.

```
username name {password {0 plainword | 1 cryptoword | plainword} [uid uid] |
    print-admin-password {0 plainword | 1 cryptoword plainword | plainword} |
    privilege {0 | 15}}
```

```
no username name {password {0 plainword | 1 cryptoword | plainword} [uid uid] |
    print-admin-password {0 plainword | 1 cryptoword plainword | plainword} |
    privilege {0 | 15}}
```

## Syntax Description

|                             |  |
|-----------------------------|--|
| <i>name</i>                 | Username.  |
| <b>password</b>             | Specifies the password for the user.   |
| <b>0</b>                    | Specifies an unencrypted user password.  |
| <i>plainword</i>            | Clear-text user password. Passwords are case sensitive, must be 1 to 31 characters, and cannot contain the characters '“  (apostrophe, double quote, or pipe) or any control characters. |
| <b>1</b>                    | Specifies a hidden user password.  |
| <i>cryptoword</i>           | Encrypted user password.   |
| <b>uid uid</b>              | (Optional) Sets the text user ID for the password (2001–65535).  |
| <b>print-admin-password</b> | Sets the user print administration password.   |
| <b>privilege</b>            | Sets the user privilege level.   |
| <b>0</b>                    | Specifies the user privilege level for the normal user.  |
| <b>15</b>                   | Specifies the user privilege level for the superuser.  |

## Defaults

The **password** value is set to 0 (clear text) by default.

The default administrator account is as follows:

- Uid: 0
- Username: admin
- Password: default
- Privilege: superuser (15)

## Command Modes

global configuration

## Device Modes

application-accelerator  
central-manager

**Usage Guidelines**

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 a single WAE or group of WAEs, which are registered with a WAAS Central Manager, see the *Cisco Wide Area Application Services Configuration Guide*.

**Examples**

The following example demonstrates how passwords and privilege levels are reconfigured:

```

WAE# show user username abeddoe
Uid : 2003
Username : abeddoe
Password : ghQ.GyGhP96K6
Privilege : normal user

WAE# show user username bwhidney
Uid : 2002
Username : bwhidney
Password : bhlohlbIwAMOk
Privilege : normal user

WAE(config)# username bwhidney password 1 victoria

WAE(config)# username abeddoe privilege 15
User's privilege changed to super user (=15)

WAE# show user username abeddoe
Uid : 2003
Username : abeddoe
Password : ghQ.GyGhP96K6
Privilege : super user

WAE# show user username bwhidney
Uid : 2002
Username : bwhidney
Password : mhYWyw.7P1Ld6
Privilege : normal user

```

**Related Commands**

[show user](#)

(config) virtual-blade

# (config) virtual-blade

To configure virtual blades on your WAAS device, use the **virtual-blade** global configuration command. To negate these actions, use the **no** form of this command.

**virtual-blade {virtual-blade-number | enable}**

**no virtual-blade {virtual-blade-number | enable}**

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | <b>virtual-blade-number</b> Number of the virtual blade that you want to edit. This value can be from 1 through 6, depending on the number of virtual blades supported on the device. Using this command enables virtual blade configuration mode. See the “Virtual Blade Configuration Mode Commands” section for more information. |
|                           | <b>enable</b> Enables the virtual blade feature on your WAAS device. You must reboot the device after executing this command.  |

---

## Defaults

No default behavior or values.

---

## Command Modes

global configuration

---

## Device Modes

application-accelerator

---

## Usage Guidelines

Use the **virtual-blade** global configuration command to enter virtual blade configuration mode. This command is available only on WAAS devices that support virtual blades.

---

## Examples

The following example shows how to enable the virtual blade feature on your device:

```
WAE(config)# virtual-blade enable
WAE(config)# exit
```

The following example shows that after a reload, you can enter **show EXEC** command to see the new virtual blade resource allocation:

```
# show virtual-blade
Virtual-blade resources:
  VB Memory: 299MiB configured, 1749MiB available.
  VB Disk space: 0GiB configured, 204GiB available.
  /local1/vbs: 128MiB used, 214203MiB available
  CPU(s) assigned: 3 4
Virtual-blade(s) state:
  virtual-blade 2 has incomplete configuration
```

The following example puts your device into virtual blade configuration mode, editing virtual blade 2. The mode change is indicated by the system prompt:

```
WAE(config)# virtual-blade 2
```

```
WAE(config-vb) #
```

**Related Commands**

[show virtual-blade](#)  
[\(config-vb\) autostart](#)  
[\(config-vb\) boot](#)  
[\(config-vb\) description](#)  
[\(config-vb\) device](#)  
[\(config-vb\) disk](#)  
[\(config-vb\) interface](#)  
[\(config-vb\) memory](#)

(config) wccp access-list

## (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. To disable this feature, use the **no** form of this command.

**wccp access-list {acl-number | ext-acl-number | acl-name}**

**no wccp access-list {acl-number | ext-acl-number | acl-name}**

|                           |  |                   |  |                       |   |                 |  |
|---------------------------|--|-------------------|--|-----------------------|---|-----------------|--|
| <b>Syntax Description</b> | <table border="0"> <tr> <td><i>acl-number</i></td><td>Standard IP access list number (1–99).</td></tr> <tr> <td><i>ext-acl-number</i></td><td>Extended IP access list number (100–199).</td></tr> <tr> <td><i>acl-name</i></td><td>Name of the access list. You can use a maximum of 30 characters.</td></tr> </table> | <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. You can use a maximum of 30 characters. |
| <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. You can use a maximum of 30 characters.   |                   |  |                       |   |                 |  |

**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. 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 shows how to configure the WAE to apply IP access list number 10 to the 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

```

**(config) wccp access-list**

```
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

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**

**no wccp flow-redirect enable**

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | <b>enable</b> Enables flow redirection.  |
| <b>Defaults</b>           | Enabled  |
| <b>Command Modes</b>      | global configuration   |
| <b>Device Modes</b>       | application-accelerator  |
| <b>Usage Guidelines</b>   | <p>Use the <b>wccp flow-redirect</b> 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 where the WAEs try to take a load appropriate for their capacity.</p> <p> <b>Note</b> When you enable bypass, the client tries to reach the origin web server. You must disable all bypass options to eliminate an unnecessary burden on the network.</p> <p>WCCP works only with IPv4 networks.</p> |
| <b>Examples</b>           | The following example shows how to enable WCCP flow protection on a WAE:<br><br>WAE(config)# <b>wccp flow-redirect enable</b>  |
| <b>Related Commands</b>   | <a href="#">show wccp</a>  |

(config) wccp router-list

## (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**

**no wccp router-list number ip-address**

|                           |  |               |                           |                   |  |
|---------------------------|--|---------------|---------------------------|-------------------|--|
| <b>Syntax Description</b> | <table border="0"> <tr> <td><i>number</i></td><td>Router list number (1–8).</td></tr> <tr> <td><i>ip-address</i></td><td>IP address of the router to add to the list.</td></tr> </table>   | <i>number</i> | Router list number (1–8). | <i>ip-address</i> | IP address of the router to add to the list. |
| <i>number</i>             | Router list number (1–8).  |               |                           |                   |  |
| <i>ip-address</i>         | IP address of the router to add to the list.   |               |                           |                   |  |
| <b>Defaults</b>           | Disabled   |               |                           |                   |  |
| <b>Command Modes</b>      | global configuration   |               |                           |                   |  |
| <b>Device Modes</b>       | application-accelerator  |               |                           |                   |  |
| <b>Usage Guidelines</b>   | <p>Each router list can contain up to 32 routers and you can have up to 8 router lists.</p> <p> <b>Note</b> Do not create or modify router list number 8. The WAAS Central Manager uses router list number 8 for a default router list that contains the default gateway.</p> <p> <b>Note</b> The <b>ip wccp</b> global configuration command must be used to enable WCCP on each router that is included on the router list.</p> <p>WCCP works only with IPv4 networks.</p> |               |                           |                   |  |

**Examples** The following example shows how 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 shows how to delete 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

## (config) wccp shutdown

To set the maximum time interval after which the WAE will perform a clean shutdown of the WCCP, use the **wccp shutdown** global configuration command. To disable the clean shutdown, use the **no** form of this command.

**wccp shutdown max-wait seconds**

**no wccp shutdown max-wait seconds**

|                           |                         |  |
|---------------------------|-------------------------|--|
| <b>Syntax Description</b> | <b>max-wait seconds</b> | Sets the clean shutdown time interval. The time is in seconds (0–86400).<br>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 the WCCP after you enter the **reload** or **wccp version** command. The WAE does not reboot until either all connections have been serviced or the configured **max-wait** interval has elapsed.



**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](#)
- (config) [wccp version](#)

(config) wccp tcp-promiscuous mask

## (config) wccp tcp-promiscuous mask

To configure the Web Cache Coordination Protocol (WCCP) Version 2 TCP promiscuous mode service (WCCP Version 2 services 61 and 62) mask on a WAE, use the **wccp tcp-promiscuous mask** global configuration command. To disable this function, use the **no** form of this command.

**wccp tcp-promiscuous mask {dst-ip-mask mask | src-ip-mask mask}**

**no wccp tcp-promiscuous mask {dst-ip-mask mask | src-ip-mask mask}**

|                           |   |
|---------------------------|---|
| <b>Syntax Description</b> |   |
| <b>mask</b>               | Specifies the mask used for WAE assignment.   |
| <b>dst-ip-mask mask</b>   | 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. |
| <b>src-ip-mask mask</b>   | 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.      |

**Command Modes** global configuration

**Device Modes** application-accelerator

**Usage Guidelines** To configure the egress method for WCCP intercepted connections, use the **egress-method** global configuration command.



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:

WAE # **wccp tcp-promiscuous mask**

**Related Commands**

- [\(config\) egress-method](#)
- [\(config\) wccp router-list](#)
- [show wccp](#)

## (config) wccp tcp-promiscuous router-list-num

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 router-list-num** global configuration command. To disable this function, use the **no** form of this command.

```
wccp tcp-promiscuous router-list-num number [assign-method-strict | hash-destination-ip |
hash-source-ip | l2-redirect | l2-return | mask-assign | password password | weight weight]}
```

```
no wccp tcp-promiscuous 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          |  |
|-----------------------------|--|
| <b>router-list-num</b>      | Specifies the 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.)   |
| <b>number</b>               |  |
| <b>assign-method-strict</b> | (Optional) Specifies that only the configured assignment method be used.   |
| <b>hash-destination-ip</b>  | (Optional) Specifies that the load-balancing hash method should make use of the destination IP address. You can specify both the <b>hash-destination-ip</b> option and the <b>hash-source-ip</b> option.   |
| <b>hash-source-ip</b>       | (Optional) Specifies that the load-balancing hash method should make use of the source IP address. This is the default.  |
| <b>l2-redirect</b>          | (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.  |
| <b>l2-return</b>            | (Optional) Specifies that Layer 2 rewriting be used for packet return.   |
| <b>mask-assign</b>          | (Optional) Specifies that the mask method be used for WAE assignment.  |
| <b>password password</b>    | (Optional) Specifies the WCCP service 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. You can use a maximum of 8 characters.  |
| <b>weight weight</b>        | (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).<br><br>The weight value ranges from 0 to 100 percent. 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

```
■ (config) wccp tcp-promiscuous router-list-num
```

**Usage Guidelines**

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:

```
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 this command.

**wccp version 2**

**no wccp version 2**

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

**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.



**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** [\(config\) wecp tcp-promiscuous mask](#)

[\(config\) wecp router-list](#)

(config) windows-domain

## (config) windows-domain

To configure Windows domain server options on a WAAS device, use the **windows-domain** global configuration command. To disable this feature, use the **no** form of this 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 }
```

```
no 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                 |  |
|------------------------------------|--|
| <b>administrative</b>              | Sets administrative options.   |
| <b>group</b>                       | Sets an administrative group name.   |
| <b>normal-user</b>                 | Sets the administrative group name for the normal user (privilege 0).  |
| <b>super-user</b>                  | Sets the administrative group name for the superuser (privilege 15).   |
| <i>groupname</i>                   | Name of the administrative group.  |
| <b>comment</b> <i>string</i>       | Specifies a comment for the Windows domain server. This is a text string.  |
| <b>netbios-name</b> <i>name</i>    | Specifies the NetBIOS name of the WAE. This name is provided when the Edge FE announces its availability for print services.   |
| <b>password-server</b>             | Specifies the password server used to verify a client password.  |
| <i>hostname</i>                    | Hostname of the password server.   |
| <i>ipaddress</i>                   | IP address of the password server.   |
| <b>realm</b> <i>kerberos-realm</i> | 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.<br><br>The value is an 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.<br><br>Example: <i>kerberos-realm</i> = MYBOX.MYCOMPANY.COM |
| <b>wins-server</b>                 | 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.   |
| <b>workgroup</b> <i>name</i>       | Specifies the name of the workgroup (or domain) in which the WAAS device resides.  |
| <b>security</b>                    | Sets Kerberos authentication.  |
| <b>ADS</b>                         | Specifies the Active Directory Service.  |

### Defaults

Windows domain options are disabled by default.

|                         |   |
|-------------------------|---|
| <b>Command Modes</b>    | global configuration  |
| <b>Device Modes</b>     | application-accelerator<br>central-manager  |
| <b>Usage Guidelines</b> | <p>Use this global configuration command to set the Windows domain server parameters for a WAAS device.</p> <p>When you enable Kerberos authentication, the default <b>realm</b> is DOMAIN.COM and the <b>security</b> is ADS. If you disable Kerberos authentication, the <b>security</b> is domain.</p>   |
| <b>Note</b>             | WAAS supports authentication by a Windows domain controller running only on Windows Server 2000 or Windows Server 2003.   |
| <b>Examples</b>         | <p>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:</p> <pre>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</pre> <p>The following example shows how to configure the windows domain server when Kerberos authentication is enabled using the <b>kerberos</b> command:</p> <pre>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</pre> |

**Related Commands** [\(config\) kerberos](#)

■ (config) windows-domain

show windows-domain

windows-domain

# Interface Configuration Mode Commands

To set, view, and test the configuration of WAAS software features on a specific interface, use the **interface** global configuration command.

```
interface {GigabitEthernet slot/port | InlineGroup slot/group | PortChannel 1 | Standby 1}
```

|                           |   |
|---------------------------|---|
| <b>Syntax Description</b> | <b>GigabitEthernet</b> <i>slot/port</i> Selects a gigabit ethernet interface to configure.<br><b>InlineGroup</b> <i>slot/group</i> Selects an inline group interface to configure.<br><b>PortChannel 1</b> Selects the port channel interface to configure.<br><b>Standby 1</b> Selects the standby group to configure. |
| <b>Defaults</b>           | No default behavior or values.  |
| <b>Command Modes</b>      | global configuration  |
| <b>Device Modes</b>       | application-accelerator   |
| <b>Usage Guidelines</b>   | <p>Within interface configuration mode, you can use the interface commands (<b>autosense</b>, <b>bandwidth</b>, <b>cdp</b>, etc.) to configure the specified interface.</p> <p>To return to global configuration mode, use the <b>exit</b> command at the interface configuration mode prompt.</p>                      |
| <b>Examples</b>           | <p>The following example shows how to enter interface configuration mode:</p> <pre>WAE(config)# interface gigabitethernet 1/0 WAE(config-if) #</pre>  |
| <b>Related Commands</b>   | <a href="#">(config) interface InlineGroup</a><br><a href="#">(config) interface PortChannel</a><br><a href="#">(config) interface standby</a>  |

---

(config-if) autosense

## (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**

**no autosense**

---

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

---

**Defaults** Autosense is enabled by default.

---

**Command Modes** interface configuration

---

**Device Modes** application-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 shows how to disable autosense on Gigabit Ethernet port 1/0:

```
WAE(config)# interface GigabitEthernet 1/0
WAE(config-if)# no autosense
```

The following example shows how to reenable 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 GigabitEthernet](#)  
[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}**

**no bandwidth {10 | 100 | 1000}**

|                           |   |
|---------------------------|---|
| <b>Syntax Description</b> |   |
| <b>10</b>                 | Sets the link speed to 10 megabits per second (Mbps).   |
| <b>100</b>                | Sets the link speed to 100 Mbps.  |
| <b>1000</b>               | Sets the link speed to 1000 Mbps. This option is not available on all ports and is the same as autosense. |

|                 |                                 |
|-----------------|---------------------------------|
| <b>Defaults</b> | No default behaviors or values. |
|-----------------|---------------------------------|

|                      |                         |
|----------------------|-------------------------|
| <b>Command Modes</b> | interface configuration |
|----------------------|-------------------------|

|                     |  |
|---------------------|--|
| <b>Device Modes</b> | application-accelerator<br>central-manager |
|---------------------|--|

|                         |  |
|-------------------------|--|
| <b>Usage Guidelines</b> | To configure the link speed of a network interface on a WAAS device, use the <b>bandwidth</b> 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 a 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 on the WAE, routers, switches, or other devices. Half duplex impedes the system ability to improve performance and should not be used. Check each Cisco WAE interface and the port configuration on the adjacent device (router, switch, firewall, WAE) to verify that full duplex is configured.

**(config-if) bandwidth****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 GigabitEthernet](#)

## (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** interface configuration command.

**cdp enable**

|                           |               |                              |
|---------------------------|---------------|------------------------------|
| <b>Syntax Description</b> | <b>enable</b> | Enables CDP on an interface. |
|---------------------------|---------------|------------------------------|

|                 |                                |
|-----------------|--------------------------------|
| <b>Defaults</b> | No default behavior or values. |
|-----------------|--------------------------------|

|                      |                         |
|----------------------|-------------------------|
| <b>Command Modes</b> | interface configuration |
|----------------------|-------------------------|

|                     |  |
|---------------------|--|
| <b>Device Modes</b> | application-accelerator<br>central-manager |
|---------------------|--|

|                         |  |
|-------------------------|--|
| <b>Usage Guidelines</b> | Using the <b>cdp enable</b> 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 <b>cdp enable</b> command in interface configuration mode. |
|-------------------------|--|



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
```

|                 |   |
|-----------------|---|
| <b>Examples</b> | The following example shows how to enable CDP on Gigabit Ethernet interface (slot 1/port 0) of the WAAS device: |
|-----------------|---|

```
WAE# configure
WAE(config)# cdp enable
WAE(config)# interface GigabitEthernet 1/0
WAE(config-if)# cdp enable
```

|                         |   |
|-------------------------|---|
| <b>Related Commands</b> | <a href="#">(config) cdp</a><br><a href="#">show cdp</a><br><a href="#">show interface</a><br><a href="#">show running-config</a> |
|-------------------------|---|

■ (config-if) cdp

**show startup-config**

# (config-if) encapsulation dot1Q

To set the VLAN ID that is to be assigned to traffic that leaves a WAE, use the **encapsulation dot1Q** interface configuration command.

**encapsulation dot1Q VLAN**

|                           |             |                      |
|---------------------------|-------------|----------------------|
| <b>Syntax Description</b> | <i>VLAN</i> | VLAN ID from 1–4094. |
|---------------------------|-------------|----------------------|

|                 |                                |
|-----------------|--------------------------------|
| <b>Defaults</b> | No default behavior or values. |
|-----------------|--------------------------------|

|                      |                         |
|----------------------|-------------------------|
| <b>Command Modes</b> | interface configuration |
|----------------------|-------------------------|

|                     |                         |
|---------------------|-------------------------|
| <b>Device Modes</b> | application-accelerator |
|---------------------|-------------------------|

|                         |   |
|-------------------------|---|
| <b>Usage Guidelines</b> | The <b>encapsulation dot1Q</b> command is available only for the inlineGroup interface. |
|-------------------------|---|



If the VLAN ID that you set with the **encapsulation dot1Q** interface command does not match the VLAN ID expected by the router subinterface, you may not be able to connect to the inline interface IP address.

The inline adapter supports only a single VLAN ID for each inline group interface. If you have configured a secondary address from a different subnet on an inline interface, you must have the same secondary address assigned on the router subinterface for the VLAN.

|                 |  |
|-----------------|--|
| <b>Examples</b> | The following example shows how to set a VLAN ID to encapsulate traffic leaving the WAE: |
|-----------------|--|

```
(config)# interface inlineGroup 1/0
(config-if)# encapsulation dot1Q 100
```

|                         |  |
|-------------------------|--|
| <b>Related Commands</b> | <a href="#">(config) interface GigabitEthernet</a><br><a href="#">(config-if) ip</a> |
|-------------------------|--|

**(config-if) exit**

## (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  
central-manager

---

**Examples** The following example shows how to terminate interface configuration mode and return 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** interface configuration command. To disable this function, use the **no** form of this command.

**failover timeout {1 | 3 | 5}**

**no failover timeout {1 | 3 | 5}**

|                           |  |          |  |          |  |          |  |
|---------------------------|--|----------|--|----------|--|----------|--|
| <b>Syntax Description</b> | <table border="0"> <tr> <td><b>1</b></td><td>Specifies the number of seconds to a failover.</td></tr> <tr> <td><b>3</b></td><td>Specifies the number of seconds to a failover.</td></tr> <tr> <td><b>5</b></td><td>Specifies the number of seconds to a failover.</td></tr> </table> | <b>1</b> | Specifies the number of seconds to a failover. | <b>3</b> | Specifies the number of seconds to a failover. | <b>5</b> | Specifies the number of seconds to a failover. |
| <b>1</b>                  | Specifies the number of seconds to a failover.   |          |  |          |  |          |  |
| <b>3</b>                  | Specifies the number of seconds to a failover.   |          |  |          |  |          |  |
| <b>5</b>                  | Specifies the number of seconds to a failover.   |          |  |          |  |          |  |

|                 |                          |
|-----------------|--------------------------|
| <b>Defaults</b> | The default is 1 second. |
|-----------------|--------------------------|

|                      |                         |
|----------------------|-------------------------|
| <b>Command Modes</b> | interface configuration |
|----------------------|-------------------------|

|                     |  |
|---------------------|--|
| <b>Device Modes</b> | application-accelerator<br>central-manager |
|---------------------|--|

|                         |   |
|-------------------------|---|
| <b>Usage Guidelines</b> | The <b>failover timeout</b> 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. |
|-------------------------|---|

|                 |   |
|-----------------|---|
| <b>Examples</b> | The following example shows how to set the failover time limit for the inline group 0 of the adapter that is installed in slot 1 to 5 seconds and then remove that setting: |
|-----------------|---|

```
(config)# interface inlineGroup 1/0
(config-if)# failover timeout 5
(config-if)# no failover timeout 5
```

|                         |  |
|-------------------------|--|
| <b>Related Commands</b> | <a href="#">(config) interface GigabitEthernet</a><br><a href="#">(config-if) inline</a><br><a href="#">(config-if) shutdown</a> |
|-------------------------|--|

(config-if) full-duplex

## (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**

**no 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  
central-manager

**Usage Guidelines** Use this interface command to configure an interface for full duplex. Full duplex allows data to travel in both directions at the same time through an interface or a cable. Half duplex ensures that data travels only 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 on the WAE, routers, switches, or other devices. Half duplex impedes the system ability to improve performance and should not be used. Check each Cisco WAE interface and 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 configure full duplex 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 shows how to disable full duplex:

```
WAE(config-if)# no full-duplex
```

**Related Commands** [\(config-if\) half-duplex](#)

```
(config) interface GigabitEthernet
show interface
show running-config
show startup-config
```

(config-if) half-duplex

## (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**

**no 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  
central-manager

**Usage Guidelines** Use this interface configuration command to configure an interface for half duplex. Full duplex allows data to travel in both directions at the same time through an interface or a cable. Half duplex ensures that data travels only 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 on the WAE, routers, switches, or other devices. Half duplex impedes the system ability to improve performance and should not be used. Check each Cisco WAE interface and 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 configure half duplex 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 shows how to disable half duplex:

```
WAE(config-if)# no half-duplex
```

**Related Commands** [\(config-if\) full-duplex](#)

```
(config) interface GigabitEthernet
show interface
show running-config
show startup-config
```

(config-if) inline

## (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}]
```

```
no inline [vlan {all | native | vlan_list}]
```

| Syntax Description | <b>vlan</b> (Optional) Modifies the VLAN list parameters.<br><b>all</b> Applies the command to all tagged and untagged packets.<br><b>native</b> Specifies untagged packets.<br><b><i>vlan_list</i></b> 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  
central-manager

**Usage Guidelines** The **inline** command is used in the 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,” 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 packetson 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, and 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

## (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]]}
```

```
no ip address {ip-address ip-subnet [secondary] | dhcp [client-id id [hostname name] | hostname name [client-id id]]}
```

| Syntax Description | <b>address</b> Sets the IP address of an interface.<br><i>ip-address</i> IP address.<br><i>ip-subnet</i> IP subnet mask.<br><b>secondary</b> (Optional) Makes this IP address a secondary address.<br><b>dhcp</b> Sets the IP address negotiated over DHCP.<br><b>client-id id</b> (Optional) Specifies the client identifier.<br><b>hostname name</b> (Optional) Specifies the hostname. |
|--------------------|---|
|--------------------|---|

**Defaults** No default behavior or values.

**Command Modes** interface configuration

**Device Modes** application-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 or Cisco WAE Inline Network Adapter. 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
```



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 1
WAE(config-if)# ip address 10.10.10.10 255.0.0.0
```

The following example shows how to delete the IP address configured on the interface:

```
WAE(config-if)# no ip address
```

The following example shows how to enable an interface for DHCP:

```
WAE(config-if)# ip address dhcp
```

The following example shows how to configure 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 GigabitEthernet](#)

[show interface](#)

[show running-config](#)

[show startup-config](#)

---

(config-if) ip access-group

## (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 this command.

**ip access-group {acl-name | acl-num} {in | out}**

**no ip access-group {acl-name | acl-num} {in | out}**

|                           |  |                 |  |                |  |           |  |            |   |
|---------------------------|--|-----------------|--|----------------|--|-----------|--|------------|---|
| <b>Syntax Description</b> | <table border="0"> <tr> <td><i>acl-name</i></td><td>Alphanumeric identifier of up to 30 characters, beginning with a letter that identifies the ACL to apply to the current interface.</td></tr> <tr> <td><i>acl-num</i></td><td>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.</td></tr> <tr> <td><b>in</b></td><td>Applies the specified access list to inbound packets on the current interface.</td></tr> <tr> <td><b>out</b></td><td>Applies the specified access list to outbound packets on the current interface.</td></tr> </table> | <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. | <b>in</b> | Applies the specified access list to inbound packets on the current interface. | <b>out</b> | Applies the specified access list to outbound packets on the current interface. |
| <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.   |                 |  |                |  |           |  |            |   |
| <b>in</b>                 | Applies the specified access list to inbound packets on the current interface.   |                 |  |                |  |           |  |            |   |
| <b>out</b>                | 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  
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 arp-cache](#)  
[\(config\) ip access-list](#)  
[show ip access-list](#)

## (config-if) mtu

To set the interface Maximum Transmission Unit (MTU) packet size, use the **mtu** interface configuration command. To reset the MTU packet size, use the **no** form of this command.

**mtu** *mtusize*

**no mtu** *mtusize*

|                           |   |
|---------------------------|---|
| <b>Syntax Description</b> | <i>mtusize</i> MTU packet size in bytes (88–1500).  |
| <b>Defaults</b>           | No default behavior or values.  |
| <b>Command Modes</b>      | interface configuration   |
| <b>Device Modes</b>       | application-accelerator<br>central-manager  |
| <b>Usage Guidelines</b>   | The MTU is the largest size of IP datagram that can be transferred using a specific data link connection. Use the <b>mtu</b> command to set the maximum packet size in bytes. |
| <b>Examples</b>           | The following example shows how to set the MTU to 1500 bytes and then remove that setting:<br><br>WAE(config-if)# <b>mtu</b> 1500<br>WAE(config-if)# <b>no mtu</b> 1500       |
| <b>Related Commands</b>   | <a href="#">show interface</a><br><a href="#">show running-config</a><br><a href="#">show startup-config</a>  |

---

(config-if) shutdown

## (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**

**no shutdown**

---

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

---

**Defaults** No default behavior or values.

---

**Command Modes** interface configuration

---

**Device Modes** application-accelerator  
central-manager

---

**Usage Guidelines** See the “[\(config\) interface GigabitEthernet](#)” command for alternative syntax.

---

**Examples** The following example shows how to shut 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 GigabitEthernet](#)  
[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** interface configuration command. To restore the default configuration of the interface, use the **no** form of this command.

**standby 1 [primary]**

**no standby 1 [primary]**

### Syntax Description

|                |   |
|----------------|---|
| <b>1</b>       | Configures standby group 1.   |
| <b>primary</b> | (Optional) Defines the active interface in the standby group. By default, the first attached interface is active. |

### Defaults

There are no standby interfaces by default.

### Command Modes

interface configuration

### Device Modes

application-accelerator  
central-manager

### Usage Guidelines

You can associate an interface with a standby group by using the **standby 1** interface configuration command. To make an interface the active interface in a standby group, use the **standby 1 primary** interface configuration command. If you have already associated an interface with a standby group but have not made it the primary interface, you cannot specify the command again to add the primary designation. First, remove the interface from the standby group by using the **no standby 1** command, then reassign it, specifying the **primary** option at the same time.

A physical interface can be a member of a standby group or a port channel, but not both.

### Examples

The following example shows how to create a standby group:

```
WAE# configure
WAE(config)# interface standby 1
WAE(config-if) #
```

The following example shows how to assign 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
```

The following example shows how to add two Gigabit Ethernet interfaces to Standby Group 1 and then assign one of these member interfaces as the active interface in the group:

- a. A Gigabit Ethernet interface (slot 1/port 0) is added to Standby Group 1.

(config-if) standby

```
WAE(config)# interface gigabitEthernet 1/0
WAE(config-if)# standby 1
```

- b. A second Gigabit Ethernet interface (slot 2/port 0) is added to Standby Group 1 and assigned as the primary (active) interface.

```
WAE(config)# interface gigabitEthernet 2/0
WAE(config-if)# standby 1 primary
WAE(config-if)# exit
WAE(config)#
```

The following example shows how to remove 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 GigabitEthernet](#)  
[show interface](#)  
[show running-config](#)  
[show startup-config](#)

# Standard ACL Configuration Mode Commands

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 this command.

**ip access-list standard {acl-name | acl-num}**

**no ip access-list standard {acl-name | acl-num}**

|                           |   |
|---------------------------|---|
| <b>Syntax Description</b> | <p><b>standard</b> 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:<br/>WAE(config-std-nacl) #</p> |
| <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  
central-manager

**Usage Guidelines** 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 the **exit** command at the ACL configuration mode prompt.

To create an entry, use the **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.

**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.

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 beginning with a letter, or identify a new or existing access list beginning 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 shows how to create 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 example shows how to 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 arp-cache](#)  
[show ip access-list](#)  
[\(config\) 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

## (config-std-nacl) delete

To delete a line from the standard IP ACL, use the **delete** standard ACL configuration command.

**delete** *line-num*

---

|                    |                 |   |
|--------------------|-----------------|---|
| Syntax Description | <i>line-num</i> | Entry at a specific line number in the access list. |
|--------------------|-----------------|---|

---

**Defaults** No default behavior or values.

**Command Modes** standard ACL configuration mode

**Device Modes** application-accelerator  
central-manager

**Examples** The following example shows how to delete 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** standard ACL configuration command. To negate a standard IP ACL, use the **no** form of this command.

**[insert line-num] deny {source-ip [wildcard] | host source-ip | any}**

**no deny {source-ip [wildcard] | host source-ip | any}**

|                    |  |
|--------------------|--|
| Syntax Description | <b>insert line-num</b> (Optional) Inserts the conditions following the specified line number into the access list.<br><b>deny</b> Causes packets that match the specified conditions to be dropped.<br><b>source-ip</b> 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).<br><b>wildcard</b> (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.<br><b>Note</b> For standard IP ACLs, the <i>wildcard</i> parameter of the <b>ip access-list</b> command is always optional. If the <b>host</b> keyword is specified for a standard IP ACL, then the <i>wildcard</i> parameter is not allowed.<br><b>host source-ip</b> Matches the following IP address.<br><b>any</b> 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  
central-manager

**Usage Guidelines** To create an entry, use the **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

---

(config-std-nacl) deny

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 shows how to create a 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  
central-manager

**Examples** The following example shows how to terminate standard ACL configuration mode and return to global configuration mode:

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

(config-std-nacl) list

## (config-std-nacl) list

To display a list of specified entries within the standard IP ACL, use the **list** standard ACL configuration command.

**list [start-line-num [end-line-num]]**

|                    |  |
|--------------------|--|
| Syntax Description | <i>start-line-num</i> (Optional) Line number from which the list begins.<br><i>end-line-num</i> (Optional) Last line number in the list. |
|--------------------|--|

**Defaults** No default behavior or values.

**Command Modes** standard ACL configuration mode

**Device Modes** application-accelerator  
central-manager

**Examples** The following example shows how to display 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** standard ACL configuration 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  
central-manager

**Examples** The following example shows how to move 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

## (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** standard ACL configuration command. To negate a standard IP ACL, use the **no** form of this command.

**[insert line-num] permit {source-ip [wildcard] | host source-ip | any}**

**no permit {source-ip [wildcard] | host source-ip | any}**

|                    |   |
|--------------------|---|
| Syntax Description | <b>insert</b> <i>line-num</i> (Optional) Inserts the conditions following the specified line number into the access list.<br><b>source-ip</b> 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).<br><b>wildcard</b> (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.<br><b>Note</b> For standard IP ACLs, the <i>wildcard</i> parameter of the <b>ip access-list</b> command is always optional. If the <b>host</b> keyword is specified for a standard IP ACL, then the <i>wildcard</i> parameter is not allowed.<br><b>host</b> <i>source-ip</i> Matches the following IP address.<br><b>any</b> 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  
central-manager

**Usage Guidelines** To create an entry, use the **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 shows how to create a 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 this command.

```
ip access-list extended {acl-name | acl-num}
no ip access-list extended {acl-name | acl-num}
```

| Syntax Description |   |
|--------------------|---|
|                    | <b>extended</b> 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:<br>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, valid values range from 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  
central-manager

**Usage Guidelines** 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 the **exit** command 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.

**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.

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 limit 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 arp-cache](#)  
[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** extended ACL configuration command.

**delete** *line-num*

|                    |   |
|--------------------|---|
| Syntax Description | <i>line-num</i><br>Entry at a specific line number in the access list.  |
| Defaults           | No default behavior or values.  |
| Command Modes      | extended ACL configuration mode   |
| Device Modes       | application-accelerator<br>central-manager  |
| Examples           | The following example shows how to delete line 10 from the extended ACL testextacl:<br><br>WAE(config)# <b>ip access-list extended testextacl</b><br>WAE(config-ext-nacl)# <b>delete 10</b> |
| Related Commands   | <a href="#">(config-ext-nacl) list</a><br><a href="#">(config-ext-nacl) move</a>  |

(config-ext-nacl) deny

## (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** extended ACL configuration 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 | <b>insert</b> <i>line-num</i> | (Optional) Specifies to insert the conditions following the specified line number into the access list.  |
|                    | <b>gre</b>                    | Specifies to match packets using the Generic Routing Encapsulation protocol.   |
|                    | <b>icmp</b>                   | Specifies to match ICMP packets.   |
|                    | <b>tcp</b>                    | Specifies to match packets using the TCP protocol.   |
|                    | <b>udp</b>                    | Specifies to match packets using the UDP protocol.   |
|                    | <b>ip</b>                     | Specifies to match all IP packets.   |
|                    | <b>proto-num</b>              | IP protocol number.  |
|                    | <b>source-ip</b>              | 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) Wildcard. The notation is in 4-digit, dotted-decimal format. The bits to match are identified by a digital value of 0; the bits to ignore are identified by a 1.  |
|                              | For extended IP ACLs, the <i>wildcard</i> parameter of the <b>ip access-list</b> command is always optional. If the <b>host</b> keyword is specified for a extended IP ACL, then the <i>wildcard</i> parameter is not allowed.   |
| <b>host</b> <i>source-ip</i> | Specifies to match the following IP address.   |
| <b>any</b>                   | Specifies to match any IP address.   |
| <b>dest-ip</b>               | Specifies 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).  |
| <b>operator port</b>         | (Optional) Operator to use with specified ports, where <b>lt</b> = less than, <b>gt</b> = greater than, <b>eq</b> = equal to, <b>neq</b> = not equal to, and <b>range</b> = an inclusive range.<br><br>The port value is a number (0–65535) or a keyword; two port numbers are required with the <b>range</b> keyword. See the “Usage Guidelines” section for a listing of the UDP and TCP keywords. |
| <b>established</b>           | (Optional) Specifies to match 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) Code type is 0–255.   |
| <i>icmp-msg</i>              | (Optional) Match a 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

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. 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

```
(config-ext-nacl) deny
```

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. 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 conditions.

**Table 3-1** lists the UDP keywords that you can use with extended access lists.

**Table 3-1 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 3-2** lists the TCP keywords that you can use with extended access lists.

**Table 3-2 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 3-2** 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 3-3 lists the keywords that you can use to match specific ICMP message types and codes.

**Table 3-3** 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 limit 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  
central-manager

**Examples** The following example shows how to terminate extended ACL configuration mode and return to global configuration mode:

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

---

(config-ext-nacl) list

## (config-ext-nacl) list

To display a list of specified entries within the extended ACL, use the **list** extended ACL configuration command.

**list [start-line-num [end-line-num]]**

|                    |  |
|--------------------|--|
| Syntax Description | <i>start-line-num</i> (Optional) Line number from which the list begins.<br><i>end-line-num</i> (Optional) Last line number in the list. |
|--------------------|--|

---

**Defaults** No default behavior or values.

---

**Command Modes** extended ACL configuration mode

---

**Device Modes** application-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** extended ACL configuration 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. |

**Defaults** No default behavior or values.

**Command Modes** extended ACL configuration mode

**Device Modes** application-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

## (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** extended ACL configuration 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 | <b>insert</b> <i>line-num</i> | (Optional) Specifies to insert the conditions following the specified line number into the access list.  |
|                    | <b>gre</b>                    | Specifies to match packets using the Generic Routing Encapsulation protocol.   |
|                    | <b>icmp</b>                   | Specifies to match ICMP packets.   |
|                    | <b>tcp</b>                    | Specifies to match packets using the TCP protocol.   |
|                    | <b>udp</b>                    | Specifies to match packets using the UDP protocol.   |
|                    | <b>ip</b>                     | Specifies to match all IP packets.   |
|                    | <b>proto-num</b>              | IP protocol number.  |
|                    | <b>source-ip</b>              | 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) Wildcard. The notation is in 4-digit, dotted-decimal format. The bits to match are identified by a digital value of 0; the bits to ignore are identified by a 1.  |
|                              | For extended IP ACLs, the <i>wildcard</i> parameter of the <b>ip access-list</b> command is always optional. If the <b>host</b> keyword is specified for a extended IP ACL, then the <i>wildcard</i> parameter is not allowed.   |
| <b>host</b> <i>source-ip</i> | Specifies to match the following IP address.   |
| <b>any</b>                   | Specifies to match any IP address.   |
| <b>dest-ip</b>               | Specifies 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).  |
| <b>operator port</b>         | (Optional) Operator to use with specified ports, where <b>lt</b> = less than, <b>gt</b> = greater than, <b>eq</b> = equal to, <b>neq</b> = not equal to, and <b>range</b> = an inclusive range.<br><br>The port value is a number (0–65535) or a keyword; two port numbers are required with the <b>range</b> keyword. See the “Usage Guidelines” section for a listing of the UDP and TCP keywords. |
| <b>established</b>           | (Optional) Specifies to match 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) Code type is 0–255.   |
| <i>icmp-msg</i>              | (Optional) Match a 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

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. 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

(config-ext-nacl) permit

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. 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 3-4** lists the UDP keywords that you can use with extended access lists.

**Table 3-4 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 3-5** lists the TCP keywords that you can use with extended access lists.

**Table 3-5 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 3-5 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 3-6 lists the keywords that you can use to match specific ICMP message types and codes.

**Table 3-6 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 limit 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](#)

# Preposition Configuration Mode Commands

To create and modify preposition directives on a WAAS device for prepositioning files for WAFS, use the **accelerator cifs preposition** global configuration command.

**accelerator cifs preposition *directive\_id***

|                           |                     |   |
|---------------------------|---------------------|---|
| <b>Syntax Description</b> | <i>directive_id</i> | Preposition directive ID of an existing preposition directive that you want to change or a new directive that you want to create. |
|---------------------------|---------------------|---|

|                 |                                |
|-----------------|--------------------------------|
| <b>Defaults</b> | No default behavior or values. |
|-----------------|--------------------------------|

|                      |                      |
|----------------------|----------------------|
| <b>Command Modes</b> | global configuration |
|----------------------|----------------------|

|                     |                         |
|---------------------|-------------------------|
| <b>Device Modes</b> | application-accelerator |
|---------------------|-------------------------|

|                         |  |
|-------------------------|--|
| <b>Usage Guidelines</b> | Use the <b>accelerator cifs preposition</b> command to create and edit preposition directives to be used with the transparent CIFS accelerator. A preposition directive defines a set of files that are to be prepositioned on the WAE device. |
|-------------------------|--|

Within preposition configuration mode, you can use the various commands (**server**, **root**, **scan-type**, **schedule**, and so on) to configure a preposition directive. To return to global configuration mode, enter the **exit** command at the preposition configuration mode prompt.



We recommend that you use the WAAS Central Manager GUI to configure preposition directives. For more information, see the “[Creating a Preposition Directive](#)” section in the *Cisco Wide Area Application Services Configuration Guide*.

|                 |  |
|-----------------|--|
| <b>Examples</b> | The following example shows how to enter preposition configuration mode and configure a preposition directive using the <b>accelerator cifs preposition</b> command: |
|-----------------|--|

```
WAE(config)# accelerator cifs preposition 1
WAE(config-preposition)#
```

|                         |   |
|-------------------------|---|
| <b>Related Commands</b> | <a href="#">(config) accelerator cifs</a> |
|-------------------------|---|

**(config-preposition) credentials**

# (config-preposition) credentials

To set the username and password credentials for a the file server in a preposition directive, use the **credentials** preposition configuration command.

```
credentials username username password {0 | 1} password}
```

|                    |   |
|--------------------|---|
| Syntax Description | <b>username <i>username</i></b> Specifies the username.<br><b>password {0   1} <i>password</i></b> Specifies the password. To indicate that the password string is unencrypted, specify <b>0</b> . To indicated that the password string is encrypted, specify <b>1</b> . |
|--------------------|---|

|                 |                                |
|-----------------|--------------------------------|
| <b>Defaults</b> | No default behavior or values. |
|-----------------|--------------------------------|

|                      |                                |
|----------------------|--------------------------------|
| <b>Command Modes</b> | preposition configuration mode |
|----------------------|--------------------------------|

|                     |                         |
|---------------------|-------------------------|
| <b>Device Modes</b> | application-accelerator |
|---------------------|-------------------------|

|                 |   |
|-----------------|---|
| <b>Examples</b> | The following example shows how to set the username and password credentials: |
|-----------------|---|

```
WAE(config)# accelerator cifs preposition 3
WAE(config-preposition)# credentials username ramyav password 0 ux5TjW8r
```

|                         |   |
|-------------------------|---|
| <b>Related Commands</b> | <a href="#">(config-preposition) server</a> |
|-------------------------|---|

# (config-preposition) dscp

To set the DSCP marking value for a preposition task, use the **dscp** preposition configuration command. To remove a DSCP marking value, use the **no** form of this command.

**dscp value**

**no dscp value**

|                    |   |
|--------------------|---|
| Syntax Description | <i>value</i><br>DSCP marking value to assign to prepositioning traffic.   |
| Defaults           | No default behavior or values.  |
| Command Modes      | preposition configuration mode  |
| Device Modes       | application-accelerator   |
| Usage Guidelines   | <p>This command specifies the DSCP marking value to be used for prepositioning traffic. DSCP is a field in an IP packet that enables different levels of service to be assigned to the network traffic. The levels of service are assigned by marking each packet on the network with a DSCP code and associating a corresponding level of service. DSCP is the combination of IP Precedence and Type of Service (ToS) fields. For more information, see RFC 2474.</p> <p>For details on the valid DSCP marking values, see <a href="#">Table 3-2 on page -537</a>.</p> |
| Examples           | The following example shows how to set the DSCP marking value to cs7:<br><br><pre>WAE(config)# accelerator cifs preposition 3 WAE(config-preposition)# dscp cs7</pre>   |
| Related Commands   | <a href="#">(config) policy-engine application set-dscp</a>   |

---

(config-preposition) duration

## (config-preposition) duration

To set the maximum duration for a preposition task, use the **duration** preposition configuration command. To remove a duration limit, use the **no** form of this command.

**duration** *minutes*

**no duration** *minutes*

---

|                    |                |  |
|--------------------|----------------|--|
| Syntax Description | <i>minutes</i> | Maximum number of minutes that the preposition task is allowed to run. |
|--------------------|----------------|--|

---

**Defaults** No default behavior or values.

**Command Modes** preposition configuration mode

**Device Modes** application-accelerator

**Usage Guidelines** This command specifies the maximum amount of time that the WAAS software should take to complete the preposition task. If the software takes longer than this amount of time, the software stops the prepositioning process before all files are copied to the Edge WAE cache. If the preposition task does not start at the scheduled start time (for example, because the Edge and the Core have no connection), the start retries are counted in the duration. If you do not specify a value for this command, WAAS takes as much time as needed to export this file server.

**Examples** The following example shows how to set the maximum task duration to 60 minutes:

```
WAE(config)# accelerator cifs preposition 3
WAE(config-preposition)# duration 60
```

**Related Commands** [\(config-preposition\) schedule](#)

## (config-preposition) enable

To enable a preposition directive, use the **enable** preposition configuration command. To disable a preposition directive, use the **no** form of this command.

**enable**

**no enable**

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

**Defaults** Not enabled.

**Command Modes** preposition configuration mode

**Device Modes** application-accelerator

**Examples** The following example shows how to enable a preposition directive:

```
WAE(config)# accelerator cifs preposition 5  
WAE(config-preposition)# enable
```

**Related Commands** [\(config\) accelerator cifs preposition](#)

(config-preposition) ignore-hidden-dir

## (config-preposition) ignore-hidden-dir

To ignore hidden directories in the set of files to be prepositioned, use the **ignore-hidden-dir** preposition configuration command.

### ignore-hidden-dir

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

**Defaults** Hidden directories are not ignored.

**Command Modes** preposition configuration mode

**Device Modes** application-accelerator

**Examples** The following example shows how to prevent hidden directories from being prepositioned:

```
WAE(config)# accelerator cifs preposition 3
WAE(config-preposition)# ignore-hidden-dir
```

**Related Commands** [\(config-preposition\) root](#)

# (config-preposition) max-cache

To set the maximum percentage of the cache that the files from a preposition directive can use, use the **max-cache** preposition configuration command.

**max-cache** *percentage*

|                    |  |  |
|--------------------|--|--|
| Syntax Description | <i>percentage</i>  | Integer from 1–100 that specifies a percentage of the overall Edge WAE cache that prepositioned files can consume. |
| Defaults           | 5  |  |
| Command Modes      |  | Preposition configuration mode   |
| Device Modes       |  | application-accelerator  |
| Examples           | The following example shows how to set the maximum cache percentage to 10 percent:           |  |
|                    | <pre>WAE(config)# accelerator cifs preposition 3 WAE(config-preposition)# max-cache 10</pre> |  |
| Related Commands   | <a href="#">(config-preposition) max-file-size</a>   |  |

---

(config-preposition) max-file-size

## (config-preposition) max-file-size

To set the maximum size file that can be prepositioned, use the **max-file-size** preposition configuration command. To remove this limit, use the **no** form of this command.

**max-file-size** *size\_in\_kb*

**no max-file-size** *size\_in\_kb*

|                    |  |   |
|--------------------|--|---|
| Syntax Description | <i>size_in_kb</i>  | Number of kilobytes of the maximum file size. |
| Defaults           | No default behavior or values.   |   |
| Command Modes      | preposition configuration mode   |   |
| Device Modes       | application-accelerator  |   |
| Usage Guidelines   | Files that are larger than the specified size are not prepositioned.   |   |
| Examples           | The following example shows how to set the maximum file size to 1000 KB:<br><br>WAE(config)# <b>accelerator cifs preposition 3</b><br>WAE(config-preposition)# <b>max-file-size 1000</b> |   |
| Related Commands   | <a href="#">(config-preposition) max-cache</a>   |   |

# (config-preposition) min-file-size

To set the minimum size file that can be prepositioned, use the **min-file-size** preposition configuration command. To remove this limit, use the **no** form of this command.

**min-file-size** *size\_in\_kb*

**no min-file-size** *size\_in\_kb*

|                    |  |
|--------------------|--|
| Syntax Description | <i>size_in_kb</i> Number of kilobytes of the minimum file size.  |
| Defaults           | 20 KB  |
| Command Modes      | preposition configuration mode   |
| Device Modes       | application-accelerator  |
| Usage Guidelines   | Files that are smaller than the specified size are not prepositioned.  |
| Examples           | The following example shows how to set the minimum file size to 50 KB:<br><pre>WAE(config)# accelerator cifs preposition 3 WAE(config-preposition)# min-file-size 50</pre> |
| Related Commands   | <a href="#">(config-preposition) max-file-size</a>   |

■ **(config-preposition) name**

## (config-preposition) name

To set the display name of a preposition directive, use the **name** preposition configuration command.

**name** *name*

|                    |             |                                  |
|--------------------|-------------|----------------------------------|
| Syntax Description | <i>name</i> | Name of a preposition directive. |
|--------------------|-------------|----------------------------------|

**Defaults** The default name is New preposition directive *n*.

**Command Modes** preposition configuration mode

**Device Modes** application-accelerator

**Examples** The following example shows how to set the preposition directive name:

```
WAE(config)# accelerator cifs preposition 3
WAE(config-preposition)# name working_files
```

**Related Commands** [\(config-preposition\) enable](#)

# (config-preposition) pattern

To filter the files included for a preposition directive, use the **pattern** preposition configuration command. To remove this filter, use the **no** form of this command.

**pattern {equals | starts-with | ends-with | contains} text**

**no pattern {equals | starts-with | ends-with | contains} text**

|                    |   |
|--------------------|---|
| Syntax Description | <b>equals</b> Specifies to limit the selected files to those filenames that are equal to the specified text.<br><b>starts-with</b> Specifies to limit the selected files to those filenames that start with the specified text.<br><b>ends-with</b> Specifies to limit the selected files to those filenames that end with the specified text.<br><b>contains</b> Specifies to limit the selected files to those filenames that contain the specified text.<br><b>text</b> Text string that filters the selected files based on the pattern option. |
|--------------------|---|

**Defaults** No default behavior or values.

**Command Modes** preposition configuration mode

**Device Modes** application-accelerator

**Examples** The following example shows how to set a pattern filter to select only files that end with .doc:

```
WAE(config)# accelerator cifs preposition 3
WAE(config-preposition)# pattern ends-with .doc
```

**Related Commands** [\(config-preposition\) root](#)

---

(config-preposition) recursive

## (config-preposition) recursive

To include files in subdirectories for a preposition directive, use the **recursive** preposition configuration command. To not include subdirectories, use the **no** form of this command.

**recursive**

**no recursive**

---

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

---

**Defaults** Subdirectories are included.

---

**Command Modes** preposition configuration mode

---

**Device Modes** application-accelerator

---

**Examples** The following example shows how to exclude subdirectories from prepositioning:

```
WAE(config)# accelerator cifs preposition 3  
WAE(config-preposition)# no recursive
```

---

**Related Commands** [\(config-preposition\) root](#)

# (config-preposition) root

To set a root directory for a preposition directive, use the **root** preposition configuration command.

**root** *path*

|                    |   |
|--------------------|---|
| Syntax Description | <i>path</i><br>Full pathname to the directory, not including the server name.   |
| Defaults           | No default behavior or values.  |
| Command Modes      | preposition configuration mode  |
| Device Modes       | application-accelerator   |
| Usage Guidelines   | You can configure multiple root directories by executing this command multiple times for a preposition directive.   |
| Examples           | The following example shows how to set a root preposition directory:<br><br>WAE(config)# <b>accelerator cifs preposition 3</b><br>WAE(config-preposition)# <b>root home/working</b>             |
| Related Commands   | <a href="#">(config-preposition) pattern</a><br><a href="#">(config-preposition) recursive</a><br><a href="#">(config-preposition) scan-type</a><br><a href="#">(config-preposition) server</a> |

(config-preposition) scan-type

# (config-preposition) scan-type

To set the file scanning type for a preposition directive, use the **scan-type** preposition configuration command.

```
scan-type {full | since last | since period units}
```

| Syntax Description |  |
|--------------------|--|
|                    | <b>full</b> Specifies to copy all files to the Edge WAE cache.   |
|                    | <b>since last</b> Specifies to copy only the files that have changed since the last preposition to the Edge WAE cache. This differential filter is applied from the second iteration of a task execution onward.<br><br>If a new directory is moved to an already prepositioned directory (without changing its last-modified time), this new directory is not prepositioned during the next prepositioning session when you choose this option. |
|                    | <b>since period units</b> Specifies to copy only the files that have changed within the specified period. Period values are the number of minutes, hours, days, or weeks (depending on the units specified). Unit values are <b>min</b> , <b>hour</b> , <b>day</b> , or <b>week</b> .  |

**Defaults** Full

**Command Modes** preposition configuration mode

**Device Modes** application-accelerator

**Examples** The following example shows how to set the scan-type for a preposition directive:

```
WAE(config)# accelerator cifs preposition 3
WAE(config-preposition)# scan-type since last
```

**Related Commands**
[\(config-preposition\) recursive](#)
  
[\(config-preposition\) root](#)

# (config-preposition) schedule

To set the schedule for starting a preposition task, use the **schedule** preposition configuration command.

```
schedule {now |
    daily time |
    date date time |
    weekly {dayname [dayname]...} time time |
    monthly {week-day dayname weeknumber time time | {day day [day]...} } time time}
```

| Syntax Description | <b>now</b>                         | Specifies that prepositioning occurs within a few minutes of submitting the schedule.   |
|--------------------|------------------------------------|---|
|                    | <b>daily time</b>                  | Specifies that prepositioning occurs daily at the defined time at which to run the prepositioning task, in the following format: <i>hh:mm</i> , where <i>hh</i> is the hour (00–23) and <i>mm</i> is the minutes (00–59).<br>Hours are in 24-hour format, as in the following example: 23:01  |
|                    | <b>date date time</b>              | Specifies that prepositioning occurs at the defined time and date at which to run the prepositioning task, in the following format: <i>DD:MM:YYYY</i> , where <i>DD</i> is the day (01–31), <i>MM</i> is the month (01–12), and <i>YYYY</i> is the year (1993–2035). The time is in the following format: <i>hh:mm</i> , where <i>hh</i> is the hour (00–23) and <i>mm</i> is the minutes (00–59).<br>Example: 28:09:2008 23:01 |
|                    | <b>weekly dayname</b>              | Specifies that prepositioning occurs on the selected days of the week at the defined time. To specify multiple days, separate them with spaces, as follows: Monday Tuesday  |
|                    | <b>time time</b>                   | Specifies the time to run the preposition task on the specified days.   |
|                    | <b>monthly</b>                     | Specifies that prepositioning occurs on the selected days or dates of the month at the defined time.  |
|                    | <b>week-day dayname weeknumber</b> | Specifies a named day of the week and week of the month to start preposition. Only one day is allowed. Week number values are 1–4.  |
|                    | <b>day day</b>                     | Specifies a numbered day of the month (integer). To specify multiple days, separate them with spaces, as follows: day 1 6 11 16 21 26 31.   |

|                      |  |
|----------------------|--|
| <b>Defaults</b>      | now  |
| <b>Command Modes</b> | preposition configuration mode   |
| <b>Device Modes</b>  | application-accelerator  |
| <b>Examples</b>      | The following example shows how to set the preposition task to run daily at 11:30 p.m.:<br><br>WAE(config)# <b>accelerator cifs preposition 3</b><br>WAE(config-preposition)# <b>schedule daily 23 30 00</b> |

**(config-preposition) schedule**

The following example shows how to set the preposition task to run on December 15, 2008 at midnight:

```
WAE(config-preposition)# schedule date 15:12:2008 00:00
```

The following example shows how to set the preposition task to run weekly on Wednesdays and Fridays at 8 p.m.:

```
WAE(config-preposition)# schedule weekly Wednesday Friday time 20:00
```

The following example shows how to set the preposition task to run monthly on the 1st and 15th days at 1:00 a.m.:

```
WAE(config-preposition)# schedule monthly day 1 time 15 1:00
```

**Related Commands** [\*\*\(config-preposition\) duration\*\*](#)

# (config-preposition) server

To set a server name for a preposition directive, use the **server** preposition configuration command.

**server** *name*

|                    |  |
|--------------------|--|
| Syntax Description | <i>name</i><br>Server name.  |
| Defaults           | No default behavior or values.   |
| Command Modes      | preposition configuration mode   |
| Device Modes       | application-accelerator  |
| Examples           | The following example shows how to set a server name for a preposition directive:<br><br>WAE(config)# <b>accelerator cifs preposition 3</b><br>WAE(config-preposition)# <b>server win12srv</b> |
| Related Commands   | <a href="#">(config-preposition) credentials</a><br><a href="#">(config-preposition) root</a>  |

■ (config-preposition) server

# Virtual Blade Configuration Mode Commands

To configure virtual blades on a WAE device, use the **virtual-blade** global configuration command. To disable a virtual blade, use the **no** form of this command.

**virtual-blade** *virtual-blade-number*

**no virtual-blade** *virtual-blade-number*

---

|                           |                             |  |
|---------------------------|-----------------------------|--|
| <b>Syntax Description</b> | <i>virtual-blade-number</i> | Number of the virtual blade that you want to configure. The range of valid values depends on the number of virtual blades that your WAE or WAVE appliance can support. |
|---------------------------|-----------------------------|--|

---

|                 |                                |
|-----------------|--------------------------------|
| <b>Defaults</b> | No default behavior or values. |
|-----------------|--------------------------------|

|                      |                      |
|----------------------|----------------------|
| <b>Command Modes</b> | global configuration |
|----------------------|----------------------|

|                     |                         |
|---------------------|-------------------------|
| <b>Device Modes</b> | application-accelerator |
|---------------------|-------------------------|

|                         |   |
|-------------------------|---|
| <b>Usage Guidelines</b> | Use the <b>virtual-blade</b> command to configure virtual blades on a WAAS device that supports virtual blades. This command initiates the virtual blade configuration mode as indicated by the (config-vb) prompt. |
|-------------------------|---|

Within virtual blade configuration mode, you can use the various commands (**device**, **disk**, **interface**, and so on) to define the resource parameters for the virtual blade. To return to global configuration mode, enter the **exit** command.

|                 |   |
|-----------------|---|
| <b>Examples</b> | The following example shows how to edit virtual blade 2 and put your WAE into virtual blade configuration mode: |
|-----------------|---|

```
WAE(config)# virtual-blade 2
WAE(config-vb) #
```

The following example shows that the prompt changes to (config-vb) to indicate virtual blade mode.

```
WAE(config-vb) # description This-is-my-virtual-blade-description
WAE(config-vb) # exit
WAE(config) #
```

---

|                         |   |
|-------------------------|---|
| <b>Related Commands</b> | <a href="#">(config-vb) autostart</a><br><a href="#">(config-vb) boot</a> |
|-------------------------|---|

(config-vb) description  
(config-vb) device  
(config-vb) disk  
(config-vb) interface  
(config-vb) memory  
(config-vb) vnc

# (config-vb) autostart

To set a virtual blade to automatically start when the WAE is started, use the **autostart** virtual blade configuration command. To prevent a virtual blade from starting automatically, use the **no** form of this command.

**autostart**

**no autostart**

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

**Defaults** No default behavior or values.

**Command Modes** virtual blade configuration mode

**Device Modes** application-accelerator

**Examples** The following example shows how to configure virtual blade 2 to start automatically when the WAE restarts:

```
WAE(config)# virtual-blade 2
WAE(config-vb)# autostart
```

**Related Commands**

- [\(config-vb\) boot](#)
- [\(config-vb\) description](#)
- [\(config-vb\) device](#)
- [\(config-vb\) disk](#)
- [\(config-vb\) interface](#)
- [\(config-vb\) memory](#)

(config-vb) boot

## (config-vb) boot

To configure the boot image location and source for a virtual blade, use the **boot** virtual blade configuration command.

```
boot {cd-image {cd-rom | disk location} | fd-image disk location | from {cd-rom | disk}}
```

|                           |   |
|---------------------------|---|
| <b>Syntax Description</b> | <b>cd-image</b> Specifies the location of the boot CD image for the virtual blade. This image can be located on a CD in the WAE CD-ROM drive or it can be an ISO file located on the WAE hard drive.<br><b>cd-rom</b> Specifies that the CD image location is a physical CD in the WAE CD-ROM drive.<br><b>disk <i>location</i></b> Specifies that the CD image location is an ISO file on the WAE hard drive (for example, /local1/vbs/windows_2003.iso).<br><b>fd-image <i>disk location</i></b> Specifies the location of the floppy disk image for the virtual blade. This image file must be located on the WAE hard drive (for example, /local1/vbs/fdimage).<br><b>from</b> Specifies the source from which the virtual blade will boot. The boot source (defined by the <b>boot cd-image</b> command) can be a physical CD or a CD image.<br><b>cd-rom</b> Specifies that the virtual blade boots from a physical CD or a CD image (.iso image file stored in the /local1/vbs directory). If you specify this option, the <b>cd-image</b> option is required and configures the location of the boot image.<br><b>disk</b> Specifies that the virtual blade boots from a guest OS installed on the WAE hard drive. If you specify this option, the <b>cd-image</b> option is optional and configures the location of a CD-ROM image that is made available to the guest OS (but is not used for booting). |
|---------------------------|---|

**Defaults**      No default behavior or values.

**Command Modes**      virtual blade configuration mode

**Device Modes**      application-accelerator

**Usage Guidelines**      The floppy disk image and bootable CD-ROM image must be located in the /local1/vbs directory. The path used with the **boot cd-image disk** and **boot fd-image disk** commands must be /local1/vbs/*filename*. The CD-ROM image can be used to boot the operating system running on the virtual blade. The floppy disk image reserves resources for an emulated floppy disk drive on the virtual blade.

Use the **boot from cd-rom** option before you have installed a guest OS, to boot from a guest OS installer CD (a physical CD or an .iso file located in /local1/vbs).

Use the **boot from disk** option after you have installed a guest OS, to boot from the installed guest OS.

If you specified **boot from disk**, the **cd-image** keyword is optional and configures the location of a CD-ROM image that is made available to the guest OS (but is not used for booting). The CD image can be changed during operation, by using the **virtual-blade n cd eject** EXEC command followed by the **virtual-blade n cd disk /local1/vbs/newimage.iso** or the **virtual-blade n cd cd-rom** EXEC command.

---

**Examples**

The following example shows how to configure virtual blade 2 to boot from a CD image file (such as a guest OS installer CD) located on the WAE hard disk:

```
WAE(config)# virtual-blade 2
WAE(config-vb)# boot from cd-rom
WAE(config-vb)# boot cd-image disk /local1/vbs/windows_2003.iso
```

The following example shows how to configure virtual blade 1 to boot from a CD-ROM located in the WAE optical drive:

```
WAE(config)# virtual-blade 1
WAE(config-vb)# boot from cd-rom
WAE(config-vb)# boot cd-image cd-rom
```

The following example shows how to configure virtual blade 1 to boot from a previously installed guest OS installed on the WAE hard disk:

```
WAE(config)# virtual-blade 1
WAE(config-vb)# boot from disk
```

---

**Related Commands**

[\(config-vb\) autostart](#)  
[\(config-vb\) description](#)  
[\(config-vb\) device](#)  
[\(config-vb\) disk](#)  
[\(config-vb\) interface](#)  
[\(config-vb\) memory](#)

**(config-vb) description**

# (config-vb) description

To enter a description for a virtual blade on your WAE, use the **description** virtual blade configuration command.

**description** *description-text*

|                    |                         |   |
|--------------------|-------------------------|---|
| Syntax Description | <i>description-text</i> | Text to briefly describe the virtual blade. |
|--------------------|-------------------------|---|

**Defaults** No default behavior or values.

**Command Modes** virtual blade configuration mode

**Device Modes** application-accelerator

**Examples** The following example shows how to define the descriptive text for virtual blade 2 as “Windows Server 2003”:

```
WAE(config)# virtual-blade 2
WAE(config-vb)# description Windows Server 2003
```

**Related Commands**

- [\(config-vb\) autostart](#)
- [\(config-vb\) boot](#)
- [\(config-vb\) device](#)
- [\(config-vb\) disk](#)
- [\(config-vb\) interface](#)
- [\(config-vb\) memory](#)

# (config-vb) device

To set the device emulation parameters used by the virtual blade on your WAE, use the **device** virtual blade configuration command.

```
device {cpu {qemu64 | qemu32} | nic {rtl8139 | E1000 | virtio} | disk {IDE | virtio} | keyboard {emulation}}
```

## Syntax Description

|                                  |   |
|----------------------------------|---|
| <b>cpu</b>                       | Specifies the CPU emulation to be used on the virtual blade.                    |
| <b>qemu64</b>                    | Specifies a 64-bit processor emulator.  |
| <b>qemu32</b>                    | Specifies a 32-bit processor emulator   |
| <b>nic</b>                       | Specifies the network interface card emulation to be used on the virtual blade. |
| <b>rtl8139</b>                   | Specifies a Realtek network card emulator.                                      |
| <b>E1000</b>                     | Specifies an Intel PRO/1000 network card emulator.                              |
| <b>virtio</b>                    | Specifies a generic NIC emulator optimized for virtual machines.                |
| <b>disk</b>                      | Specifies the type of hard drive emulation to be used on the virtual blade.     |
| <b>IDE</b>                       | Specifies an IDE (ATA) type disk emulator.                                      |
| <b>virtio</b>                    | Specifies a generic disk controller emulator optimized for virtual machines.    |
| <b>keyboard</b> <i>emulation</i> | Specifies the keyboard device emulation. See Usage Guidelines for values.       |

## Defaults

The default values are as follows:

- **device cpu qemu64**
- **device nic rtl8139**
- **device disk IDE**
- **device keyboard en-us**

## Command Modes

virtual blade configuration mode

## Device Modes

application-accelerator

## Usage Guidelines

[Table 3-1](#) shows valid values for keyboard device emulation.

**Table 3-1 Keyboard Device Emulation Values**

| Emulation | Value |
|-----------|-------|
| Arabic    | ar    |
| Danish    | da    |
| German    | de    |

(config-vb) device

**Table 3-1** Keyboard Device Emulation Values (continued)

| Emulation              | Value |
|------------------------|-------|
| German (Swiss)         | de-ch |
| English (UK)           | en-gb |
| English (US) (default) | en-us |
| Spanish                | es    |
| Estonian               | et    |
| Finnish                | fi    |
| Faroese                | fo    |
| French                 | fr    |
| French (Belgium)       | fr-be |
| French (Canada)        | fr-ca |
| French (Switzerland)   | fr-ch |
| Croatian               | hr    |
| Hungarian              | hu    |
| Icelandic              | is    |
| Italian                | it    |
| Japanese               | ja    |
| Lithuanian             | lt    |
| Latvian                | lv    |
| Macedonian             | mk    |
| Dutch                  | nl    |
| Dutch (Belgium)        | nl-be |
| Norwegian              | nor   |
| Polish                 | pl    |
| Portuguese             | pt    |
| Portuguese (Brazil)    | pt-br |
| Russian                | ru    |
| Slovenian              | sl    |
| Swedish                | sv    |
| Thai                   | th    |
| Turkish                | tr    |

**Examples**

The following example shows how to set the device emulation parameters for virtual blade 2. The CPU emulator is set to qemu64, the NIC emulator is set to rtl8139, and the disk type emulator is set to IDE.

```
WAE(config)# virtual-blade 2
WAE(config-vb)# device cpu qemu64
WAE(config-vb)# device nic rtl8139
WAE(config-vb)# device disk IDE
```

**Related Commands**

(config-vb) [autostart](#)  
(config-vb) [boot](#)  
(config-vb) [description](#)  
(config-vb) [disk](#)  
(config-vb) [interface](#)  
(config-vb) [memory](#)

(config-vb) disk

## (config-vb) disk

To allocate disk space for a virtual blade on the WAE hard drive, use the **disk** virtual blade configuration command.

**disk disk1-size disk2-size disk3-size disk4-size**

| Syntax Description |   |
|--------------------|---|
|                    | <i>disk1-size</i> Amount of disk space allocated for the virtual disk 1 of the virtual blade in gigabytes. The range of valid values is from 1 to 1000.   |
|                    | <i>disk2-size</i> Amount of disk space allocated for the virtual disk 2 of the virtual blade in gigabytes. The range of valid values is from 0 to 1000.   |
|                    | <i>disk3-size</i> Amount of disk space allocated for the virtual disk 3 of the virtual blade in gigabytes. The range of valid values is from 0 to 1000. If you are using IDE disk emulation, you must specify 0 for the size of disk 3, because this IDE bus position is used for a CD-ROM. |
|                    | <i>disk4-size</i> Amount of disk space allocated for the virtual disk 4 of the virtual blade in gigabytes. The range of valid values is from 0 to 1000.   |

**Defaults** No default behavior or values.

**Command Modes** virtual blade configuration mode

**Device Modes** application-accelerator

**Usage Guidelines** You can configure up to four virtual hard disks on the virtual blade.

**Examples** The following example shows how to allocate 40 GB of disk space for a single virtual hard disk in virtual blade 1:

```
WAE(config)# virtual-blade 1
WAE(config-vb)# disk 40
```

The following example shows how to allocate four virtual hard disks in virtual blade 2:

```
WAE(config)# virtual-blade 2
WAE(config-vb)# disk 10 30 0 15
```

**Related Commands** [\(config-vb\) autostart](#)

[\(config-vb\) boot](#)

[\(config-vb\) description](#)

[\(config-vb\) device](#)

(config-vb) interface

(config-vb) memory

**(config-vb) interface**

# (config-vb) interface

To bridge a virtual blade interface to an interface on your WAE, use the **interface** virtual blade configuration command.

```
interface vb-interface bridge {GigabitEthernet [slot]/[port] | PortChannel channel}
```

|                                   |  |                     |   |               |   |                        |   |             |                                  |             |                             |                                   |  |
|-----------------------------------|--|---------------------|---|---------------|---|------------------------|---|-------------|----------------------------------|-------------|-----------------------------|-----------------------------------|--|
| Syntax Description                | <table border="0"> <tr> <td><i>vb-interface</i></td><td>Virtual blade interface to be bridged; valid values are 1 or 2.</td></tr> <tr> <td><b>bridge</b></td><td>Specifies that a virtual blade interface will be bridged to a physical WAE interface.</td></tr> <tr> <td><b>GigabitEthernet</b></td><td>Specifies a Gigabit Ethernet interface on the WAE, and the port value is 0.</td></tr> <tr> <td><i>slot</i></td><td>(Optional) Slot value is 1 or 2.</td></tr> <tr> <td><i>port</i></td><td>(Optional) Port value is 0.</td></tr> <tr> <td><b>PortChannel</b> <i>channel</i></td><td>Specifies a port channel interface on the WAE. The value is 1.</td></tr> </table> | <i>vb-interface</i> | Virtual blade interface to be bridged; valid values are 1 or 2. | <b>bridge</b> | Specifies that a virtual blade interface will be bridged to a physical WAE interface. | <b>GigabitEthernet</b> | Specifies a Gigabit Ethernet interface on the WAE, and the port value is 0. | <i>slot</i> | (Optional) Slot value is 1 or 2. | <i>port</i> | (Optional) Port value is 0. | <b>PortChannel</b> <i>channel</i> | Specifies a port channel interface on the WAE. The value is 1. |
| <i>vb-interface</i>               | Virtual blade interface to be bridged; valid values are 1 or 2.  |                     |   |               |   |                        |   |             |                                  |             |                             |                                   |  |
| <b>bridge</b>                     | Specifies that a virtual blade interface will be bridged to a physical WAE interface.  |                     |   |               |   |                        |   |             |                                  |             |                             |                                   |  |
| <b>GigabitEthernet</b>            | Specifies a Gigabit Ethernet interface on the WAE, and the port value is 0.  |                     |   |               |   |                        |   |             |                                  |             |                             |                                   |  |
| <i>slot</i>                       | (Optional) Slot value is 1 or 2.   |                     |   |               |   |                        |   |             |                                  |             |                             |                                   |  |
| <i>port</i>                       | (Optional) Port value is 0.  |                     |   |               |   |                        |   |             |                                  |             |                             |                                   |  |
| <b>PortChannel</b> <i>channel</i> | Specifies a port channel interface on the WAE. The value is 1.   |                     |   |               |   |                        |   |             |                                  |             |                             |                                   |  |

**Defaults** No default behavior or values.

**Command Modes** virtual blade configuration mode

**Device Modes** application-accelerator

**Usage Guidelines** The virtual blade requires bridging of its virtual interface to a physical interface on the WAE so that it can connect to the network and other services.

**Examples** The following example shows how to bridge interface 1 on virtual blade 2 to Gigabit Ethernet slot 2, port 0 on the WAE:

```
WAE(config)# virtual-blade 2
WAE(config-vb)# interface 1 bridge GigabitEthernet 2/0
```

**Related Commands**

- [\(config-vb\) autostart](#)
- [\(config-vb\) boot](#)
- [\(config-vb\) description](#)
- [\(config-vb\) device](#)
- [\(config-vb\) disk](#)
- [\(config-vb\) memory](#)

# (config-vb) memory

To allocate memory for a virtual blade from the WAE system, use the **memory** virtual blade configuration command.

**memory** *memory-allocation*

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | <i>memory-allocation</i> Amount of memory allocated for the virtual memory of a virtual blade, in megabytes. |
|---------------------------|--|

|                 |                                |
|-----------------|--------------------------------|
| <b>Defaults</b> | No default behavior or values. |
|-----------------|--------------------------------|

|                      |                                  |
|----------------------|----------------------------------|
| <b>Command Modes</b> | virtual blade configuration mode |
|----------------------|----------------------------------|

|                     |                         |
|---------------------|-------------------------|
| <b>Device Modes</b> | application-accelerator |
|---------------------|-------------------------|

|                         |  |
|-------------------------|--|
| <b>Usage Guidelines</b> | The amount of memory that can be allocated for a virtual blade depends on the amount of memory in your WAE or WAVE appliance, and on the amount of memory that is assigned to other virtual blades. The minimum amount of memory that you can allocate for a single virtual blade is 512 MB. |
|-------------------------|--|

|                 |   |
|-----------------|---|
| <b>Examples</b> | The following example shows how to allocate 4 MB of memory for virtual blade 2: |
|-----------------|---|

```
WAE(config)# virtual-blade 2
WAE(config-vb)# memory 4
```

|                         |   |
|-------------------------|---|
| <b>Related Commands</b> | <a href="#">(config-vb) autostart</a><br><a href="#">(config-vb) boot</a><br><a href="#">(config-vb) description</a><br><a href="#">(config-vb) device</a><br><a href="#">(config-vb) disk</a><br><a href="#">(config-vb) interface</a> |
|-------------------------|---|

---

(config-vb) vnc

## (config-vb) vnc

To enable the VNC server for a virtual blade, use the **vnc** virtual blade configuration command. To disable the VNC server for a virtual blade, use the **no** form of this command.

**vnc**

**no vnc**

---

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

---

**Defaults** The VNC server is enabled by default.

---

**Command Modes** virtual blade configuration mode

---

**Device Modes** application-accelerator

---

**Usage Guidelines** The VNC server is enabled by default.  
When you disable the VNC server, any active VNC connections are closed.

---

**Examples** The following example shows how to disable the VNC server for virtual blade 2:

```
WAE(config)# virtual-blade 2
WAE(config-vb)# no vnc
```

---

**Related Commands**

- [\(config-vb\) autostart](#)
- [\(config-vb\) boot](#)
- [\(config-vb\) description](#)
- [\(config-vb\) device](#)
- [\(config-vb\) disk](#)
- [\(config-vb\) interface](#)

# PKI Certificate Authority Configuration Mode Commands

---

To configure public key infrastructure (PKI) encryption certificate authorities on a WAAS device, use the **crypto pki ca** global configuration command. To delete a PKI encryption certificate authority, use the **no** form of the command.

```
crypto pki ca certificate_authority_name
no crypto pki ca certificate_authority_name
```

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | <i>certificate_authority_name</i> The name of the certificate authority (CA). The CA name may contain up to 64 characters. |
|---------------------------|--|

|                 |                                |
|-----------------|--------------------------------|
| <b>Defaults</b> | No default behavior or values. |
|-----------------|--------------------------------|

|                      |                      |
|----------------------|----------------------|
| <b>Command Modes</b> | global configuration |
|----------------------|----------------------|

|                     |  |
|---------------------|--|
| <b>Device Modes</b> | application-accelerator<br>central-manager |
|---------------------|--|

|                         |  |
|-------------------------|--|
| <b>Usage Guidelines</b> | Use the <b>crypto pki ca</b> command to add and configure a certificate authority. This command initiates the certificate authority configuration mode, indicated by the <b>(config-ca)</b> prompt. Within certificate authority configuration mode, you can use the various commands ( <b>ca-certificate</b> , <b>description</b> , <b>revocation check</b> , and so on) to define an encryption certificate authority. To return to global configuration mode, enter <b>exit</b> at the certificate authority configuration mode prompt. |
|-------------------------|--|

|                 |  |
|-----------------|--|
| <b>Examples</b> | The following example shows how to create or edit a certificate authority named mycertauth. If the certificate authority is already established on the WAAS device, the <b>crypto pki ca</b> command edits it. If the certificate authority does not exist, the <b>crypto pki ca</b> command creates it. |
|-----------------|--|

```
WAE(config)# crypto pki ca mycertauth
WAE(config-ca)# description This-is-my-CA-description
WAE(config-ca)# exit
WAE(config)#
```

|                         |   |
|-------------------------|---|
| <b>Related Commands</b> | <a href="#"><b>(config-ca) ca-certificate</b></a> |
|-------------------------|---|

(config-ca) description  
(config-ca) revocation-check

# (config-ca) ca-certificate

To set the certification authority file to be used by the WAAS device, use the **ca-certificate** certification authority configuration command.

**ca-certificate** *filename.ca*

|                           |                    |  |
|---------------------------|--------------------|--|
| <b>Syntax Description</b> | <i>filename.ca</i> | The filename of the certificate authority. The filename must end in .ca and be no longer than 32 characters. |
|---------------------------|--------------------|--|

|                 |                                |
|-----------------|--------------------------------|
| <b>Defaults</b> | No default behavior or values. |
|-----------------|--------------------------------|

|                      |                                       |
|----------------------|---------------------------------------|
| <b>Command Modes</b> | certification authority configuration |
|----------------------|---------------------------------------|

|                     |  |
|---------------------|--|
| <b>Device Modes</b> | application-accelerator<br>central-manager |
|---------------------|--|

|                         |  |
|-------------------------|--|
| <b>Usage Guidelines</b> | Before you can assign a certification authority file using the <b>ca-certificate</b> command, the certification authority file must be imported using the <b>crypto import ca-certificate</b> EXEC command. See the <a href="#">crypto import</a> command. |
|-------------------------|--|

|                 |   |
|-----------------|---|
| <b>Examples</b> | The following example shows how to specify the certification authority file to use: |
|-----------------|---|

```
WAE(config)# crypto pki ca mycertauth
WAE(config-ca)# ca-certificate mycafile.ca
```

|                         |   |
|-------------------------|---|
| <b>Related Commands</b> | <a href="#">(config-ca) description</a><br><a href="#">(config-ca) revocation-check</a> |
|-------------------------|---|

(config-ca) description

# (config-ca) description

To enter a description for the certification authority to be used by the WAAS device, use the **description** command.

**description** *description-text*

|                           |   |   |
|---------------------------|---|---|
| <b>Syntax Description</b> | <i>description-text</i>   | Text to briefly describe the certification authority being used. The description text cannot contain spaces and must not exceed 256 characters. |
| <b>Defaults</b>           | No default behavior or values.  |   |
| <b>Command Modes</b>      | certification authority configuration   |   |
| <b>Device Modes</b>       | application-accelerator<br>central-manager  |   |
| <b>Examples</b>           | <p>The following example shows how to define the descriptive text for the certification authority:</p> <pre>WAE(config)# crypto pki ca mycertauth WAE(config-ca)# description This-is-my-CA-description</pre> |   |
| <b>Related Commands</b>   | <a href="#">(config-ca) ca-certificate</a><br><a href="#">(config-ca) revocation-check</a>  |   |

# (config-ca) revocation-check

To configure the certification authority revocation checking method, use the **revocation-check** command.

```
revocation-check {none | ocsp-cert-url | ocsp-url} [none | ocsp-cert-url | ocsp-url]
```

## Syntax Description

|                      |   |
|----------------------|---|
| <b>none</b>          | No revocation checking is used.   |
| <b>ocsp-cert-url</b> | Enables Online Certificate Status Protocol (OCSP) revocation status checking using the CA server URL defined in the CA certificate. |
| <b>ocsp-url</b>      | Enables OCSP revocation status checking using the URL defined for the global OCSP settings.   |

## Defaults

No default behavior or values.

## Command Modes

certification authority configuration

## Device Modes

application-accelerator  
central-manager

## Examples

The following example shows how to configure certification authority revocation checking to use the URL defined in the global OCSP settings:

```
WAE(config)# crypto pki ca mycertauth
WAE(config-ca)# revocation-check ocsp-url
```

The following example shows how to configure revocation checking to use the URL defined in the global OCSP settings as the first method, and to use no checking as the second method:

```
WAE(config)# crypto pki ca mycertauth
WAE(config-ca)# revocation-check ocsp-url none
```

## Related Commands

[\(config-ca\) ca-certificate](#)  
[\(config-ca\) description](#)

■ (config-ca) revocation-check

# PKI Global Settings Configuration Mode Commands

To configure public key infrastructure (PKI) encryption global settings on a WAAS device, use the **crypto pki global-settings** global configuration command.

**crypto pki global-settings**

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

**Defaults** No default behavior or values.

**Command Modes** global configuration

**Device Modes** application-accelerator

**Usage Guidelines** Use the **crypto pki global-settings** command to configure OCSP and revocation checking. The **crypto pki global-settings** command initiates the global settings configuration mode, as indicated by the following prompt:

WAE(config-pki-global-settings)

Within global settings configuration mode, you can use the global settings configuration commands to define PKI settings. To return to global configuration mode, enter **exit** at the global settings configuration mode prompt.

**Examples** The following example shows how to enter PKI global settings configuration mode:

```
WAE(config)# crypto pki global-settings
WAE(config-pki-global-settings) #
```

**Related Commands** [\(config-pki-global-settings\) ocsps](#)  
[\(config-pki-global-settings\) revocation-check](#)

---

(config-pki-global-settings) ocsp

## (config-pki-global-settings) ocsp

To enter the URL to be used as the global settings for the Online Certificate Status Protocol (OCSP) protocol revocation status checking, use the `ocsp` PKI global settings configurations mode command.

**ocsp url http://address**

|                           |   |
|---------------------------|---|
| <b>Syntax Description</b> | <b>url http://address</b> The URL to be used for OCSP revocation status checking.   |
| <b>Defaults</b>           | No default behavior or values.  |
| <b>Command Modes</b>      | PKI global-settings configuration   |
| <b>Device Modes</b>       | application-accelerator<br>central-manager  |
| <b>Examples</b>           | The following example shows how to define the OCSP URL as <code>www.myocspurl.com</code> :<br><br>WAE(config)# <b>crypto pki global-settings</b><br>WAE(config-pki-global-settings)# <b>ocsp url http://www.myocspurl.com</b> |
| <b>Related Commands</b>   | <a href="#">(config-pki-global-settings) revocation-check</a>   |

# (config-pki-global-settings) revocation-check

To configure the global settings revocation checking method, use the **revocation-check** command.

```
revocation-check {ocsp-cert-url | ocsp-url} [none]
```

|                           |   |
|---------------------------|---|
| <b>Syntax Description</b> | <b>ocsp-cert-url</b> Enables Online Certificate Status Protocol (OCSP) revocation status checking using the CA server URL defined in the CA certificate.<br><b>ocsp-url</b> Enables OCSP revocation status checking using the URL defined for the global OCSP settings. |
|---------------------------|---|

|                 |                                |
|-----------------|--------------------------------|
| <b>Defaults</b> | No default behavior or values. |
|-----------------|--------------------------------|

|                      |                                   |
|----------------------|-----------------------------------|
| <b>Command Modes</b> | PKI global settings configuration |
|----------------------|-----------------------------------|

|                     |  |
|---------------------|--|
| <b>Device Modes</b> | application-accelerator<br>central-manager |
|---------------------|--|

|                 |   |
|-----------------|---|
| <b>Examples</b> | The following example shows how to configure the global revocation checking to use the URL defined in the global OCSP settings: |
|-----------------|---|

```
WAE(config)# crypto pki global-settings
WAE(config-pki-global-settings)# revocation-check ocsp-url
```

The following example shows how to configure the global revocation checking use the URL defined in the global OCSP settings as the first method, and to use no checking as the second method:

```
WAE(config)# crypto pki global-settings
WAE(config-pki-global-settings)# revocation-check ocsp-url none
```

|                         |   |
|-------------------------|---|
| <b>Related Commands</b> | <a href="#">(config-pki-global-settings) ocsp</a> |
|-------------------------|---|

■ (config-pki-global-settings) revocation-check

# SSL Cipher List Configuration Mode Commands

A cipher list is customer list of cipher suites that you assign to an SSL connection. To configure secure socket layer (SSL) encryption cipher lists on a WAAS device, use the **crypto ssl cipher-list** global configuration command. To delete a cipher list use the **no** form of the command.

```
crypto ssl cipher-list cipher-list-name  
no crypto ssl cipher-list cipher-list-name
```

|                           |                         |   |
|---------------------------|-------------------------|---|
| <b>Syntax Description</b> | <i>cipher-list-name</i> | The name of the cipher list you want to create or edit. The cipher list name may contain up to 64 characters. |
|---------------------------|-------------------------|---|

|                 |                                |
|-----------------|--------------------------------|
| <b>Defaults</b> | No default behavior or values. |
|-----------------|--------------------------------|

|                      |                      |
|----------------------|----------------------|
| <b>Command Modes</b> | global configuration |
|----------------------|----------------------|

|                     |  |
|---------------------|--|
| <b>Device Modes</b> | application-accelerator<br>central-manager |
|---------------------|--|

|                         |   |
|-------------------------|---|
| <b>Usage Guidelines</b> | Use the <b>crypto ssl cipher-list</b> command to add and configure a cipher list. The <b>crypto ssl cipher-list</b> command initiates the cipher list configuration mode, as indicated by the following prompt: |
|-------------------------|---|

```
WAE(config-cipher-list) #
```

Within cipher list configuration mode, you can use the **cipher** cipher list configuration command to define list of cipher suites. To return to global configuration mode, enter **exit** at the cipher list configuration mode prompt.

|                 |  |
|-----------------|--|
| <b>Examples</b> | The following example shows how to create or edit a cipher list called myciphers. If the cipher list is already established on the WAAS device, the <b>crypto ssl cipher-list</b> command edits it. If the cipher list does not exist, the <b>crypto ssl cipher-list</b> command creates it: |
|-----------------|--|

```
WAE(config)# crypto ssl cipher-list myciphers
WAE(config-ca)# cipher rsa-with-rc4-128-sha
WAE(config-ca)# exit
WAE(config)#+
```

|                         |   |
|-------------------------|---|
| <b>Related Commands</b> | <a href="#">(config-cipher-list) cipher</a> |
|-------------------------|---|

(config-cipher-list) cipher

## (config-cipher-list) cipher

To add a cipher suite to a cipher list, or to change the priority of a cipher suite on the list, use the **cipher** command.

**cipher** *cipher-suite-name* [**priority value**]

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | <i>cipher-suite-name</i><br>The name of the cipher suite you want to add or reprioritize. Type any of the following strings:<br><b>dhe-rsa-with-3des-edc-cbc-sha</b><br><b>dhe-rsa-with-aes-128-cbc-sha</b><br><b>dhe-rsa-with-aes-256-cbc-sha</b><br><b>dhe-rsa-with-des-cbc-sha</b><br><b>rsa-with-3des-edc-cbc-sha</b><br><b>rsa-with-aes-128-cbc-sha</b><br><b>rsa-with-aes-256-cbc-sha</b><br><b>rsa-with-des-cbc-sha</b><br><b>rsa-with-rc4-128-md5</b><br><b>rsa-with-rc4-128-sha</b><br>If you are establishing an SSL connection to a Microsoft IIS server, do not select a DHE-based cipher suite. |
| <b>priority value</b>     | The priority of the cipher suite in relation to other suites in the list. The priority value is from 1 to 15 (15 is the highest).  |

**Defaults** No default behavior or values.

**Command Modes** cipher list configuration mode

**Device Modes** application-accelerator  
central-manager

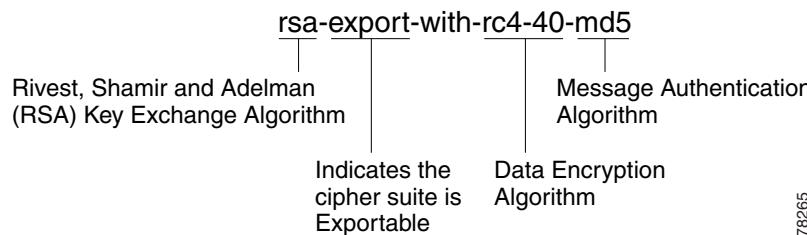
**Usage Guidelines** The SSL protocol supports a variety of different cryptographic algorithms, or ciphers, for use in operations such as authenticating the server and client to each other, transmitting certificates, and establishing session keys. Clients and servers may support different cipher suites, or sets of ciphers, depending on various factors such as the version of SSL they support, company policies regarding acceptable encryption strength, and government restrictions on export of SSL-enabled software. Among its other functions, the SSL handshake protocol determines how the server and client negotiate which cipher suites they will use to authenticate each other to transmit certificates and to establish session keys.

**Note**

Note *Exportable* cipher suites are those cipher suites that are considered not to be as strong as some of the other cipher suites (for example, 3DES or RC4 with 128-bit encryption) as defined by U.S. export restrictions on software products. Exportable cipher suites may be exported to most countries from the United States, and provide the strongest encryption available for exportable products.

Each cipher suite specifies a set of key exchange algorithms. For example, [Figure 3-1](#) summarizes the algorithms associated with the rsa-export-with-rc4-40-md5 cipher suite.

**Figure 3-1** *Cipher Suite Algorithms*



78265

[Table 3-1](#) lists the supported cipher suites and indicates whether those cipher suites are exportable, the authentication certificate, and the encryption key required by the cipher suite.

**Table 3-1** *SSL Cipher Suites*

| <b>Cipher Suite</b>           | <b>Exportable</b> | <b>Authentication Certificate Used</b> | <b>Key Exchange Algorithm Used</b>    |
|-------------------------------|-------------------|--|---------------------------------------|
| rsa-with-rc4-128-md5          | No                | RSA certificate                        | RSA key exchange                      |
| rsa-with-rc4-128-sha          | No                | RSA certificate                        | RSA key exchange                      |
| rsa-with-des-cbc-sha          | No                | RSA certificate                        | RSA key exchange                      |
| rsa-with-3des-ede-cbc-sha     | No                | RSA certificate                        | RSA key exchange                      |
| dhe-rsa-with-des-cbc-sha      | No                | RSA certificate                        | Ephemeral Diffie-Hellman key exchange |
| dhe-rsa-with-3des-ede-cbc-sha | No                | RSA certificate                        | Ephemeral Diffie-Hellman key exchange |

**Note**

The client-specified order for ciphers overrides the cipher list priority assigned here if the cipher list is applied to an accelerated service. The priorities assigned in this cipher list are only applicable if the cipher list is applied to SSL peering and management services.

**Examples**

The following example shows how to enter cipher list configuration mode for the cipher list named myciphers, and then add the cipher suite rsa-with-3des-ede-cbc-sha with a priority of 1:

```
WAE(config)# crypto ssl cipher-list myciphers
```

**(config-cipher-list) cipher**

```
WAE(config-cipher-list)# cipher rsa-with-3des-edc-cbc-sha priority 1
```

**Related Commands** [\*\*\(config\) crypto ssl\*\*](#)



# A P P E N D I X 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)

| <b>Acronym</b> | <b>Expansion</b>                    |
|----------------|-------------------------------------|
| 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 [3-415](#)
- (config) accelerator cifs [3-418](#)
- (config) accelerator cifs preposition [3-420](#)
- (config) accelerator epm [3-421](#)
- (config) accelerator http [3-422](#)
- (config) accelerator mapi [3-423](#)
- (config) accelerator nfs [3-424](#)
- (config) accelerator ssl [3-425](#)
- (config) accelerator video [3-427](#)
- (config) accelerator windows-print [3-429](#)
- (config) alarm overload-detect [3-430](#)
- (config) asset [3-432](#)
- (config) authentication configuration [3-433](#)
- (config) authentication content-request [3-438](#)
- (config) authentication fail-over [3-442](#)
- (config) authentication login [3-446](#)
- (config) auto-discovery [3-453](#)
- (config) auto-register [3-454](#)
- (config) banner [3-456](#)
- (config) bypass [3-459](#)
- (config) cdp [3-461](#)
- (config) central-manager [3-462](#)
- (config) clock [3-464](#)
- (config) cms [3-468](#)
- (config) crypto pki [3-471](#)
- (config) device mode [3-473](#)
- (config) directed-mode [3-474](#)
- (config) disk disk-name [3-475](#)
- (config) disk encrypt [3-477](#)
- (config) disk error-handling [3-478](#)
- (config) disk logical shutdown [3-479](#)
- (config) egress-method [3-480](#)
- (config) end [3-482](#)
- (config) exec-timeout [3-483](#)
- (config) exit [3-484](#)
- (config) flow monitor [3-485](#)
- (config) help [3-486](#)
- (config) hostname [3-488](#)
- (config) inetd [3-490](#)
- (config) inline vlan-id-connection-check [3-491](#)
- (config) interface GigabitEthernet [3-492](#)
- (config) interface InlineGroup [3-497](#)
- (config) interface PortChannel [3-499](#)
- (config) interface standby [3-501](#)
- (config) ip [3-502](#)
- (config) ip access-list [3-504](#)
- (config) kerberos [3-507](#)
- (config) kernel kdb [3-509](#)
- (config) kernel kdump [3-510](#)
- (config) line [3-511](#)
- (config) logging console [3-512](#)
- (config) logging disk [3-514](#)
- (config) logging facility [3-516](#)
- (config) logging host [3-518](#)
- (config) ntp [3-520](#)
- (config) policy-engine application classifier [3-522](#)
- (config) policy-engine application map adaptor EPM [3-524](#)
- (config) policy-engine application map adaptor WAFS transport [3-526](#)
- (config) policy-engine application map basic [3-528](#)
- (config) policy-engine application map other optimize DRE [3-531](#)
- (config) policy-engine application map other optimize full [3-533](#)

(config) policy-engine application map other pass-through **3-534**  
(config) policy-engine application name **3-535**  
(config) policy-engine application set-dscp **3-537**  
(config) policy-engine config **3-539**  
(config) port-channel **3-541**  
(config) primary-interface **3-542**  
(config) print-services **3-544**  
(config) radius-server **3-546**  
(config) smb-conf **3-548**  
(config) snmp-server access-list **3-552**  
(config) snmp-server community **3-553**  
(config) snmp-server contact **3-555**  
(config) snmp-server enable traps **3-556**  
(config) snmp-server group **3-559**  
(config) snmp-server host **3-561**  
(config) snmp-server location **3-563**  
(config) snmp-server mib **3-564**  
(config) snmp-server notify inform **3-566**  
(config) snmp-server trap-source **3-567**  
(config) snmp-server user **3-568**  
(config) snmp-server view **3-570**  
(config) sshd **3-571**  
(config) ssh-key-generate **3-574**  
(config) tacacs **3-575**  
(config) tcp **3-578**  
(config) telnet enable **3-580**  
(config) tfo exception **3-581**  
(config) tfo optimize **3-582**  
(config) tfo tcp adaptive-buffer-sizing **3-583**  
(config) tfo tcp keepalive **3-584**  
(config) tfo tcp optimized-mss **3-585**  
(config) tfo tcp optimized-receive-buffer **3-586**  
(config) tfo tcp optimized-send-buffer **3-587**  
(config) tfo tcp original-mss **3-588**  
(config) tfo tcp original-receive-buffer **3-589**  
(config) tfo tcp original-send-buffer **3-590**  
(config) transaction-logs **3-591**  
(config) username **3-594**

(config) virtual-blade **3-596**  
(config) wccp access-list **3-598**  
(config) wccp flow-redirect **3-601**  
(config) wccp router-list **3-602**  
(config) wccp shutdown **3-604**  
(config) wccp tcp-promiscuous mask **3-606**  
(config) wccp tcp-promiscuous router-list-num **3-607**  
(config) wccp version **3-609**  
(config) windows-domain **3-610**

---

## EXEC Mode Commands

authentication strict-password-policy **3-451**  
cd **3-4**  
cifs **3-5**  
clear arp-cache **3-7**  
clear cache **3-8**  
clear cdp **3-9**  
clear ip **3-10**  
clear license **3-11**  
clear logging **3-12**  
clear statistics **3-13**  
clear statistics accelerator **3-15**  
clear statistics connection **3-16**  
clear transaction-log **3-18**  
clear users **3-19**  
clear windows-domain-log **3-21**  
clock **3-22**  
cms **3-23**  
cms secure-store **3-26**  
configure **3-29**  
copy cdrom **3-30**  
copy cdrom wow-recovery **3-31**  
copy compactflash **3-32**  
copy disk **3-33**  
copy ftp **3-35**  
copy http **3-39**  
copy running-config **3-43**  
copy startup-config **3-45**

|                                  |                                  |
|----------------------------------|----------------------------------|
| copy sysreport <b>3-46</b>       | deltree <b>3-120</b>             |
| copy system-status <b>3-48</b>   | dir <b>3-121</b>                 |
| copy tech-support <b>3-49</b>    | disable <b>3-123</b>             |
| copy tftp <b>3-51</b>            | disk <b>3-124</b>                |
| cpfile <b>3-53</b>               | dnslookup <b>3-126</b>           |
| crypto delete <b>3-54</b>        | enable <b>3-127</b>              |
| crypto export <b>3-55</b>        | exit <b>3-128</b>                |
| crypto generate <b>3-57</b>      | find-pattern <b>3-129</b>        |
| crypto import <b>3-59</b>        | help <b>3-131</b>                |
| crypto pki <b>3-61</b>           | install <b>3-132</b>             |
| debug aaa accounting <b>3-62</b> | less <b>3-134</b>                |
| debug accelerator <b>3-64</b>    | license add <b>3-135</b>         |
| debug all <b>3-67</b>            | lls <b>3-136</b>                 |
| debug authentication <b>3-69</b> | ls <b>3-138</b>                  |
| debug buf <b>3-71</b>            | mkdir <b>3-140</b>               |
| debug cdp <b>3-73</b>            | mkfile <b>3-141</b>              |
| debug cli <b>3-75</b>            | ntpdate <b>3-142</b>             |
| debug cms <b>3-77</b>            | ping <b>3-143</b>                |
| debug dataserver <b>3-79</b>     | pwd <b>3-144</b>                 |
| debug dhcp <b>3-81</b>           | reload <b>3-145</b>              |
| debug dre <b>3-83</b>            | rename <b>3-146</b>              |
| debug egress-method <b>3-85</b>  | restore <b>3-147</b>             |
| debug emdb <b>3-87</b>           | rmdir <b>3-151</b>               |
| debug epm <b>3-89</b>            | scp <b>3-152</b>                 |
| debug flow <b>3-91</b>           | script <b>3-154</b>              |
| debug generic-gre <b>3-93</b>    | setup <b>3-155</b>               |
| debug key-manager <b>3-95</b>    | show aaa accounting <b>3-156</b> |
| debug logging <b>3-97</b>        | show accelerator <b>3-158</b>    |
| debug ntp <b>3-99</b>            | show alarms <b>3-160</b>         |
| debug print-spooler <b>3-101</b> | show arp <b>3-163</b>            |
| debug rbcpc <b>3-103</b>         | show authentication <b>3-164</b> |
| debug rpc <b>3-105</b>           | show auto-discovery <b>3-166</b> |
| debug snmp <b>3-107</b>          | show auto-register <b>3-167</b>  |
| debug stats <b>3-109</b>         | show banner <b>3-168</b>         |
| debug tfo <b>3-111</b>           | show bypass <b>3-169</b>         |
| debug translog <b>3-113</b>      | show cdp <b>3-170</b>            |
| debug wafs <b>3-115</b>          | show cifs <b>3-176</b>           |
| debug wccp <b>3-117</b>          | show clock <b>3-178</b>          |
| delfile <b>3-119</b>             | show cms <b>3-180</b>            |

|                                |              |   |              |
|--------------------------------|--------------|---|--------------|
| show cms secure-store          | <b>3-183</b> | show statistics connection                | <b>3-288</b> |
| show crypto                    | <b>3-184</b> | show statistics connection auto-discovery | <b>3-290</b> |
| show debugging                 | <b>3-186</b> | show statistics connection closed         | <b>3-292</b> |
| show device-mode               | <b>3-187</b> | show statistics connection conn-id        | <b>3-295</b> |
| show directed-mode             | <b>3-189</b> | show statistics connection egress-methods | <b>3-298</b> |
| show disks                     | <b>3-190</b> | show statistics connection optimized      | <b>3-302</b> |
| show egress-methods            | <b>3-197</b> | show statistics connection pass-through   | <b>3-305</b> |
| show filtering list            | <b>3-198</b> | show statistics crypto ssl ciphers        | <b>3-307</b> |
| show flash                     | <b>3-200</b> | show statistics datamover                 | <b>3-308</b> |
| show hardware                  | <b>3-201</b> | show statistics directed-mode             | <b>3-310</b> |
| show hosts                     | <b>3-204</b> | show statistics dre                       | <b>3-311</b> |
| show inetd                     | <b>3-205</b> | show statistics filtering                 | <b>3-313</b> |
| show interface                 | <b>3-206</b> | show statistics flow                      | <b>3-315</b> |
| show inventory                 | <b>3-211</b> | show statistics generic-gre               | <b>3-318</b> |
| show ip access-list            | <b>3-212</b> | show statistics icmp                      | <b>3-319</b> |
| show ip routes                 | <b>3-214</b> | show statistics ip                        | <b>3-321</b> |
| show kdump                     | <b>3-215</b> | show statistics netstat                   | <b>3-324</b> |
| show kerberos                  | <b>3-216</b> | show statistics pass-through              | <b>3-325</b> |
| show license                   | <b>3-217</b> | show statistics peer                      | <b>3-327</b> |
| show logging                   | <b>3-218</b> | show statistics radius                    | <b>3-330</b> |
| show memory                    | <b>3-219</b> | show statistics services                  | <b>3-332</b> |
| show ntp                       | <b>3-220</b> | show statistics snmp                      | <b>3-333</b> |
| show policy-engine application | <b>3-222</b> | show statistics synq                      | <b>3-335</b> |
| show policy-engine status      | <b>3-226</b> | show statistics tacacs                    | <b>3-336</b> |
| show print-services            | <b>3-228</b> | show statistics tcp                       | <b>3-338</b> |
| show processes                 | <b>3-230</b> | show statistics tfo                       | <b>3-342</b> |
| show radius-server             | <b>3-232</b> | show statistics udp                       | <b>3-346</b> |
| show running-config            | <b>3-234</b> | show statistics wccp                      | <b>3-347</b> |
| show services                  | <b>3-236</b> | show statistics windows-domain            | <b>3-351</b> |
| show smb-conf                  | <b>3-237</b> | show statistics windows-print requests    | <b>3-353</b> |
| show snmp                      | <b>3-239</b> | show synq list                            | <b>3-355</b> |
| show ssh                       | <b>3-245</b> | show sysfs volumes                        | <b>3-356</b> |
| show startup-config            | <b>3-246</b> | show tacacs                               | <b>3-357</b> |
| show statistics accelerator    | <b>3-248</b> | show tcp                                  | <b>3-359</b> |
| show statistics aoim           | <b>3-275</b> | show tech-support                         | <b>3-361</b> |
| show statistics application    | <b>3-279</b> | show telnet                               | <b>3-364</b> |
| show statistics authentication | <b>3-282</b> | show tfo tcp                              | <b>3-365</b> |
| show statistics auto-discovery | <b>3-283</b> | show transaction-logging                  | <b>3-366</b> |
| show statistics cifs           | <b>3-286</b> | show user                                 | <b>3-368</b> |

show users administrative **3-369**  
 show version **3-371**  
 show virtual-blade **3-372**  
 show wccp **3-375**  
 show windows-domain **3-381**  
 shutdown **3-383**  
 snmp trigger **3-386**  
 ssh **3-390**  
 tcpdump **3-391**  
 telnet **3-393**  
 terminal **3-394**  
 test **3-395**  
 tethereal **3-398**  
 traceroute **3-400**  
 transaction-log **3-401**  
 type **3-402**  
 type-tail **3-403**  
 virtual-blade **3-405**  
 wafs **3-407**  
 whoami **3-409**  
 windows-domain **3-410**  
 write **3-413**

(config-if) encapsulation dot1Q **3-619**  
 (config-if) exit **3-620**  
 (config-if) failover timeout **3-621**  
 (config-if) full-duplex **3-622**  
 (config-if) half-duplex **3-624**  
 (config-if) inline **3-626**  
 (config-if) ip **3-628**  
 (config-if) ip access-group **3-630**  
 (config-if) mtu **3-631**  
 (config-if) shutdown **3-632**  
 (config-if) standby **3-633**

## PKI Certificate Authority Configuration Mode Commands

(config-ca) ca-certificate **3-697**  
 (config-ca) description **3-698**  
 (config-ca) revocation-check **3-699**

## PKI Global Settings Configuration Mode Commands

(config-pki=global-settings) revocation-check **3-703**  
 (config-pki-global-settings) ocsp **3-702**

## Preposition Configuration Mode Commands

(config-preposition) credentials **3-664**  
 (config-preposition) dscp **3-665**  
 (config-preposition) duration **3-666**  
 (config-preposition) enable **3-667**  
 (config-preposition) ignore-hidden-dir **3-668**  
 (config-preposition) max-cache **3-669**  
 (config-preposition) max-file-size **3-670**  
 (config-preposition) min-file-size **3-671**  
 (config-preposition) name **3-672**  
 (config-preposition) recursive **3-674**  
 (config-preposition) root **3-675**

## Extended ACL Configuration Mode Commands

(config-ext-nacl) delete **3-649**  
 (config-ext-nacl) deny **3-650**  
 (config-ext-nacl) exit **3-655**  
 (config-ext-nacl) list **3-656**  
 (config-ext-nacl) move **3-657**  
 (config-ext-nacl) permit **3-658**

## Interface Configuration Mode Commands

(config-if) autosense **3-614**  
 (config-if) bandwidth **3-615**  
 (config-if) cdp **3-617**

---

## ■ Command Summary by Mode

(config-preposition) scan-type [3-673, 3-676](#)

(config-preposition) schedule [3-677](#)

(config-preposition) server [3-679](#)

---

## SSL Cipher List Configuration Mode Commands

(config-cipher-list) cipher [3-706](#)

---

## Standard ACL Configuration Mode Commands

(config-std-nacl) delete [3-638](#)

(config-std-nacl) deny [3-639](#)

(config-std-nacl) exit [3-641](#)

(config-std-nacl) list [3-642](#)

(config-std-nacl) move [3-643](#)

(config-std-nacl) permit [3-644](#)

---

## Virtual Blade Configuration Mode Commands

(config-vb) autostart [3-683](#)

(config-vb) boot [3-684](#)

(config-vb) description [3-686, 3-687](#)

(config-vb) disk [3-690](#)

(config-vb) interface [3-692](#)

(config-vb) memory [3-693](#)

(config-vb) vnc [3-694](#)